



IBM System Networking Switch Center

Version 7.1.1

User Guide



IBM System Networking Switch Center

Version 7.1.1

User Guide

Note: Before using this information and the product it supports, read the general information in the *Getting Started* document.

Fourth Edition (April 2013)

© Copyright IBM Corporation 2013

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Installing IBM System Networking Switch Center 7.1	1
Installation Prerequisites	1
System Requirements	1
Windows System Requirements	1
Linux System Requirements	2
AIX System Requirements	2
Disk Storage Requirements	2
Browser Requirements	2
Enabling JavaScript in Microsoft Internet Explorer	2
Enabling JavaScript in Mozilla Firefox	3
Switch Configuration Requirements	3
General Requirements	4
FTP/SFTP/TFTP Server Requirements	4
Installing System Networking Switch Center Manager 7.1	5
Installing IBM System Networking Switch Center 7.1 on an AIX System	5
Installing IBM System Networking Switch Center 7.1 on a Linux System	6
Installing IBM System Networking Switch Center 7.1 on a Windows System	7
Verifying Installation	7
Uninstalling IBM System Networking Switch Center 7.1	9
Uninstalling IBM System Networking Switch Center 7.1 on AIX	9
Uninstalling IBM System Networking Switch Center 7.1 on Linux	9
Uninstalling IBM System Networking Switch Center 7.1 on Windows	9
Getting Started With System Networking Switch Center 7.1	35
Logging into IBM System Networking Switch Center	35
Configuring IBM System Networking Switch Center Installed on a Multi-Homed System	36
On Linux System	37
First Steps	38

Enabling and Disabling Root Users	39
Enabling the Root User	40
Disabling the Root User	41
Changing the Default Passwords	42
Changing the Default Administrator Password	43
Changing the Default Operator Password	44
Changing the Default User Password	45
Changing the Default Root Password	46
How to Discover Switches	47
Using Auto Discovery	47
Auto Discovering Switches in a Subnet Range	49
Auto Discovering Switches by IP Address	52
Using Manual Discovery	54
Importing Device Lists from a CSV File	56
Importing the Device List	57
Exporting a Discovered List of Switches to a CSV File	60
Troubleshooting Switch Import and Discovery Problems	61
About the System Networking Switch Center User Interface	62
About the Home Page	63
Health Status Summary Pane	64
Panic Dump Summary Pane	67
Save Pending Summary Pane	68
Discovery Time Range Summary Pane	69
Running Software Version Summary Pane	70
About the Device List Page	71
The Domains Pane	72
The Summary Status Pane	73
The Device List Pane	74
Stacked Switches	75
Device List Page – Menu Bar	76
Device Menu	77
Group Operations Menu	78
Reports Menu	80
Logs Menu	81
Options Menu	82
Discovery Menu	83

Virtualization Tools Menu	84
Maintenance Menu	85
Help Menu	86
About the Device Console Page	87
Device Console - Top Frame	89
Device Console – Feature (or Left) Frame	90
Device Console – Content (or Right) Frame	91
Device Console Page – Menu Bar	92
Device Console Page – Panel Menu Bar	94
Device List – Go To search option	95
Device List – Favorite Marking and Adding Notes	96
Removing Notes	99
Changing IBM System Networking Switch Center Configuration	100
Changing the Default General Properties	101
Changing the Default Health Check Properties	102
Changing the Default Refresh Configuration Parameters	103
Changing the Default Data Collection Configuration Parameters	104
Changing the Default Log File Configuration Parameters	105
Changing the Default DB Data Purge Configuration Parameters	106
Configuring Authentication	108
Local Authentication	109
TACACS+ Authentication	110
RADIUS Authentication	112
Configuring FTP/SFTP/TFTP Server Parameters	114
Modifying Discovery Parameters	115
VM Management Server – Connector Configuration and VMware Infrastructure (VI) Client Integration	117
Dial Home Configuration	123
Configuring Email Parameters	124
Adding Traps for Dial Home	126
Adding Health Status Messages for Dial Home	127
Email Message Format	128
Configuring Console (SSH/Telnet Client) Application	130
How to View Information About IBM System Networking Switch Center	132
How to View Logs	134
Navigating the Log Files	135

Viewing the Discovery Import Log	136
Viewing the Concurrent Backup Log	137
Viewing the Concurrent Download Log	138
Viewing the Concurrent Reset Log	139
Viewing the Scheduled Backup Log	140
Viewing the Scheduled Download Log	141
Viewing the Scheduled Reset Log	142
Viewing the CLI Push Log File	143
Viewing the DB Log File	144
Viewing the CMI Log	145
Viewing the VSI DB – RESTful Access Log	146
Viewing the Authentication Log	147
Viewing the Sync Config Log File	148
Viewing the VM Server Log	149
Viewing the VMready Deployment Log	150
Advanced Configuration and Tuning	152
Modifying the log.properties Configuration File	153
Modifying the server_config.properties Configuration File	154
Modifying the backup.properties Configuration File	155
Modifying the config-substitutions.properties Configuration File	156
Modifying the alertseverity.properties Configuration File	157
Modifying the cmi.properties Configuration file	158
How to Manually Set Device Discovery Date	159
How to Configure Discovery Time Range	160
Viewing Reports	161
How to View the SNSC Alerts Report	162
How to View the Switch Version Report	164
How to View the Transceiver Information Report	166
How to View the VM Data Center Report	168
How to View the VMready VM Report	170
VMready VM Report – VM Groups	171
VMready VM Report – Port Groups	173
How to Customize Information in Reports	175
Changing the Column Sort Order	176
Displaying or Hiding Columns	177

Performing Group Operations	179
How to Deploy Switch Image and Configuration on One or More Switches	180
How to Upgrade Switch Image on One or More Switches	182
How to Backup Switch Image from One or More Switches	184
How to Upgrade Switch Configuration on One or More Switches	185
How to Backup Switch Configuration from One or More Switches	186
How to Download Panic Dump from One or More Switches	187
How to Download Tech Support Dump from One or More Switches	188
How to View Scheduled Jobs	189
How to Run CLI Commands on One or More Switches	191
How to Collect Data from One or More Switches on Demand	193
How to Retrieve Switch Version Report from One or More Switches	194
How to Retrieve Transceiver Information Report from One or More Switches	195
How to Retrieve VM Data Center Report from One or More Switches	196
How to Invoke Actions on One or More Switches	197
How to Manually Set Discovery Date on One or More Switches	198
How to Add/Remove Notes to/from One or More Switches	199
Monitoring a Switch	201
How to Monitor the Switch	203
Using the Monitoring Buttons	204
About Various Monitor Tabs	205
How to Modify a Statistical Monitoring Page	206
Changing the Column Sort Order	207
Displaying or Hiding Columns	208
How to View Switch Summary	209
Viewing Health Status	210
Viewing Information	211
Viewing Port Status	212
Viewing Port Summary	214
Viewing Events	215
Viewing Syslog	216
How to Monitor Switch Statistics	217
Monitoring SNMP Statistics	218
Viewing Information Summary	220

Monitoring Packet Statistics	221
Monitoring MP CPU Statistics	222
Monitoring STP Statistics	223
Monitoring UFD Statistics	224
Monitoring UFD Information	225
Monitoring NTP Statistics	226
Monitoring Trunk Groups	227
Monitoring Trunk Group Ports	228
Monitoring TACACS+ Authentication Statistics	229
How to Monitor a Port	231
Monitoring Port—Summary	232
Monitoring Port—Interface Statistics	233
Monitoring Port—802.1x Statistics	235
Monitoring Port—LACP Statistics	236
Monitoring Port—LACP Aggregator Information	237
Monitoring Port—LACP Port Aggregator Information	238
Monitoring Port—IP Statistics	239
Monitoring Port—Authenticator Diagnostics Statistics	240
Monitoring Port—Bridge Statistics	242
Monitoring Port—Ethernet Error Statistics	243
Monitoring Port – Transceiver Information	245
How to Monitor Bridge Statistics	246
Monitoring Bridge—Forwarding Database Information	247
Monitoring Bridge—Forwarding Statistics	248
Monitoring Bridge—Base Port Information	249
Monitoring Bridge—CIST Bridge Information	250
Monitoring Bridge—CIST Port Information	251
Monitoring Bridge—STP Information	252
How to Monitor LLDP Information	253
Monitoring LLDP Port Information	254
Viewing EVB (Edge Virtual Bridging) Local Information	255
Viewing EVB (Edge Virtual Bridging) Remote Information	256
How to Monitor Failover Information	257
Monitoring General Trigger Status	258
Monitoring Trigger Information	259
Monitoring Monitored Port Status	260

Monitoring Controlled Port Status	261
How to Monitor vLAG Information	262
Monitoring vLAG General Information	263
Monitoring vLAG PDU Statistics	264
Monitoring vLAG IGMP Statistics	266
Monitoring vLAG ISL Statistics	267
How to Monitor Hotlinks Statistics	268
Monitoring Hotlinks Summary	269
Monitoring Hotlinks Statistics	270
Monitoring Hotlinks Information	271
How to Monitor 802.1x/p Information	272
Monitoring 802.1x General Information	273
Monitoring 802.1p—Priority COSq Information	274
Monitoring Port Priority Information	275
How to Monitor ECP (Edge Control Protocol) Information	276
Viewing ECP (Edge Control Protocol) Channel Information	277
How to Monitor IP Routing	278
Monitoring IP Routing—IP Interface Statistics	279
Monitoring IP Routing—Interface Information	280
Monitoring IP Routing—TCP Statistics	281
Monitoring IP Routing—TCP Connections	282
Monitoring IP Routing—UDP Statistics	283
Monitoring IP Routing—UDP Information	284
Monitoring IP Routing—IP Statistics	285
Monitoring IP Routing—ICMP In Statistics	287
Monitoring IP Routing—ICMP Out Statistics	288
Monitoring IP Routing—DNS Statistics	289
Monitoring IP Routing—Routes	290
Monitoring IP Routing—Routes Standard	291
Monitoring IP Routing—Routes Statistics	292
Monitoring IP Routing—ARP	293
Monitoring IP Routing—ARP Statistics	294
Monitoring IP Routing—Gateway Information	295
Monitoring IP Routing—IP Address Information	296
How to Monitor BGP Routing	297
Monitoring BGP Routing—BGP Peers Summary	298

Monitoring BGP Routing—BGP Routing Table	300
How to Monitor RIP Routing	301
Monitoring RIP Routing—RIP V2 Statistics	302
Monitoring RIP Routing—RIP Route Information	303
How to Monitor OSPF Routing	304
Monitoring OSPF Routing—General OSPF Statistics	305
Monitoring OSPF Routing—OSPF Area Statistics	308
Monitoring OSPF Routing—OSPF Area Neighbor Statistics	309
Monitoring OSPF Routing—OSPF Area Interface Statistics	310
Monitoring OSPF Routing—OSPF Area Receive Error Statistics	311
Monitoring OSPF Routing—OSPF Area Interface Receive Error Statistics	312
Monitoring OSPF Routing—OSPF Interface Change Statistics	313
Monitoring OSPF Routing—OSPF Interface Transmission Statistics	314
Monitoring OSPF Routing—OSPF Interface Neighbor Statistics	315
Monitoring OSPF Routing—OSPF Area Information	317
Monitoring OSPF Routing—OSPF Interface Information	318
Monitoring OSPF Routing—OSPF Neighbor Interface Information	319
Monitoring OSPF Routing—OSPF Virtual Interface Information	320
Monitoring OSPF Routing—OSPF Stats2 Information	321
Monitoring OSPF Routing—OSPF Link-State DB Information	322
Monitoring OSPF Routing—OSPF External Link-State DB Information	323
Monitoring OSPF Routing—OSPF Summary Range Information	324
Monitoring OSPF Routing—OSPF Routes Information	325
How to Monitor IGMP Routing	326
Monitoring IGMP Routing—IGMP Information	327
Monitoring IGMP Routing—Multicast Router Information	328
Monitoring IGMP Routing—IGMP Snooping Statistics	329
How to Monitor Virtual Routing	330
Monitoring Virtual Routing Statistics	331
Monitoring Virtual Routing State	332
How to Monitor Access Control Lists	333
Monitoring ACL Statistics	334
Monitoring ACL Port Statistics	335
Monitoring MAC ACL Statistics	336
Monitoring IP ACL Statistics	337
How to Monitor Fiber Channel over Ethernet (FCoE)	338

Viewing FIP Snooping Port Information	339
Viewing FIP Snooping Statistics	340
Viewing FIP Snooping Information	341
Viewing FIP Snooping FCF Detected Information	342
Viewing FIP Snooping FCoE Connections Detected Information	343
Viewing FIP Snooping VLAN Information	344
How to Monitor QoS Information	345
Monitoring QoS Counters	346
How to Monitor Virtualization	347
Viewing VMready Port Information	348
Viewing VMready VM Information	349
How to Monitor Edge Virtual Bridging (EVB)	350
Viewing VDP TLV (VSI Discovery Protocol Type-Length-Value) Information ...	351
Viewing VSI (Virtual Station Interface) Information	352
Viewing VM Information	353
Viewing VSI DB Information	354
Viewing VSI DB ACL Information	355
How to Monitor Unified Fabric Port Information	356
Monitoring CDCP Information	357
Monitoring Port Information	358
Monitoring QoS Information	359
Monitoring TLV Information	360
Monitoring VLAN Information	361
Monitoring Virtual Port Information	362
How to Monitor iSwitch Information	363
Viewing Port Information	364
Viewing Host Uplink Information	365
How to Launch a Chart	366
How to Export a Statistical Summary	368
Administering Exported Files	369
How to Print a Statistical Summary	370
Configuring the Switch	371
Configuration Steps	373
Editing in Form Pane	374
Editing in Tabular Pane	375

Selection Windows	376
Submitting and Applying Changes	377
About Various Configure Tabs	378
General Switch Configuration	379
General Configuration	380
Software Image Configuration	382
Syslog Hosts Configuration	384
Levels of Severity	386
SNMP Trap Settings	387
Syslog Settings	388
General RADIUS Configuration	390
RADIUS Server Configuration	391
General TACACS+ Configuration	393
TACACS+ Server Configuration	394
TACACS+ User Map Configuration	396
TACACS+ Command Authorization Configuration	397
LDAP Server Configuration	398
Network Time Protocol Configuration	399
NTP MD5 Key Configuration	400
Management Network Configuration	401
Port Mirroring Configuration	402
Configuration, Image, and Dump Control	403
USB Copy	405
Configuring Access Users	406
Configuring Access User	407
Configuring Layer 2 Protocols	408
General Layer 2 Protocol Configuration	409
Configuring Trunks	410
IP Trunk Hash Configuration	411
Trunk Groups Configuration	412
LACP Trunk Group Configuration	413
Configuring LACP	414
LACP General Configuration	415
LACP Ports Configuration	416
Configuring 802.1x	417
General 802.1x Configuration	418

Global 802.1x Configuration	419
Guest VLAN Configuration	420
Port Configuration	421
Configuring MSTP and RSTP	422
MSTP/RSTP Configuration	423
Configuring CIST	424
CIST Bridge Configuration	425
CIST Port Configuration	426
Configuring Spanning Tree Protocol	427
Spanning Tree Configuration	428
STP Groups Configuration	431
STG Port Configuration	432
Configuring Forwarding Database	433
FDB General Configuration	434
FDB Static Configuration	435
FDB Static Multicast Configuration	436
Configuring Virtual Link Aggregation Groups	437
General Configuration	438
Health Check Configuration	439
Trunk Configuration	440
LACP Configuration	441
Inter-Switch Link (ISL) Configuration	442
Configuring Hot Links	443
Hot Links General Configuration	444
Hot Links Triggers Configuration	445
Configuring Virtual LANs	446
VLAN Memberships Configuration	447
Private VLAN Configuration	448
Protocol VLAN Configuration	449
VMAP Configuration for Non-Server Ports	450
VMAP Configuration for Server Ports	451
VMAP Configuration for All Ports	452
Configuring Link Layer Discovery Protocol (LLDP)	453
LLDP General Configuration	454
LLDP Port Configuration	455
Port Global TLV State	457

Configuring Failover	458
General Configuration	459
Triggers Configuration	460
Configuring Active Multipath Protocol (AMP)	461
General Configuration	462
Group Configuration	463
Configuring Edge Control Protocol (ECP)	464
ECP General Configuration	465
Configuring IP Interfaces	466
IP General Configuration	467
IP Interfaces Configuration	468
IP Forwarding Configuration	469
Network Filters Configuration	470
Loopback Interfaces Configuration	471
Static ARP Configuration	472
Configuring Gateways	473
Gateways Configuration	474
Configuring Routes	475
General Configuration	476
IP Static Routes Configuration	477
IPMC Ports Configuration	478
IPMC Trunks Configuration	479
IPMC Adminkeys Configuration	480
Configuring RMAPs	481
General Configuration	482
Access List Configuration	483
AS-Path Access List Configuration	484
Configuring RIP	485
General Configuration	486
RIP Interface Configuration	487
Static Route Redistribute Configuration	488
BGP External Route Redistribute Configuration	489
BGP Internal Route Redistribute Configuration	490
Fixed Route Redistribute Configuration	491
OSPF Route Redistribute Configuration	492
OSPF External Route Redistribute Configuration	493

Configuring OSPF	494
OSPF General Configuration	495
OSPF Area Configuration	496
OSPF Interface Configuration	497
OSPF Summary Range Configuration	499
OSPF Virtual Interface Configuration	500
OSPF Host Table Configuration	501
OSPF Static Routes Configuration	502
OSPF Fixed Routes Configuration	503
OSPF RIP Configuration	504
OSPF MD5 Key Configuration	505
OSPF Loopback Interface Configuration	506
OSPF BGP External Route Redistribute Configuration	507
OSPF BGP Internal Route Redistribute Configuration	508
Configuring BGP	509
General Configuration	510
Peer Configuration	511
Peer Redistribution Configuration	512
Aggregation Configuration	513
Group Configuration	514
Group Redistribution Configuration	515
Configuring IGMP	516
General Configuration	517
Snooping Configuration	518
IGMPv3 Snooping Configuration	519
Static Multicast Router Configuration	520
Relay Configuration	521
Relay Multicast Router Configuration	522
Filter Configuration	523
Filter Ports Configuration	524
Advanced Configuration	525
Querier Configuration	526
Configuring DNS	527
DNS Server Configuration	528
Configuring Bootp-Relay	529
General Configuration	530

Server Configuration	531
Broadcast Domain Configuration	532
Broadcast Domain Server Configuration	533
Option82 Configuration	534
Configuring Flooding	535
VLAN Flooding Configuration	536
Configuring VRRP	537
VRRP General Configuration	538
VRRP Virtual Router Configuration	539
VRRP Virtual Interface Configuration	541
VRRP Virtual Router Group Configuration	542
Configuring DHCP Snooping	543
DHCP Snooping Configuration	544
DHCP Snooping VLAN Configuration	545
Configuring ARP	546
ARP Configuration	547
Static ARP Configuration	548
Configuring Ports	549
Port Properties Configuration	550
Ports General Configuration	552
Threshold Rate Configuration	553
Gigabit Link Configuration	554
Unidirectional Link Detection (UDLD) Configuration	555
Operations, Administration and Management (OAM) Configuration	556
ACL Configuration	557
STP Configuration	558
Port Priority Configuration	559
DHCP Snooping Configuration	560
WRED/ECN General Configuration	561
WRED/ECN Profile Configuration	562
Configuring QoS – WRED/ECN	563
General Configuration	564
Global Profile Configuration	565
Configuring ACLs	566
General ACL Properties Configuration	567
Adding an ACL	568

ACL Groups Configuration	570
ACL Block Configuration	571
Management ACL Configuration	572
ACL Log Configuration	573
ACL VMAPs Configuration	574
Adding VMAPs to an ACL	575
MAC ACL Configuration	577
IP ACL Configuration	578
Configuring CEE (Converged Enhanced Ethernet)	580
CEE General Configuration	581
Priority Allocation Configuration	582
Bandwidth Allocation Configuration	583
PFC (Priority Flow Control) Configuration	584
PFC Status Configuration	585
Port PFC Configuration	586
Port PFC Status Configuration	587
DCBX (Data Center Bridging Capability Exchange) Protocol Configuration ...	588
Configuring Multicast Priority	589
Configuring Multicast Bandwidth Allocation	590
Configuring FCoE (Fiber Channel over Ethernet)	591
FIP Snooping Configuration	592
FIP Snooping Port Configuration	593
Configuring Switch Partition	594
SPAR IDs Configuration	595
SPAR Local Domains Configuration	596
Configuring Virtualization	597
General VM Configuration	598
VMware vCenter Configuration	599
VM Profiles Configuration	600
VM Groups Configuration	601
VM Bandwidth Configuration	602
VM Check Configuration	603
VM Hello Configuration	604
VM Ports Configuration	605
Virtual Machines Configuration	606
VM Advanced Pre-Provisioning	607

vNIC General Configuration	608
vNIC Port Configuration	609
vNIC Group Configuration	610
EVB General Configuration	611
EVB Profiles Configuration	612
VSI DB Host Configuration	613
Configuring iSwitch Virtual Data Station	614
vCenter Configuration	615
Virtual Data Station Configuration	616
Configuring Unified Fabric Port (UFP)	617
UFP General Configuration	618
UFP Ports Configuration	619
UFP Virtual Ports Configuration	620
Using the VMready Across the Datacenter Wizard.....	621
Configuring VMready Across the Datacenter Wizard	622
Step 2: Select VMready Switches	626
Step 3: Define the VM Management Server	628
Step 4: Select Hypervisors	631
Step 5: Configure VM Groups	633
Step 6: Configure Virtual Machines	635
Step 6.1: Pre-Provisioned VM MAC	637
Step 6.2: Add VMs Learned or Retrieved	638
Step 7: VMAPs	639
Step 7.1: Configure VMAPs	640
Step 7.2: Add VMAP Configuration	642
Step 7.3: Deploy VMAP Configuration	644
Step 8: Configure Server Ports	645
Step 8.1: Configuring Server Ports	647
Step 9: Configure Switch-Specific Settings	648
Step 9.1: Modifying Switch-Specific Settings	650
Step 10: Configure Port Groups	651
Step 10.1: Modify Port Group Settings	653
Step 11: Associate Port Group to a vSwitch	654
Step 12: Review and Deploy the Configuration	657
Step 12.1: Deploying the VMready Configuration	659

Centralized VSI Database	661
VSI Database Overview	662
How to Configure VSI DB from the VSI DB Console	663
VSI ACL Configuration	664
VSI Type Configuration	667
How to Administer VSI Database Using RESTful APIs	669
VSI Types RESTful APIs	670
Access Control for RESTful APIs	671
XML Schema for VSI Types	672
VSI Types RESTful API Reference - Examples	675
GET Request to Retrieve VSI Types Configured with a Specific Version	676
GET Request to Retrieve an Individual VSI Type	679
GET Request to Retrieve All Configured VSI Types	681
POST Request to Create a VSI Type	685
PUT Request to Modify an Existing VSI Type	687
DELETE Request to Delete an Existing VSI Type	688
Performing Device-Specific Actions	689
Synchronizing the Configuration - Sync Config	690
VLAN and Port Synchronization	692
Global Actions	694
Launching Device Access Utilities	695
Launching CLI Interface	696
Launching Web Interface	697
Maintenance	699
Taking System Networking Switch Center's Critical Data Backup	700
Setting Backup Directory on IBM System Networking Switch Center Server	701
Initiating Critical Data Backup	702
Restoring the Data from the Critical Data Backup	703
Restoring the Data for IBM System Networking Switch Center Installed on a Linux System	704
Taking IBM System Networking Switch Center Support Dump	705

Manager of Managers	707
Manager of Managers Overview	708
Enabling the Manager of Managers Service	709
Logging In to the Manager of Managers	710
About Manager of Managers Windows and Panels	711
Main Window	712
Instance View Window	713
Summary Panel	714
Performing Actions in the Manager of Managers	716
Adding an Instance of IBM System Networking Switch Center	717
Renaming an Instance of IBM System Networking Switch Center	718
Deleting an Instance of IBM System Networking Switch Center	719
Launching Switch Version Report	720
Launching IBM System Networking Switch Center	722
Using the Command Line Interface	723
Launching the CLI Shell	724
Using the CLI for Individual Command Execution	724
CLI Command Reference	724
options general	725
options refresh	726
options security	726
options purge	728
options logfile	728
options data_collection	729
options cli_conf	729
options hpsim	730
options dial_home	732
options vm	734
show	737
device add	740
device delete	742
device import	743
device export	744
reports event	744

reports svr	745
reports vmr	746
stats acl	746
stats bridge	748
stats port	748
stats routing	750
stats switch	754
stats virtual_routing	755
info 8021	756
info bridge	756
info hotlinks	758
info port	758
info routing	759
info switch	763
info virtual_routing	764
firmware apply	764
firmware backup	765
firmware conf_backup	768
firmware conf_upload	771
firmware config_dump	774
firmware diff_config	774
firmware diff_flash	774
firmware panicdump	775
firmware reset	778
firmware save	779
firmware tsdump	780
firmware upload	783
data backup	786
support dump	787

Appendix A: Externally Launching IBM System Networking Switch Center789

List of Page IDs	790
------------------------	-----

Appendix B: Integrating SNSC with IBM Tivoli Network Manager 799

Requirements	799
Step 1: Generate Signer Certificate	799

Step 2: Create Key Store	803
Step 3: Configure System Networking Switch Center for LIC & SSO	804
Step 4: Create System Networking Switch Center User Groups in IBM Tivoli Network Manager	805
Step 5: Edit IBM Tivoli Network Manager tools and menu configuration files ...	809
Step 5.1: IBM Tivoli Network Manager – TNM Properties	810
Step 5.2: IBM Tivoli Network Manager – Create System Networking Switch Center Launch-In-Context Tools Files	811
Step 5.3: IBM Tivoli Network Manager – Create System Networking Switch Center Launch-In-Context Menu File	812
Step 5.4: IBM Tivoli Network Manager – Update Global Launch-In-Context Menu File 813	
Step 6: Re-login to IBM Tivoli Network Manager TIP GUI	813
Appendix C: Integrating System Networking Switch Center with IBM Systems Director	815
Step 1: Create External App Launch Template File	815
Step 2: Register External App Launch Template File	821
Step 3: Configure Single Sign-On Credentials	822
Appendix D: Using Third-Party JDBC/ODBC Tools for Querying SNSC Database 827	
Requirements	827
Task 1: EasySoft ODBC-JDBC Gateway – Configuring JVM	827
Task 2: EasySoft ODBC-JDBC Gateway – Configuring Data Source (DSN) ...	828
Task 3: ODBC Test Utility – Connecting to Data Source	829
Task 4: ODBC Test Utility – Retrieving the Data from the Database and Viewing	830
Index	833

Installing IBM System Networking Switch Center 7.1

IBM System Networking Switch Center allows you to administer and maintain switches through a Web browser interface.

- [“Installation Prerequisites” on page 1](#)
- [“Installing System Networking Switch Center Manager 7.1” on page 5](#)
- [“Uninstalling IBM System Networking Switch Center 7.1” on page 9](#)

Installation Prerequisites

- [“System Requirements” on page 1](#)
- [“Disk Storage Requirements” on page 2](#)
- [“Browser Requirements” on page 2](#)
- [“Switch Configuration Requirements” on page 3](#)
- [“General Requirements” on page 4](#)
- [“FTP/SFTP/TFTP Server Requirements” on page 4](#)

System Requirements

IBM System Networking Switch Center (SNSC) is a Web application that you install on an AIX, Linux, or Windows system. The system must meet the following requirements:

Windows System Requirements

- Intel 32-bit or 64-bit system
- Windows 500 MB 500 MB Server 2008 or Windows Server 2012
- Minimum 1 GB RAM
- Minimum 500 MB free disk space during installation

Linux System Requirements

- Intel 32-bit system
- SUSE Linux Enterprise Server 10, SUSE Linux Server 11, Red Hat Enterprise Linux 6.1 for x86, or Red Hat Enterprise Linux 6.2 for x86
- Minimum 1 GB RAM
- Minimum 500 MB free disk space during installation

AIX System Requirements

- AIX® 6.1 on Power or AIX 7.1 on Power
- Minimum 1 GB RAM
- Minimum 500 MB free disk space during installation

Disk Storage Requirements

Consider the following when you plan disk space for SNSC:

- The total number of discovered devices.
- The number of SNSC active UI sessions with a page monitoring/viewing performance data
- The number of days that you plan to store switch performance data and events in the SNSC database

Typically, you need to plan for the following amount of disk space:

- 1K per device.
- 5 MB per hour for each SNSC UI session monitoring performance data at 10 seconds frequency
- 1 MB for storing 5000 events (traps and syslogs) received from a device

Browser Requirements

System Networking Switch Center is a Web application. You can log into SNSC from any system that supports the following browser versions:

- Microsoft Internet Explorer Version 8.x and 9.x
- Mozilla Firefox Version 10.x or higher

You must enable JavaScript on each browser.

Enabling JavaScript in Microsoft Internet Explorer

- 1 Open Microsoft Internet Explorer.

- 2 Click **Tools > Internet Options**.
- 3 Click **Security**.
- 4 Click the Internet icon.
- 5 Click **Custom Level**.
- 6 Scroll to **Scripting**.
- 7 Click **Enable Active Scripting**.
- 8 Click **OK**.

Enabling JavaScript in Mozilla Firefox

- 1 Open Mozilla Firefox.
- 2 Click **Tools > Options**.
- 3 Click **Content**.
- 4 Click **Enable JavaScript**.
- 5 Click **OK**.

Switch Configuration Requirements

Be sure that each switch that you plan to discover meets the following requirements.

- Ensure that SNMP access is enabled on the switch. See the *User Guide* documentation for the switch for information about how to enable SNMP access.
- Ensure that the switch is physically connected to the network.
- Ensure that the switch is turned on and receiving power.
- Ensure that the switch has a correct IP address.
- Ensure that the switch is not blocking access from the client IP address.
- Be sure that you can successfully ping the switch.
- If you plan to use the automatic switch discovery feature, you must configure the switches in either SNMPv1 or SNMPv2c.
- If you plan to use the manual discovery feature, you can configure the switch in SNMPv1 or SNMPv2c or v3.

General Requirements

- You must locate a copy of the SNSC 7.1 installation image.
- You must have an ID with administrator privileges on the server where you plan to install SNSC 7.1.
- SNSC 7.1 uses the following ports:
 - Port 40080 for HTTP
 - Port 40443 for HTTPs
 - Port 40999 for RMI Service

Ensure that no applications use the ports, or configure SNSC to use different ports.

SNSC 7.1 also uses the following standard ports:

- Port 162 for SNMP trap reception
- Port 514 for syslog reception

Ensure that no other applications use the ports in the list.

FTP/SFTP/TFTP Server Requirements

SNSC requires but does not install an FTP, SFTP, or TFTP server. You must provide and configure an FTP, SFTP, or TFTP server to perform any of the image and configuration management functions (see [“Configuring FTP/SFTP/TFTP Server Parameters” on page 114](#)).

Installing System Networking Switch Center Manager 7.1

The instructions in this section explain how to install SNSC 7.1 on AIX, Linux, or Windows systems.

Installing IBM System Networking Switch Center 7.1 on an AIX System

Note: The installers have the signature `7.1.x.x_install_aix.sh`. In the following procedures, `<installer>.sh` is used to indicate the signature being installed.

New Installation

- 1 Log in as root on the AIX system where you plan to install SNSC 7.1.
- 2 Download the SNSC 7.1 installer for AIX from the IBM Web site.
- 3 Run the installation script as follows:
`# <installer>.sh`
- 4 The SNSC 7.1 application will be installed in the following directory:
`/opt/ibm/SNSC`

The installer automatically starts SNSC services near the end of the installation process.

SNSC services are registered with the init process, which causes the services to start automatically when the AIX system starts.

Upgrading the Existing System Networking Switch Center

- 1 Log in as root on the AIX system that includes the System Networking Switch Center software you want to upgrade.
- 2 Download the SNSC 7.1 installer for AIX from the IBM Web site.
- 3 Run the installation script as follows:
`# <installer>.sh`
- 4 The installation prompts you to confirm whether to proceed with the upgrade. Enter **yes** to upgrade SNSC to version 7.1.

The installer automatically starts SNSC services near the end of upgrade process.

Installing IBM System Networking Switch Center 7.1 on a Linux System

Note: The installers have the signature `7.1.x.x_install_lin.sh`. In the following procedures, `<installer>.sh` is used to indicate the signature being installed.

New Installation

- 1 Log in as root on the Linux system where you plan to install SNSC 7.1.
- 2 Download the SNSC 7.1 installer for Linux from the IBM Web site.
- 3 Run the installation script as follows:
`# <installer>.sh`
- 4 The SNSC 7.1 application will be installed in the following directory:
`/opt/ibm/SNSC`

The installer automatically starts SNSC services near the end of the installation process.

SNSC services are registered with the init process, which causes the services to start automatically when the Linux system starts.

Upgrading the Existing System Networking Switch Center

- 1 Log in as root on the Linux system that includes the SNSC software you want to upgrade.
- 2 Download the SNSC 7.1 installer for Linux from the IBM Web site.
- 3 Run the installation script as follows:
`# <installer>.sh`
- 4 The installation prompts you to confirm whether to proceed with the upgrade. Enter **yes** to upgrade SNSC to version 7.1.

The installer automatically starts SNSC services near the end of the upgrade process.

Installing IBM System Networking Switch Center 7.1 on a Windows System

Note: The installers have the signature 7.1.x.x_install_win.exe. In the following procedures, *<installer>.exe* is used to indicate the signature being installed.

New Installation

- 1 Log in as an administrator on the Windows system where you plan to install SNSC 7.1.
- 2 Download the SNSC 7.1 installer for Windows from the IBM site.
- 3 Double-click *<installer>.exe*
- 4 Click **Next**.
- 5 Select the typical installation option.
- 6 Click **Finish**.

The installer automatically starts SNSC services near the end of the installation process.

SNSC services are registered as Windows Services. Hence, they are automatically started when the Windows system starts up.

Upgrading the Existing System Networking Switch Center

- 1 Log in as an administrator on the Windows system that includes the SNSC software you want to upgrade.
- 2 Download the SNSC 7.1 installer for Windows from the IBM site.
- 3 Double-click *<installer>.exe*
- 4 Click **Next**.
- 5 The installation program prompts you to confirm whether to proceed with the upgrade. Click **yes** to upgrade SNSC to version 7.1.
- 6 Click **Finish**.

The installer automatically starts SNSC services near the end of the installation process.

Verifying Installation

Prerequisite: Before you can verify installation, you must ensure that the SNSC 7.1 services are started on the server where SNSC is installed.

- To check if the SNSC services are running on AIX or Linux, login as 'root' and run the following shell script:
/opt/ibm/SNSC/bin/check.sh
- To start SNSC services on AIX or Linux, login as 'root' and run the following shell script:
/opt/ibm/SNSC/bin/startup.sh
- To check if the SNSC services are running on Windows, login as Administrator and choose menu **Start > All Programs > IBM > System Networking Switch Center > Check Services.**
- To start the services on Windows, login as Administrator and choose menu **Start > All Programs > IBM > System Networking Switch Center > Start Services.**

In this procedure you test the local browser connection on the server and verify that the three default users created by the installation program can log in successfully. For information about the privileges available to the default users, see ["Changing the Default Passwords" on page 42.](#)

- 1 Launch a browser.
 - a If you are logged in to the server where you installed SNSC 7.1, enter
http://localhost:40080/snc
or https://localhost:40443/snc
 - b If you are logging in to SNSC 7.1 from another computer, enter
http://<hostname>:40080/snc, where <hostname> is the DNS name or IP address of the server where SNSC 7.1 is installed. If you enabled HTTPS, enter:
https://<hostname>:40443/snc
- 2 Enter admin/admin.
- 3 Verify that the home page displays.
- 4 Click **Logout.**
- 5 Enter oper/oper.
- 6 Verify that the home page displays.
- 7 Click **Logout.**
- 8 Enter user/user.
- 9 Verify that the home page displays.
- 10 Click **Logout.**
- 11 Make a note of the hostname where you installed SNSC. You will distribute the hostname to other administrators, operators and users.

Uninstalling IBM System Networking Switch Center 7.1

The instructions in this section explain how to uninstall SNSC 7.1 on an AIX, Linux, or Windows system.

- [“Uninstalling IBM System Networking Switch Center 7.1 on AIX” on page 9](#)
- [“Uninstalling IBM System Networking Switch Center 7.1 on Linux” on page 9](#)
- [“Uninstalling IBM System Networking Switch Center 7.1 on Windows” on page 9](#)

Uninstalling IBM System Networking Switch Center 7.1 on AIX

- 1 Log in as root on the system where you have installed SNSC 7.1.
- 2 Uninstall SNSC 7.1 by issuing the following command:
`# /opt/ibm/SNSCManager/uninstall/uninstall.sh`

Uninstalling IBM System Networking Switch Center 7.1 on Linux

- 1 Log in as root on the system where you have installed SNSC 7.1.
- 2 Uninstall SNSC 7.1 by issuing the following command:
`# /opt/ibm/SNSC/uninstall/uninstall.sh`

Uninstalling IBM System Networking Switch Center 7.1 on Windows

- 1 Log in as administrator on the system where you have installed SNSC 7.1.
- 2 Uninstall SNSC 7.1 by clicking **Start > Programs > IBM > System Networking Switch Center > Uninstall System Networking Switch Center**.
- 3 You can also uninstall SNSC 7.1 by clicking **Start > Settings > Control Panel > Add or Remove Programs**. Select **System Networking Switch Center – 7.x.x.x** and click **Change/Remove**.

Getting Started With System Networking Switch Center 7.1

Logging into IBM System Networking Switch Center

Launch a browser and log in to IBM System Networking Switch Center (SNSC). If you did not configure HTTP security on the System Networking Switch Center server, you might enter a URL that is similar to `http://<hostname>:40080/snsc`, where *hostname* is the domain name or IP address of the server where you installed System Networking Switch Center. If System Networking Switch Center is installed on a multi-homed system and is configured to use a specific IP address (see [“Configuring IBM System Networking Switch Center Installed on a Multi-Homed System” on page 36](#)), then *<hostname>* should be that IP address.

If you configured and enabled security on the System Networking Switch Center server and you want to log in with a secure HTTPS connection, you might enter a URL that is similar to `https://<hostname>:40443/snsc`

Enter `admin` in the User Name field and enter `admin` in the Password field the first time that you log in.

- [“Configuring IBM System Networking Switch Center Installed on a Multi-Homed System” on page 36](#)
- [“First Steps” on page 38](#)
- [“How to Discover Switches” on page 47](#)
- [“About the System Networking Switch Center User Interface” on page 62](#)
- [“How to View Information About IBM System Networking Switch Center” on page 132](#)
- [“How to View Information About IBM System Networking Switch Center” on page 132](#)
- [“How to View Logs” on page 134](#)
- [“Advanced Configuration and Tuning” on page 152](#)
- [“How to Manually Set Device Discovery Date” on page 159](#)

Configuring IBM System Networking Switch Center Installed on a Multi-Homed System

If you are planning to install System Networking Switch Center on a multi-homed system that has multiple IP addresses to connected networks, you may want System Networking Switch Center to use a particular IP address of that system for all operations.

You can configure System Networking Switch Center to use a particular IP address using the following steps:

On Linux System

- 1 Login to the system as a root user.
- 2 Stop SNSC Service by issuing the following command:
`# /opt/ibm/snsc/bin/shutdown.sh`
- 3 Run `configure_multihome.bat` by issuing the following command:
`# /opt/ibm/snsc/bin/configure_multihome.sh`
- 4 This script prompts you to continue and then lists all the IP addresses configured on that system.
- 5 Choose the IP address that you want System Networking Switch Center to use (this step also requires a confirmation).
- 6 Once the operation is complete, start SNSC Service by issuing the following command:
`# /opt/ibm/snsc/bin/startup.sh`
- 7 System Networking Switch Center listens on the given IP address for UI requests and it also uses the IP address for administering the devices.

First Steps

The first time that you log in to System Networking Switch Center, complete the following steps. You must log in as an administrator to complete the steps.

- 1 Enable or Disable Root Users (see [“Enabling and Disabling Root Users” on page 39](#))
- 2 Change the default admin, oper and user passwords (see [“Changing the Default Passwords” on page 42](#)).
- 3 Discover switches (see [“How to Discover Switches” on page 47](#)).

Enabling and Disabling Root Users

By default, System Networking Switch Center allows users who have administrator privileges to modify user passwords (Security Configuration) and change the authentication mechanism (Local or RADIUS or TACACS+ through Authentication Configuration). However, some deployments may want to enforce stricter access privileges for such operations. To address such deployments, System Networking Switch Center allows users to enable a special privileged 'root' user. The root user brings in the following changes:

- When you enable root user mode, System Networking Switch Center requires that you enter the root password before you can perform security and authentication configuration
- You cannot directly log in to System Networking Switch Center as root. You must login with the normal Admin/Oper/User credentials and then enter root password while performing Security and Authentication Configuration.
- The default root password is root.
- The root user is disabled by default.

Enabling the Root User

Use the following procedure to enable the Root User.

1 Stop SNSC Service:

On a Linux system, issue the following command:

```
# /opt/ibm/snsc/bin/shutdown.sh
```

2 Navigate to the following directory:

```
<SNSC Installation Directory>/conf/auth
```

3 Open the following file in a text editor: `rootuser.properties`

4 Set `enabledRootUser` to `true`.

5 Start SNSC Service:

On a Linux system, issue the following command:

```
# /opt/ibm/snsc/bin/startup.sh
```


Disabling the Root User

Use the following procedure to disable the Root User.

1 Stop SNSC Service:

On a Linux system, issue the following command:

```
# /opt/ibm/snsc/bin/shutdown.sh
```

2 Navigate to the following directory:

<SNSC Installation Directory>/conf/auth

3 Open the following file in a text editor: `rootuser.properties`

4 Set `EnableRootUser` to `false`.

5 Start SNSC Service:

On a Linux system, issue the following command:

```
# /opt/ibm/snsc/bin/startup.sh
```

Changing the Default Passwords

The System Networking Switch Center installation program creates three default users. The default user names and passwords are:

- admin/admin
- oper/oper
- user/user

If you are an administrator, you can log in to System Networking Switch Center as each user type and change the default passwords to help improve system security.

- **Administrator**—Only administrators can make permanent changes to the switch that persist after a switch is rebooted. Administrators can access switch functions to configure and troubleshoot problems on the switch.
- **Operator**—Operators have the same capabilities as listed for User plus the ability to reboot switches. Operators cannot change the switch configuration, such as uploading images and configuration files.
- **User**—User interaction with the switch is completely passive; nothing can be changed on the switch. Users can display information that has no security or privacy implications, such as switch statistics and current operational state information.

Changing the Default Administrator Password

- 1 Login to System Networking Switch Center.
- 2 Choose menu **Options > Security Configuration**.
- 3 Click **admin** in the **Modify Password For** list.
- 4 If Admin is mapped to root, enter the Admin password in the Admin Password field or enter the root password in the Root Password field.
- 5 Enter and re-enter the new administrator password.
- 6 Click **Modify**.
- 7 Test the new password:
 - a Click **Logout**.
 - b Enter admin in the User Name field.
 - c Enter the updated administrator password.
 - d Click **Login**.

Changing the Default Operator Password

- 1 Login to System Networking Switch Center.
- 2 Choose menu **Options > Security Configuration**.
- 3 Click **oper** in the **Modify Password For** list.
- 4 If Admin is mapped to root, enter the Admin password in the Admin Password field or enter the root password in the Root Password field.
- 5 Enter and re-enter the new password for operator.
- 6 Click **Modify**.
- 7 Test the new password:
 - a Click **Logout**.
 - b Enter **oper** in the User Name field.
 - c Enter the updated operator password.
 - d Click **Login**.

Changing the Default User Password

- 1 Login to System Networking Switch Center.
- 2 Choose menu **Options > Security Configuration**.
- 3 Click **user** in the **Modify Password For** list.
- 4 If **Admin** is mapped to root, enter the Admin password in the Admin Password field or enter the root password in Root Password field.
- 5 Enter the current administrator password in the Admin Password field.
- 6 Enter and re-enter the new user password.
- 7 Click **Modify**.
- 8 Test the new password:
 - a Click **Logout**.
 - b Enter user in the User Name field.
 - c Enter the updated user password.
 - d Click **Login**.

Changing the Default Root Password

Important: You can only perform this task if the Admin user is not mapped to the root user. See “Enabling and Disabling Root Users” on page 39.

- 1 Log in to System Networking Switch Center.
- 2 Choose menu **Options > Security Configuration**.
- 3 Click **root** in the **Modify Password For** list.
- 4 Enter the root password in the Root Password field.
- 5 Enter and re-enter the new root password.
- 6 Click **Modify**.

How to Discover Switches

System Networking Switch Center has two switch discovery options. You can automatically discover switches via IP address or subnet range. You can also use the manual discovery method to add individual switches.

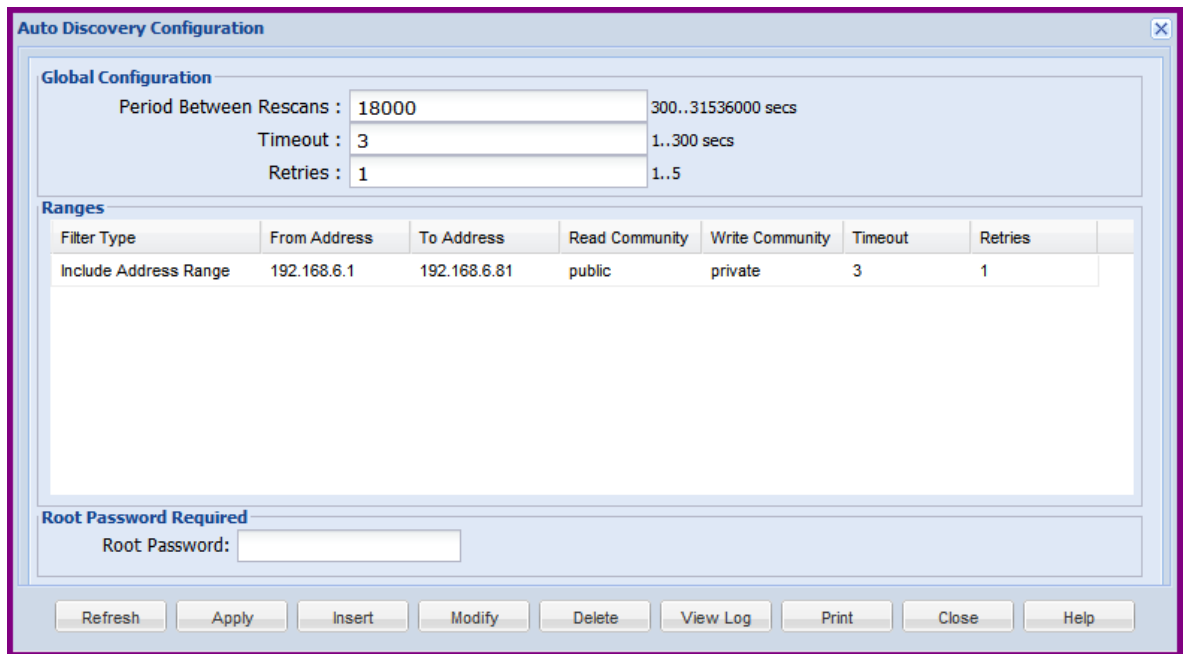
Domain and node configuration and administration is available only to the users login as an administrator (in case, if Root user is disabled) or to those users, who know 'root' password (in case, if Root user is enabled).

- [“Using Auto Discovery” on page 47](#)
- [“Using Manual Discovery” on page 54](#)
- [“Importing Device Lists from a CSV File” on page 56](#)
- [“Exporting a Discovered List of Switches to a CSV File” on page 60](#)
- [“Troubleshooting Switch Import and Discovery Problems” on page 61](#)

Using Auto Discovery

Use this switch discovery process to add more than one switch at a time to the System Networking Switch Center system. The Auto Discovery Configuration window displays the configuration parameters that System Networking Switch Center uses to find switches when you start the Auto Discovery operation. You must configure the switches in either SNMPv1 or SNMPv2 to use the auto-discovery feature.

Choose menu **Options > Discovery > Discovery Configuration** to open the Auto Discovery Configuration window (see [Figure 1 on page 48](#)).

Figure 1 Auto Discovery Configuration Window


The screenshot shows the 'Auto Discovery Configuration' window. It has a title bar with a close button. The window is divided into three main sections: 'Global Configuration', 'Ranges', and 'Root Password Required'. The 'Global Configuration' section contains three rows of settings: 'Period Between Rescans' (18000, 300..31536000 secs), 'Timeout' (3, 1..300 secs), and 'Retries' (1, 1..5). The 'Ranges' section is a table with columns: Filter Type, From Address, To Address, Read Community, Write Community, Timeout, and Retries. It contains one row: 'Include Address Range', '192.168.6.1', '192.168.6.81', 'public', 'private', '3', and '1'. The 'Root Password Required' section has a label and a text input field. At the bottom, there is a row of buttons: Refresh, Apply, Insert, Modify, Delete, View Log, Print, Close, and Help.

Global Configuration						
Period Between Rescans :	18000	300..31536000 secs				
Timeout :	3	1..300 secs				
Retries :	1	1..5				

Ranges						
Filter Type	From Address	To Address	Read Community	Write Community	Timeout	Retries
Include Address Range	192.168.6.1	192.168.6.81	public	private	3	1

Root Password Required

Root Password:

Buttons: Refresh, Apply, Insert, Modify, Delete, View Log, Print, Close, Help

You can perform the following auto discovery configuration tasks:

- Modify global configuration parameters
- Print global configuration and range summary values
- Modify or delete an existing configuration
- Insert a configuration

Table 1 Auto Discovery Configuration field descriptions

Field	Description
Period Between Rescan	The delay, in seconds, after which the Auto-Discovery process is activated to re-scan the configured IP address and subnet ranges. The default value is 18000 seconds (5 hours).
Timeout	<p>The timeout value, in seconds. The timeout value controls how long SNSC waits for a response from a switch during auto-discovery. You can specify a timeout while configuring auto-discovery parameters. If you do not specify a timeout, SNSC uses the global timeout value.</p> <p>Note: This timeout value is applicable to both ICMP and SNMP requests sent during auto discovery.</p>

Table 1 Auto Discovery Configuration field descriptions (continued)

Field	Description
Retries	<p>The number of retries that you want SNSC to attempt during auto-discovery. You can specify the number of retries while configuring auto-discovery parameters. If you do not specify a retry interval, SNSC uses the global retries value.</p> <p>Note: The Retries is applicable only to SNMP requests sent during auto discovery. For ICMP, no retries are attempted.</p>
Filter Type	Lists whether the entry is to be included (Include Address Range) or excluded (Exclude Address Range) while performing discovery operation.
From Address	Starting IP address of the range.
To Address	Ending IP address of the range.
Read Community	SNMP v1/v2c read-community password.
Write Community	SNMP v1/v2c write-community password.
Timeout	The timeout value, in seconds. The timeout value controls how long SNSC waits for a response from a switch during auto-discovery. You can specify a timeout while configuring auto-discovery parameters. If you do not specify a timeout, SNSC uses the global timeout value.
Retries	<p>The number of retries that you want SNSC to attempt during auto-discovery. You can specify the number of retries while configuring auto-discovery parameters. If you do not specify a retry interval, SNSC uses the global retries value.</p>
Root Password	<p>Allows you to enter the root password. When the 'Root' user is enabled, the discovery configuration window can be launched by all users. However, the operations are allowed only when user enters the valid Root password.</p> <p>Note: This field is visible only when Root user is enabled.</p>

Auto Discovering Switches in a Subnet Range

You can configure System Networking Switch Center to automatically discover switches by searching for a specified subnet or subnet mask range.

- 1 Choose menu **Options > Discovery > Discovery Configuration**.
- 2 If Root user is enabled, enter the root password.
- 3 Click **Insert**.
- 4 Select **Include Address Range - Subnet** from the Filter Type list (see [Figure 2 on page 50](#)).

- 5 Enter the subnet information in the Subnet and Subnet Mask fields.
- 6 If required, change the default community strings entered in the Read Community and Write Community fields. The default strings are public and private respectively. These settings apply to SNMP version 1 or 2 access.
- 7 (Optional) Enter a subnet range to exclude from the Auto Discovery process.
 - a Click **Insert**. The Auto Discovery dialog box reopens.
 - b Select **Exclude Address Range - Subnet** from the Filter Type list.
 - c Enter the subnet information to exclude in the Subnet and Subnet Mask fields.
 - d Click **Insert**. The Exclude Address Range appears in the Auto Discovery Configuration window.
- 8 Click **Insert**.
- 9 Click **OK** to close the Auto Discovery information message. System Networking Switch Center begins to discover switches according to the values you defined for the subnets and masks.

Click **Close** to close the Auto Discovery Configuration window. Choose menu **Logs > Auto Discovery Log** to view the status of the Auto Discovery process.

Figure 2 Auto-Discovery Configuration by Subnet Range Window

See also:

- [“Auto Discovering Switches by IP Address” on page 52](#)
- [“Using Manual Discovery” on page 54](#)

- [“Troubleshooting Switch Import and Discovery Problems” on page 61](#)
- [“How to View Logs” on page 134](#)

Auto Discovering Switches by IP Address

You can only use this feature for switches that are configured in SNMPv1 or SNMPv2.

- 1 Choose menu **Options > Discovery > Discovery Configuration**.
- 2 If Root user is enabled, enter the root password.
- 3 Click **Insert**.
- 4 Select **Include Address Range - IP address range** from the Filter Type list (see [Figure 3 on page 53](#)).
- 5 Enter the IP address range in the *From* and *To* fields.
- 6 Type the appropriate community strings in the Read Community and Write Community fields. The default strings are public and private, respectively. These settings apply to SNMP version 1 or 2 access.
- 7 Click **Insert**.
- 8 (Optional) Enter an IP address range to exclude from the Auto Discovery process.
 - a Click **Insert**.
 - b Select **Exclude Address Range - IP Address Range** from the Filter Type list.
 - c Enter the IP address range to exclude in the *From* and *To* fields.
 - d Click **Insert**. The Exclude Address Range appears in the Auto Discovery Configuration window.
- 9 Click **Insert**.
- 10 Click **OK** to close the Auto Discovery information message.

System Networking Switch Center begins to discover switches according to the values you defined for the IP address range.

Click **Close** to close the Auto Discovery Configuration window. Choose menu **Logs > Auto Discovery Log** to view the status of the Auto Discovery process.

After the System Networking Switch Center service starts, the Auto Discovery program attempts discovery on all of the ranges that you entered. This is the only time when all ranges are discovered.

After you enter a new range, that range, and only that range, is discovered.

Figure 3 Auto-discovery Configuration by IP Address Range Window

Auto Discovery Configuration - Insert

Filter Type: Include Address Range - IP address range

Subnet: 0.0.0.0

Subnet Mask: 255.255.255.255

From: 0.0.0.0

To: 0.0.0.0

Read Community: *****

Write Community: *****

Timeout: 3

Retries: 1

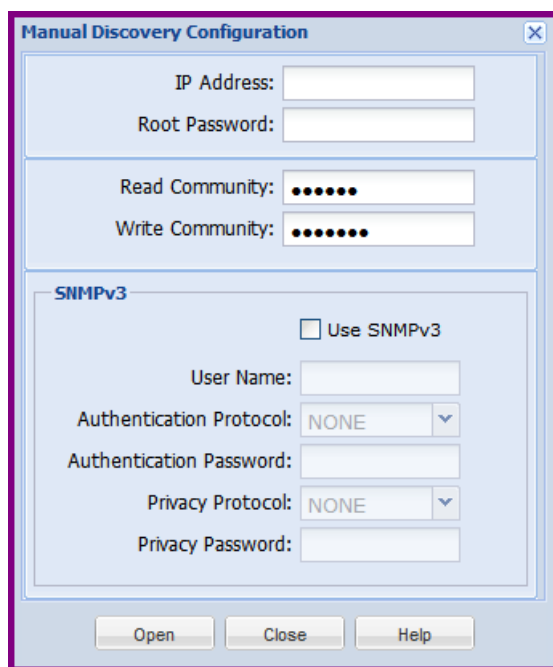
Insert

Close

Using Manual Discovery

Use this switch discovery process to add one switch at a time to the System Networking Switch Center system.

- 1 Perform the manual discovery using one of the following steps:
 - a Click **Add Device** in Summary Page or Main Page. This operation results in adding the newly discovered device under the Root node in the navigation tree.
 - b In Main Page, right-click **Root** or a domain name in the left pane and click **Add Device**.
- 2 Type the IP address of the switch that you want to discover in the IP Address field (see [Figure 4 on page 55](#)).
- 3 If Root user is enabled, enter the root password in Root Password field (this field is not visible if Root user is disabled).
- 4 If you are discovering the switch configured with SNMPv1 or SNMPv2c:
 - a Enter the correct read and write community strings in Read Community and Write Community fields respectively.
 - b Click **Open**. System Networking Switch Center begins the switch discovery process.
- 5 To discover a switch that is configured as SNMPv3:
 - a Click **Use SNMPv3**.
 - b Enter the user name in User Name field.
 - c If Authentication is enabled on the switch (switch is configured in AuthNoPriv or AuthPriv), select the authentication protocol (**MD5** or **SHA1**) from Authentication Protocol list and enter the authentication password in Authentication Password field.
 - d If Privacy is enabled on the switch (switch is configured in AuthPriv), select **DES** in the Privacy Protocol list and enter the privacy password in the Privacy Password field.
 - e Click **Open**. System Networking Switch Center begins the switch discovery process.

Figure 4 Manual Discovery Configuration Window

The image shows a 'Manual Discovery Configuration' dialog box with a light blue background and a purple border. It contains several input fields and a section for SNMPv3 configuration.

Manual Discovery Configuration [X]

IP Address:

Root Password:

Read Community:

Write Community:

SNMPv3

☐ Use SNMPv3

User Name:

Authentication Protocol: ▼

Authentication Password:

Privacy Protocol: ▼

Privacy Password:

Open Close Help

Importing Device Lists from a CSV File

System Networking Switch Center's auto-discovery mechanism uses ICMP and SNMP to discover the devices. If you don't want to use auto-discovery or don't want to allow ICMP, then you can import the devices from a CSV (comma separated value) list. Importing the devices from the list saves precious time as you don't have to individually discover each devices using Manual Discovery option.

Note: The Import Device List window can import only devices that are Up and can be manually discovered by System Networking Switch Center.

The following sections show the Device List CSV file format along with some samples:

File Format:

```
<each row> ::= <Device Address>[,<SNMP Data>]

<Device Address> ::= <IP Address> | <IP Address Range>
<SNMP Data> ::= [<Timeout>], [<Retries>], <SNMP Params>
<SNMP Params> ::= <SNMP Version>, { <SNMP v1/v2c Data> | <SNMP v3 Data> }
<SNMP Version> ::= v1 | v2c | v3
<SNMP v1/v2c Data> ::= <Read Community>, <Write Community>
<Read Community> ::= <Plain Text> | <Encrypted Text>
<Write Community> ::= <Plain Text> | <Encrypted Text>
<SNMP v3 data> ::= <User Name>,[<Authentication Info>, <Privacy Info>]
<Authentication Info> ::= { MD5 | SHA }, <Password>
<Privacy Info> ::= DES, <Password>
<Password> ::= <Plain Text> | <Encrypted Text>
```

As we can see in the file format, the Device Address is mandatory and the SNMP Data information is optional. You can specify SNMP Data during import and this information is utilized as below:

- If the row contains SNMP data, then it is used instead of the data specified during import.
- If the row doesn't contain SNMP data, then the information supplied during import is used.

Note: You can only specify Community Strings and Passwords in plain-text. When System Networking Switch Center exports the device list, it saves the Community Strings and Passwords in encrypted form, which can only be deciphered by System Networking Switch Center.

File Samples:***No SNMP Data:***

```
192.168.1.10
192.168.1.20-192.168.1.24
192.168.20.100
...
```

With SNMPv1/v2 Data with plain-text community strings:

```
192.168.1.10,3,1,v1,public,private
192.168.1.20-192.168.1.24,5,2,v2c,public1,private1
192.168.20.100,3,1,v1,public2,private2
...
```

With SNMPv3 Data with plain-text passwords:

```
192.168.1.10,3,1,v3,bnt1 # NO_AUTH_NO_PRIV
192.168.1.20-192.168.1.24,5,1,v3,bnt2,MD5,adminmd5 # AUTH_NO_PRIV
192.168.20.100,3,1,v3,bnt3,SHA,adminsha,DES,adminde # AUTH_PRIV
```

Importing the Device List

Choose menu **Discovery > Import Device List** to open the Import Device List window (see [Figure 5 on page 58](#)). To import the device list, perform the following steps:

- 1** Click **Browse...** and select the CSV file containing the import list.

If Root user is enabled, enter the correct root password in Root Password field (this field is not visible, in case, if Root user is disabled).

If one or more rows in the CSV file doesn't contain SNMP Data, you can specify the information by checking Specify Other Information check box and following the additional steps given below:

- a** Select **SNMP Version**.
- b** Enter the timeout value in seconds in Timeout field.
- c** Enter the retries in Retries field.
- d** If SNMP v1 or v2c is selected, Enter appropriate community strings in Read Community and Write Community fields.
- e** If SNMP v3 is selected:
 - Enter user name in User Name field.
 - Select the authentication protocol from Authentication Protocol list.

If authentication protocol is not set to NONE, enter the authentication password in Authentication Password field.

Select the privacy protocol from Privacy Protocol list.

If privacy protocol is not set to NONE, enter the privacy password in Privacy Password field.

- 2 Click **Import** to import the list.

Figure 5 Import Device List Window

Discovery List - Import

IP Address Ranges File:

Root Password:

☐ Specify Other Information

General

SNMP Version:

Timeout: 1..300

Retries: 1..5

SNMPv1/2c

Read Community:

Write Community:

SNMPv3

User Name:

Authentication Protocol:

Authentication Password:

Privacy Protocol:

Privacy Password:

Table 2 Import Device List field descriptions

Field	Description
IP Address Ranges File	The CSV file containing the list of IP addresses of the switches to be discovered.
Root Password	The root password field. This field is visible if Root user is enabled.
Specify Other Information	Enables or disables SNMP specific fields.
SNMP Version	The SNMP version to use for those entries in CSV file that doesn't contain SNMP data.
Timeout	The timeout in seconds to use for those entries in CSV file that doesn't contain SNMP data. The range is 1 to 300 seconds.
Retries	The number of retries to use for those entries in CSV file that doesn't contain SNMP data. The range is 1 to 5.
Read Community	The Read Community to use for those entries in CSV file that doesn't contain SNMP data. This field is enabled only when SNMPv1 or SNMPv2c is selected in SNMP Version.
Write Community	The Write Community to use for those entries in CSV file that doesn't contain SNMP data. This field is enabled only when SNMPv1 or SNMPv2c is selected in SNMP Version.
User Name	The user name to use for those entries in CSV file that doesn't contain SNMP data. This field is enabled only when SNMPv3 is selected in SNMP Version.
Authentication Protocol	The authentication protocol to use for those entries in CSV file that doesn't contain SNMP data. This field is enabled only when SNMPv3 is selected in SNMP Version.
Authentication Password	The authentication password to use for those entries in CSV file that doesn't contain SNMP data. This field is enabled only when Authentication Protocol is set to MD5 or SHA1.
Privacy Protocol	The privacy protocol to use for those entries in CSV file that doesn't contain SNMP data. This field is enabled only Authentication Protocol is set to MD5 or SHA1.
Privacy Password	The privacy password to use for those entries in CSV file that doesn't contain SNMP data. This field is enabled only Privacy Protocol is set to DES.

Exporting a Discovered List of Switches to a CSV File

You can export the discovered switches along with SNMP data to a CSV file. You can import the CSV file into System Networking Switch Center (see [“Importing Device Lists from a CSV File” on page 56](#)). To export the discovered switches:

- 1** Choose menu **Discovery > Export Device List**.
- 2** In the resulting dialog, select “Save File” option and click **OK**.
- 3** In the resulting file browser window, select the file, in which the contents to be saved.

Note 1: While exporting the data, System Networking Switch Center encrypts the Community Strings (in case of SNMPv1 or SNMPv2c) and Passwords (in case of SNMPv3). This can be decrypted only by System Networking Switch Center during import.

Note 2: If SNMP data is not completely available, the associated SNMP data field is blank.

Troubleshooting Switch Import and Discovery Problems

Check the following items if System Networking Switch Center displays an error message during switch discovery.

- In slower networks, increase the **Retry Count** and **Timeout** values on the Auto Discovery Configuration window. See [Table 1 on page 48](#) for more information.
- In the **Open Device** window, ensure that the correct read and write community strings have been entered for SNMP version 1 and 2 connections.
- In the **Open Device** window, ensure that the correct SNMP version 3 information has been entered for SNMP version 3 connections.
- Ensure that the switch is physically connected to the network.
- Ensure that the switch is turned on and receiving power.
- Ensure that the switch has been assigned a correct IP address.
- Verify that you entered the correct IP address is being used in the **Open Device** window.
- Ensure that the problem does not exist because of an unrelated network misconfiguration.
- Ensure that SNMP access is enabled on the switch. See the *User Guide* for the selected switch for information about how to enable SNMP access.
- Ensure that the switch is not blocking access from the client IP address.
- After the System Networking Switch Center service starts, auto discovery attempts to discover switches using all of the ranges you entered. This is the only time when all ranges are discovered.
- After you enter a new range, that range, and only that range, is discovered.

See also:

[“How to Discover Switches” on page 47](#)

About the System Networking Switch Center User Interface

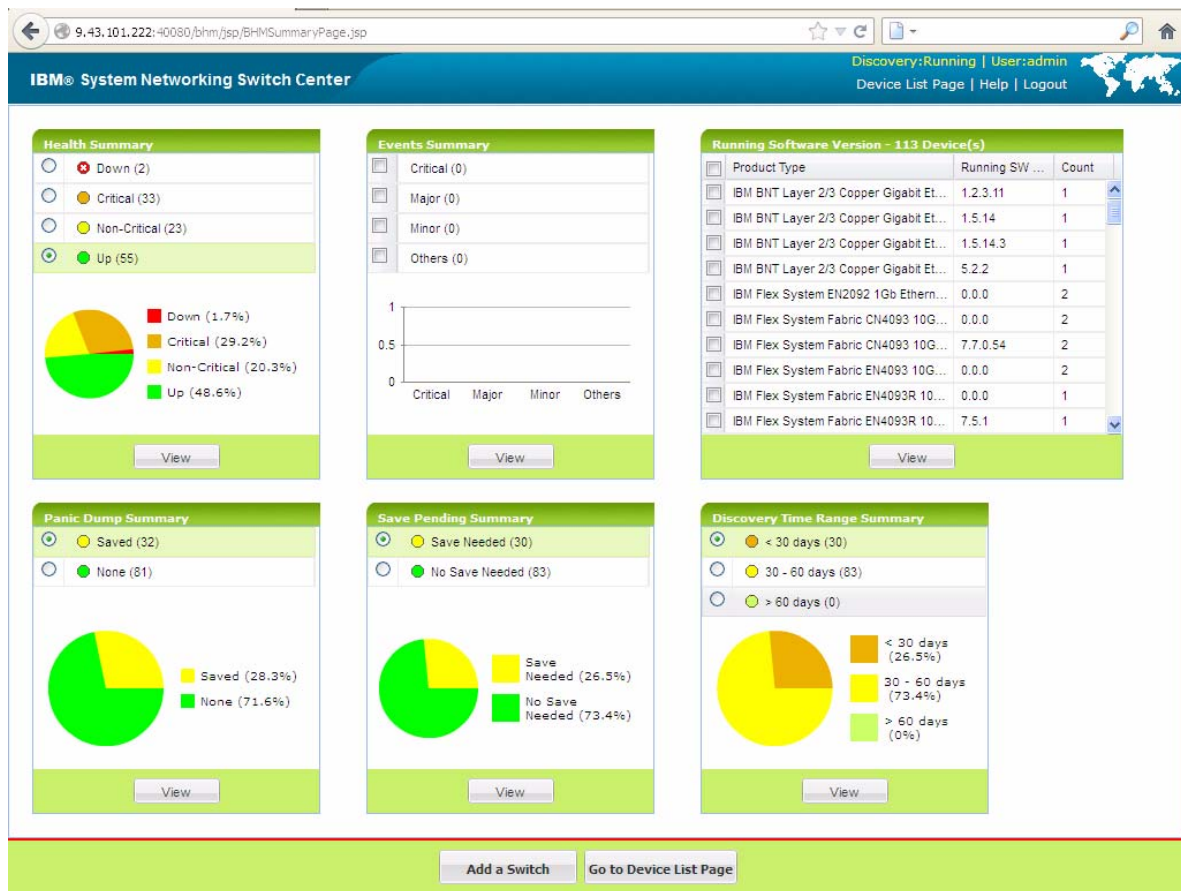
The following topics are discussed in this section:

- [“About the Home Page” on page 63](#)
- [“The Device List Pane” on page 74](#)
- [“The Domains Pane” on page 72](#)
- [“The Summary Status Pane” on page 73](#)
- [“The Device List Pane” on page 74](#)
- [“Device List Page – Menu Bar” on page 76](#)
- [“Device Menu” on page 77](#)
- [“Group Operations Menu” on page 78](#)
- [“Reports Menu” on page 80](#)
- [“Logs Menu” on page 81](#)
- [“Options Menu” on page 82](#)
- [“Help Menu” on page 86](#)
- [“About the Device Console Page” on page 87](#)
- [“Changing IBM System Networking Switch Center Configuration” on page 100](#)
- [“Changing the Default Refresh Configuration Parameters” on page 103](#)
- [“Changing the Default Data Collection Configuration Parameters” on page 104](#)
- [“Changing the Default DB Data Purge Configuration Parameters” on page 106](#)
- [“Configuring Authentication” on page 108](#)
- [“Configuring FTP/SFTP/TFTP Server Parameters” on page 114](#)

About the Home Page

The System Networking Switch Center home page gives a quick summary of the devices discovered. It provides a graphical representation of Health Status, Panic Dump, Save Pending, Running Software Version and Device Discovery Timestamp, grouped into separate panels along with the device counts. (See [Figure 6 on page 63](#)). The information is updated periodically to give the actual counts and status of managed devices. It provides an option for the user to filter the devices available on the device list page based on the selection made here. Click **Add a Switch** to directly perform a manual discovery of switches for the SNSC system. The **Go to Device List Page** option lists all the devices discovered and does not perform any filtering.

Figure 6 System Networking Switch Center Manager Home Page Example



Health Status Summary Pane

The Health Status pane shows the individual count of devices discovered that are Down (red), Critical (orange), Non-Critical (yellow) and Up (green). It also provides a pie chart that indicates the percentages of Down/Critical/Non-Critical/Up devices (See [Figure 7 on page 65](#)). You can filter out the devices depending on the Health Status by selecting the appropriate choice and clicking View, which takes you to the Device list page (See [Figure 8 on page 65](#)).

You can clear the selection any time by clicking on top of the device list to reset the filter and see the complete list of devices discovered.

Figure 7 Health Summary Pane

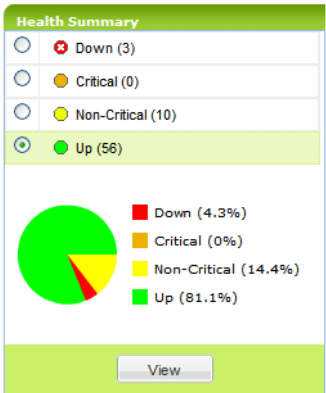
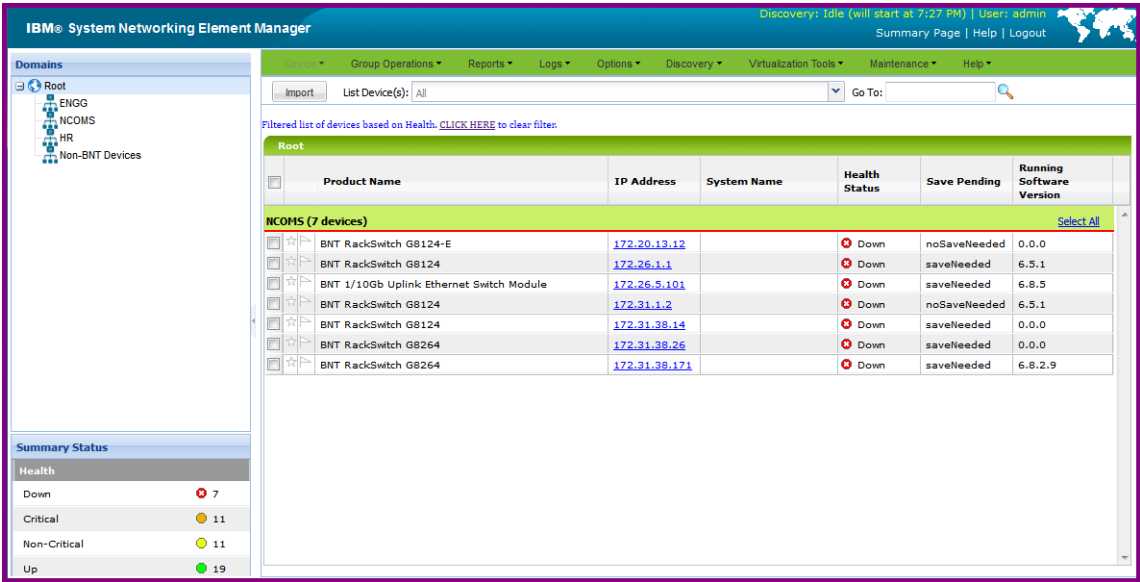


Figure 8 Filtered Device List Based on Health Status



Note: System Networking Switch Center shows Critical and Non-Critical status for RackSwitches and IBM BladeCenter switches.

For RackSwitches, System Networking Switch Center directly gets the status information that indicates one or more of the following conditions:

- Critical:
 - One or more temperature sensors are in the failure range (e.g. ≥ 100 C).

- Fan Modules/Fans are not working properly, as follows:
 - BNT RackSwitch G8000, BNT RackSwitch G8100, BNT RackSwitch G8124/G8124-E: One or more fans are running at less than or equal to 500 RPM
 - BNT RackSwitch G8052: Fewer than 3 Fan Modules are in good state. A Fan Module is considered good if fans in that module are running at more than 500 RPM
 - BNT RackSwitch G8264: Fewer than 4 Fan Modules are in good state. A Fan Module is considered good if fans in that module are running at more than 500 RPM
- One power supply is off.
- Non-Critical:
 - One or more temperature sensors are in the warning range (e.g. ≥ 85 and < 100 C).
 - A panic dump exists in flash.

For IBM BladeCenter switches, System Networking Switch Center assigns the status by combining the status of the following discreet variables on those switches:

- Critical:
 - One or more temperature sensors are in the failure range.
- Non-Critical:
 - One or more temperature sensors are in the warning range.
 - A panic dump exists in flash.

Panic Dump Summary Pane

The Panic Dump Summary shows the count of discovered devices based on their panic-dump status, as follows:

- Devices that have a panic dump saved (yellow)
- Devices with no panic dump (green)

It also provides a pie chart that indicates the panic-dump status of all devices. Click **View** to filter devices based on the status of their panic dumps.

Save Pending Summary Pane

The Save Pending Summary shows the count of discovered devices based on their save status, as follows:

- Devices that have configuration saved (No Save Needed)
- Devices that do not have configuration (Save Needed)

It also provides a pie chart that indicates the saved status of all devices. Click **View** to filter devices based on their saved status.

Discovery Time Range Summary Pane

The Discovery Time Range Summary shows the count of discovered devices based on duration of discovery (the number of days elapsed since their discovery in System Networking Switch Center). This Summary Pane also provides a pie chart that indicates the number of devices discovered in the given time range. Click **View** to filter devices based on their discovery date.

Running Software Version Summary Pane

The Running Software Version Summary categorizes the devices discovered by product type and running software version. You can filter the devices by product type and version by selecting one or more product types and clicking **View**.

About the Device List Page

The System Networking Switch Center Device List page consists of three framed windows with menu and filter bars. The left-hand frame has two sub-panes – Domains and Summary Status. The right-hand or center frame consists of a menu bar, filter bar, and the Device List pane.

The Domains Pane

The Domains pane displays the list of domains. By default, Switch Center is shipped with two domains:

- Root
- Non-BNT Devices

When the discovery information is imported from Tivoli Network Manager, the domains are created under Root and these domains maps to the Network Domains in Tivoli Network Manager.

The newly discovered devices imported from a CSV file are placed under Root domain.

The Non-BNT Devices domain serves as a place holder for listing non supported devices.

The Summary Status Pane

The Summary Status window displays information about the health status for all discovered switches.. The data in the Summary Status window is refreshed automatically.

The Summary Status Health column displays the count of discovered devices that are Up, Down, Critical and Non-Critical. If System Networking Switch Center is able to send and receive SNMP messages to a device, the switch health is set as Up or else, the status is set as Down. For RackSwitches and IBM BladeCenter specific switches, System Networking Switch Center can show additional status information (Critical and Non-Critical).

The Device List Pane

The Device List content pane displays the list of all the devices discovered in System Networking Switch Center.

By default, the device list shows Product Name along with Favorite Icon and Notes flag, IP Address, System Name, Health Status, Save Pending and Running Software Version fields, while other fields such as Config For Next Reset, Discovery Date, MAC address, Location, Rack, Chassis, Module Bay, and Domain are hidden. You can enable System Networking Switch Center to either show or hide any column by clicking the right corner of any column, then selecting Columns and then checking or clearing one or more columns to show or hide them.

The Health Status column shows the status as a combination of colored icon with appropriate text for better readability (see [Figure 9 on page 74](#)).

Figure 9 Device List Showing Health Status

Root						
	Product Name	IP Address	System Name	Health Status	Save Pending	Running Software Version
Root (57 devices) Select All						
	BNT/Nortel Layer 2-3 Giga	172.25.160.3		Up	saveNeeded	5.1.3
	BNT RackSwitch G8000	172.25.160.90		Critical	saveNeeded	6.5.1
	BNT/Nortel 1/10Gb Uplink	192.168.6.75		Down	noSaveNeeded	0.0.0
	BNT RackSwitch G8100	192.168.130.11		Non-Critical	saveSuccessful	1.0.7.0
	BNT RackSwitch G8100	192.168.130.31		Up	saveSuccessful	1.0.7.0

Stacked Switches

For easy recognition, the Device List displays stacked switches in a slightly different manner (see [Figure 10 on page 75](#)):

- The switches in the stack are grouped together in the device list with the same IP Address.
- The master switch shows the Product Name, whereas the other switches in the stack do not show this field. This distinction makes it easier to recognize the stack of switches.
- The health status of stacked switches (except the master switch) will show as either `inStack` or `detached`.

Figure 10 Device List Showing Stacked Switches

Root						
	Product Name	IP Address	System Name	Health Status	Save Pending	Running Software Version
Marketing (10 devices) Select All						
<input type="checkbox"/>	BNT 10-port 10Gb Etherne	192.168.141.11		● Up	noSaveNeeded	5.0.1.0
<input type="checkbox"/>	BNT 10-port 10Gb Etherne	192.168.141.31		● Up	noSaveNeeded	5.0.1.0
<input type="checkbox"/>	BNT 10-port 10Gb Etherne	192.168.141.51		● Up	noSaveNeeded	6.3.1.0
<input type="checkbox"/>	BNT 10-port 10Gb Etherne	192.168.141.61		● Up	noSaveNeeded	6.3.1.0
<input type="checkbox"/>		192.168.141.61		○ inStack		
<input type="checkbox"/>		192.168.141.61		○ inStack		
<input type="checkbox"/>		192.168.141.61		○ inStack		
<input type="checkbox"/>		192.168.141.61		○ inStack		
<input type="checkbox"/>		192.168.141.61		○ inStack		

Device List Page – Menu Bar

The menu bar of the Device List page provides the global commands that can be invoked either on an individual device or a group of devices. The following table describes the main menu bar items.

Table 3 Device List Page — Menu Bar Items

Menu	Description
Device	This menu item is enabled only for individual device selection and provides commands for opening Monitor, Configure pages and for performing actions.
Group Operations	Provides commands associated with firmware and configuration deployment, reports and actions that can be invoked on an individual or a group of devices.
Reports	Displays various reports such as Events, Syslog, Alerts, Switch Version Report, VMready VM report associated with all the discovered devices.
Logs	Displays various log windows showing the messages logged by SNSC.
Options	Provides various windows to assist configuring SNSC properties.
Discovery	Provides various windows to assist Device Import operations from Tivoli Network Manager and CSV file.
Virtualization Tools	Provides the options for launching virtualization tools: VSI DB Console and VMready Across the Datacenter wizard.
Maintenance	Provides commands associated with SNSC maintenance operations such as Purging DB configuration, Log file configuration, Backing up critical data and creating Tech Support Dump.
Help	Provides commands for accessing online help and support options for SNSC.

Device Menu

The following table describes the Device List page **Device** menu commands:

Table 4 Device List Page — Device Menu

Sub-menu	Description
Monitor	This menu launches Device Console showing Monitor frame. The Monitor frame consists of multiple panels displaying various switch data and statistical information.
Configure	This menu is enabled only for few supported devices. When activated, it shows Device Console's configuration frame enabling privileged user to set various device parameters.
Sync Config	Opens the Sync Config frame that can be used for synchronizing switch configuration such as VLAN and Ports for other switches.
Set Discovery Date	Opens the Set Discovery Date dialog that can be used for manually setting the discovery date for the selected device/switch.
Change SNMP Parameters	Opens the Modify Discovery Parameters dialog that can be used for changing the SNMP parameters used by SNSC for managing the selected device/switch.
Actions	<p>Provides a set of actions commands that can be invoked on the selected device. The following lists various commands:</p> <ul style="list-style-type: none"> • <i>Apply</i> - Applies any changes that you have made to the switch configuration. • <i>Save</i> - Saves the current configuration to the flash memory. • <i>Diff Config</i> - Opens a window to display any pending configuration changes. • <i>Diff Flash</i> - Opens a window to display any pending configuration changes and the affected configuration stored in flash memory on the switch. • <i>Config Dump</i> - Opens a window to display a dump of the current switch configuration. • <i>Syslog Dump</i> – Opens a window to display the syslogs available on the switch. • <i>Revert</i> - Reverts the switch to the current active configuration. This command is available if you did not apply the new configuration settings. • <i>Revert Apply</i> - Reverts the switch to the current saved configuration. This is available if you applied but did not save the new configuration settings. • <i>Reboot Switch</i> - Reboots the switch by reloads and saving the current RAM memory. • <i>Delete</i> – Deletes the switch entry from SNSC device list.
Launch	Provides the commands for launching Browser Based Interface (Web) and SSH/Telnet application (Console).

Group Operations Menu

The following table describes the Device List page **Group Operations** menu commands:

Table 5 Device List Page — Group Operations Menu

Sub-menu	Description
CLI Push	Opens a text window enabling the user to type-in CLI commands that can be invoked on the selected switch(es).
Collect Data From Device	Refreshes the device data by retrieving the information from the selected switch(es).
Switch Version Report	Displays the switch version report associated with the selected switch(es).
Transceiver Information Report	Displays the transceiver information report associated with the selected switch(es). Note: Transceiver Information is available only for those switches supporting 10G ports.
VM Data Center Report	Displays the VM Data Center report associated with VMready switches in the selected list of switch(es).
Set Discovery Date	Opens the Set Discovery Date dialog that can be used for manually setting the discovery date for the selected device(s)/switch(es).
Deployment	Provides a set of commands for performing various operations related to firmware and configuration deployment on the selected switch(es): <ul style="list-style-type: none"> • <i>Image Upgrade</i> – Uploads the selected firmware from the given FTP/SFTP/TFTP server on to the selected switch(es). • <i>Image Backup</i> – Backs up the firmware from the selected switch(es) and stores them on the given FTP/SFTP/TFTP server. • <i>Configuration Upgrade</i> – Uploads the selected configuration file from the given FTP/SFTP/TFTP server on to the selected switch(es). • <i>Configuration Backup</i> - Backs up the configuration from the selected switch(es) and stores them on the given FTP/SFTP/TFTP server. • <i>Panic Dump</i> – Downloads the panic dump from the selected switch(es) and stores them on the given FTP/SFTP/TFTP server. • <i>Tech Support Dump</i> – Generates the tech support dump on the selected switch(es) and stores them on the given FTP/SFTP/TFTP server. • <i>Scheduled Jobs</i> – Displays the window for viewing and cancelling the scheduled jobs.

Table 5 Device List Page — Group Operations Menu

Sub-menu	Description
Group Actions	<p>Provides a set of actions commands that can be invoked on the selected switch(es). The following lists various commands:</p> <ul style="list-style-type: none">• <i>Apply</i> - Applies any changes that you have made to the switch configuration of the selected switch(es).• <i>Save</i> - Saves the current configuration to the flash memory on the selected switch(es).• <i>Reboot Switch</i> - Reboots the selected switch(es).• <i>Delete</i> – Deletes the selected switch entry/entries from SNSC device list.
Notes	<p>Provides a set of commands associated with adding or removing notes as given below:</p> <ul style="list-style-type: none">• <i>Add</i> – Opens up Notes dialog that can be used for adding notes for the selected device(s)/switch(es).• <i>Remove</i> – Removes the notes, if present, for the selected device(s)/switch(es).

Reports Menu

The following table describes the Device List page **Reports** menu commands:

Table 6 Device List Page — Reports Menu

Sub-menu	Description
SNSC Alerts	Displays the list of alerts generated by SNSC.
Switch Version Report	Displays the switch version report of the switches.
Transceiver Information Report	Displays the transceiver information report associated with those switches supporting 10G ports.
VM Data Center Report	Displays the VM Data Center report associated with VMready switches.
VMready VM Report	Provides the following VM reports: <ul style="list-style-type: none">• <i>Port Groups</i> – Port Groups memberships that are configured on the discovered VMready switches.• <i>VM Groups</i> – Virtual Machine Groups memberships that are configured on the discovered VMready switches.

Logs Menu

The following table describes the Device List page **Logs** menu commands:

Table 7 Device List Page — Logs Menu

Sub-menu	Description
Discovery Import Log	Opens the log window showing the messages logged while importing the discovery information from Tivoli Network Manager.
Concurrent Backup Log	Opens the log window showing the messages logged by while performing firmware or configuration backup operation.
Concurrent Download Log	Opens the log window showing the messages logged by while performing firmware or configuration download operation.
Concurrent Reset Log	Opens the log window showing the messages logged by while performing switch reboot (reset) operation.
Scheduled Backup Log	Opens the log window showing the messages logged by while performing firmware or configuration backup operation at a scheduled time.
Scheduled Download Log	Opens the log window showing the messages logged by while performing firmware or configuration download operation at a scheduled time.
Scheduled Reset Log	Opens the log window showing the messages logged by while performing switch reboot (reset) operation at a scheduled time.
CLI Push Log	Opens the log window showing the messages logged while performing CLI push operation.
DB Log	Opens the log window showing the messages logged while performing Database operation.
CMI Log	Opens the log window showing the messages logged while communicating with the switches.
VSI DB RESTful Access Log	Opens the log window showing the messages logged by while processing access to VSI DB from REST clients.
Authentication Log	Opens the log window showing the messages logged while performing user authentication.
Sync Config Log	Opens the log window showing the messages logged while performing sync config operation.
VM Server Log	Opens the log window showing the messages logged while communicating with Virtual Machine Management Server.
VMready Deployment	Contains the following logs: <ul style="list-style-type: none"> • VMready Across Datacenter <ul style="list-style-type: none"> - VMAP: Displays VMAPs deployed to the switches from the VMready Across the Datacenter Wizard. - VMready: Displays VMready configuration deployment to the various switches from the VMready Across the Datacenter Wizard.

Options Menu

The following table describes the Device List page **Options** menu commands:

Table 8 Device List Page — Options Menu

Sub-menu	Description
General Properties	Opens up the properties window where you can set the values such as Concurrent Limit, Session Timeout and Temperature format.
Refresh Configuration	Opens the properties window where you can set the refresh interval.
Security Configuration	Opens the properties window where you can set the user password.
Data Collection Configuration	Opens the properties window where you can set the polling interval for health check and performance statistics collector.
Authentication Configuration	Opens the properties window where you can set the authentication mechanism and the associated properties.
FTP/SFTP/TFTP Configuration	Opens the properties window where you can set the IP address and login credentials (FTP only) to use for accessing FTP, TFTP, or SFTP server.
Discovery Time Range Configuration	Opens the Discovery Time Range Configuration window, which allows you to set the time range in number of days.
Local Console Configuration	Opens the Set Console Application Path window, which allows you to set the path and parameters of the local console application that you want to use for opening up SSH or Telnet based CLI session with the switch.
VM Manager Server Connector	<i>Configuration</i> – Opens up the configuration window where you can manage VM Manager Server credentials
Dial Home	Provides Commands for configuring Dial Home: <ul style="list-style-type: none"> • <i>Email Configuration</i> – Opens a configuration window where you can configure Mail Server parameters and add the list of email addresses for Dial Home operation. • <i>Traps Configuration</i> – Opens a configuration window where you can add or remove a list of SNMP traps for Dial Home operation. • <i>Health Status Configuration</i> – Opens a configuration window where you can add or remove a list of health status messages for Dial Home operation.

Discovery Menu

The following table describes the Device List page Discovery menu commands:

Table 9 Device List Page — Discovery Menu

Sub-menu	Description
Discovery Configuration	<p>Opens the discovery configuration window, where you can view/edit the following parameters:</p> <ul style="list-style-type: none">• Period Between Rescans – The delay, in seconds, after which SNSC's automatic device import process is activated to import the discovery data from Tivoli Network Manager.• Timeout – The timeout value, in seconds, used while performing the data gathering operation during device discovery.• Retries – The number of retries used while performing the data gathering operation during device discovery.
Import Device List	Imports the devices from a CSV file and starts discovering them.
Export Device List	Allows you to export the discovered devices to a CSV file.

Virtualization Tools Menu

The following table describes the Device List page Virtualization Tools menu commands:

Table 10 Device List Page — Virtualization Tools Menu

Sub-menu	Description
VSI DB Console	Opens the VSI Console window for configuring ACL and VSI types, so that SNSC can be used as the centralized VSI DB manager.
VMready Across Datacenter	Opens the wizard for configuring VMready features across all supported switches.

Maintenance Menu

The following table describes the Device List page Maintenance menu commands:

Table 11 Device List Page — Maintenance Menu

Sub-menu	Description
DB Data Purge Configuration	Opens the properties window where you can set the database purge interval.
Log File Configuration	Opens the properties window where you can set the log file size and backup count.
SNSC Support Dump	Opens the support dump dialog that can be used for saving tech support dump data on the browser system for debugging.
Data Backup	<div>Provides commands for taking the backup of SNSC's critical data.</div> <ul style="list-style-type: none">• Take Data Backup – Backs up SNSC's critical data and stores the backup data in the configured directory.• Set Data Backup Directory – Opens the window where you can set the directory on SNSC server to use for keeping the backup data.

Help Menu

The following table describes the Device List page **Help** menu commands:

Table 12 Device List Page — Help Menu

Sub-menu	Description
Help Contents	Opens the context specific online Help page.
IBM Systems Networking	Takes you to IBM Systems Networking page in a separate window.
About IBM System Networking Switch Center	Opens a dialog box that shows the version, license details and the list of supported switches.

About the Device Console Page

The Device Console page (see [Figure 11 on page 88](#)) enables you to view various monitoring pages associated with device parameters and statistics data. This page also allows you to configure device parameters for which configuration management is supported.

You can open the device console page using one of the below approaches:

- In the Device List content pane, click the IP Address hyper-link.
- Enter the IP Address of the device in "Go To" field and click **Search** icon (Magnifying Glass).
- Select the switch and click either menu **Devices > Monitor** or **Devices > Configure**.

The Device Console page consists of three framed windows with menu bars. The top frame shows the device information. The left-hand frame shows the feature tabs (Monitor and Configure) and a tree listing the supported features. The right-hand frame consists of menu bar, sub-feature tabs and the content pane showing the data associated with the selected tab.

Figure 11 IBM System Networking Switch Center – Device Console Page

The screenshot shows the IBM System Networking Switch Center Device Console page for a BNT RackSwitch G8124. The interface includes a top header with tabs, a left sidebar with a feature tree, and a main content area with sub-feature tabs and a data table.

Annotations:

- Tabs:** Points to the top header area containing "Monitor" and "Configure" tabs.
- Device Title:** Points to the header area displaying "192.168.130.81 BNT RackSwitch G8124".
- Global Menu Bar:** Points to the "Actions" and "Help" dropdown menus.
- Sub-feature Tabs:** Points to the tabs "Health Status", "Information", "Port Status", "Port Summary", "Events", and "Syslog".
- Save Status:** Points to the "No Save Needed" status indicator.
- Features:** Points to the left sidebar tree structure.
- Panel Menu Bar:** Points to the "Refresh", "Export", "Print", and "Help" buttons at the bottom of the main content area.
- Sub-feature Panel:** Points to the "Information" tab content area.

Information Tab Content:

Name	Value
System Description	BNT RackSwitch G8124
Management/Switch MAC Address	3a:30:d2:a1:b2:81
System Up Since	0 days, 7 hours, 32 minutes and 41 seconds
Location	
Contact	
Boot Code Version	6.3.1.0
Image 1 Software Version	version 6.3.1.0, downloaded 15:20:00 Mon May 26 2008
Image 2 Software Version	version 6.3.2.0, downloaded 17:32:10 Mon May 26 2008
Current Image	image1
Current Config	active

Device Console - Top Frame

On the left-hand side, the top frame shows the selected switch information consisting of IP address, switch type. On the right-hand side, it shows the save pending status indicating whether configuration save is needed for that switch or not.

Device Console – Feature (or Left) Frame

The feature (or left) frame displays the tabs corresponding to Monitor and Configure options. The Configure tab is enabled only for those switches for which configuration management is supported.

When you select a tab, the corresponding features listed in a tree hierarchy. When you select a node, the right hand content pane is refreshed to display the tabs associated with the selected feature (node).

Device Console – Content (or Right) Frame

The content (or right) frame displays the global menu bar, tabs and panel menu bar corresponding to feature selected in Feature (or Right) frame.

Device Console Page – Menu Bar

The menu bar of the Device Console page provides the global commands that can be invoked for the selected switch irrespective of the selected tab. The following table describes the Main Menu Bar items.

Table 13 Device Console Page — Menu Bar Items

Menu	Description
Actions	Provides a set of actions commands that can be invoked on the selected switch.
Help	Provides commands for accessing online help and support options for SNSC.

Actions Menu

The following table describes the Device Console page **Actions** menu commands:

Table 14 Device Console Page — Actions Menu

Sub-menu	Description
Apply	Applies any changes that you have made to the switch configuration.
Save	Saves the current configuration to the flash memory.
Diff Config	Opens a window to display any pending configuration changes.
Diff Flash	Opens a window to display any pending configuration changes and the affected configuration stored in flash memory on the switch.
Config Dump	Opens a window to display a dump of the current switch configuration.
Syslog Dump	Opens a window to display the syslogs available on the switch.
Revert	Reverts the switch to the current active configuration. This command is available if you did not apply the new configuration settings.
Revert Apply	Reverts the switch to the current saved configuration. This is available if you applied but did not save the new configuration settings.
Reboot Switch	Reboots the switch by reloads and saving the current RAM memory.
Exit	Closes the Device Console window.

Help Menu

The following table describes the Device Console **Help** menu commands:

Table 15 Device Console — Help Menu

Sub-menu	Description
Help Contents	Opens the context specific online Help page.
IBM Systems Networking	Takes you to IBM Systems Networking page in a separate window.
About IBM System Networking Switch Center	Opens a dialog box that shows the version, license details and the list of supported switches.

Device Console Page – Panel Menu Bar

The panel menu bar is specific to the panel shown in the content pane. Though some of them are disabled for some panels, but the associated action remains the same across panels.

Table 16 Device Console — Panel Menu Bar Items

Menu	Description
Submit	Submits the configuration changes you have made to the switch parameters. This menu is available only for configuration panels.
Apply	Applies any changes that you have made to the switch configuration. This menu is available only for configuration panels.
Refresh	Refreshes the panel contents.
Export	Export the data displayed in the panel to a CSV file.
Print	Opens the Print dialog so that you can print the current page.
Help	Launches the context-sensitive help page.

Device List – Go To search option

The Device List page includes a *Go To* field that allows you to list the device based on IP address or System Name string. You can perform this operation by specifying the IP address or part/full system name string in the *Go To* field and click the **Search** icon (Magnifying Glass).

If you enter an IP address or System Name in *Go To* field and if a device with that IP address is discovered, the corresponding Device Console page launches upon the completion of search operation.

If you specify part of the System Name string and it matches multiple devices (for example, there are 3 switches configured with system names “Core Switch1”, “Router Switch2”, “Gateway Switch3” and you specify the search string as “Switch”), then all those matched devices are provided in a filtered list (similar to the List Device(s) drop-down function).

Note: SNSC-C provides an option at the top of the filtered list to clear the filter.

Device List – Favorite Marking and Adding Notes

The Device List page enables you to set any row as a Favorite row so that you can list only those devices using List Device(s) filter (see [Figure 12 on page 97](#)). If you have logged in as an Administrator, you can also add notes for any discovered device to indicate any changes such as firmware upgrade, config upgrade occurring at a later date/time so that other users can see that message.

Favorite Marking

The Favorite marking works in toggle mode – clicking a favorite row removes the favorite marking and likewise, clicking a non-favorite row makes it a favorite one. Favorite row is marked with green star icon, where as the non-favorite row displays hollow gray star icon (see [Figure 11 on page 88](#)).

Note: Favorite markings are user-specific and the feature is available to all types of users.

Figure 12 Device List Showing Favorites and Notes Icons

Favorite row

Notes Added

List Device(s) filter

Notes Absent

Non-favorite row

Root				
	Product Name	IP Address	System Name	Health Status
Root (57 devices)				
<input type="checkbox"/>	BNT/Nortel Layer 2-3 Giga	172.25.160.3		Up
<input type="checkbox"/>	BNT RackSwitch G8000	172.25.160.90		Critical
<input type="checkbox"/>	BNT/Nortel 1/10Gb Uplink	192.168.6.75		Up
<input type="checkbox"/>	BNT RackSwitch G8100	192.168.130.11		Up
<input type="checkbox"/>	BNT RackSwitch G8100	192.168.130.31		Up
<input type="checkbox"/>	BNT RackSwitch G8000	192.168.130.91		Up

Adding Notes

If you have logged into System Networking Switch Center as an Administrator, you can add Notes for an individual device/switch, using the following steps:

- 1 Click the Notes icon (see [Figure 12 on page 97](#)) to open the Notes dialog.
- 2 Type-in the text you want to add.
- 3 Click **OK**.

You can also add Notes to group of rows, using the following steps:

- 1 In Device List table, select one or more rows.
- 2 Choose menu **Group Operations > Notes > Add** to bring up Notes dialog.


3 Type-in the text you want to add.

4 Click **OK**.

Note: When Notes is added, the Notes icon changes to Notes Added icon (orange flag).

You can see the added Notes as a tool tip by moving the mouse on Notes Added icon (see [Figure 13 on page 98](#)).

Figure 13 Display of Notes as a Tool Tip



Root			
<input type="checkbox"/>		Product Name	IP Address
Root (57 devices)			
<input type="checkbox"/>	★	BNT/Nortel Layer 2-3 Giga	172.25.160.3
<input type="checkbox"/>	☆	BNT RackSwitch G8000	172.25.160.90
<input type="checkbox"/>	☆	BNT RackSwitch G8100	172.25.160.91
<input type="checkbox"/>	★	BNT RackSwitch G8100	192.168.130.1
<input type="checkbox"/>	★	BNT RackSwitch G8100	192.168.130.3

Removing Notes

You can remove the Notes through Administrator login using the following steps:

- 1 Click the **Notes Added** icon (see [Figure 13 on page 98](#)) to open the Notes dialog.
- 2 Click **Remove**.

Notes from group of rows also can be removed using the following steps:

- 1 In Device List table, select one or more rows.
- 2 Choose menu **Group Operations > Notes > Remove**.

Changing IBM System Networking Switch Center Configuration

You can change many of the parameters that influence System Networking Switch Center's behavior. You can find the corresponding commands under the **Options** and **Maintenance** menus. The following sub sections list those parameters that can be configured:

- ["Changing the Default General Properties" on page 101](#)
- ["Changing the Default Health Check Properties" on page 102](#)
- ["Changing the Default Refresh Configuration Parameters" on page 103](#)
- ["Changing the Default Data Collection Configuration Parameters" on page 104](#)
- ["Changing the Default Log File Configuration Parameters" on page 105](#)
- ["Changing the Default DB Data Purge Configuration Parameters" on page 106](#)

Changing the Default General Properties

The General Properties parameters control the number of servers on which you can currently perform group operations and session timeout. See [Figure 14 on page 101](#) for an example of the General Properties window.

- 1 Choose menu **Options > General Properties**.
- 2 Change the Concurrent Limit setting. The value range is 10 to 50.
- 3 Change the Session Timeout setting. The value range is 10 to 1000 minutes.
- 4 Change whether the temperature should be displayed in Celsius or Fahrenheit.
- 5 Click **Save**. The changes take effect immediately.

Figure 14 General Properties Window

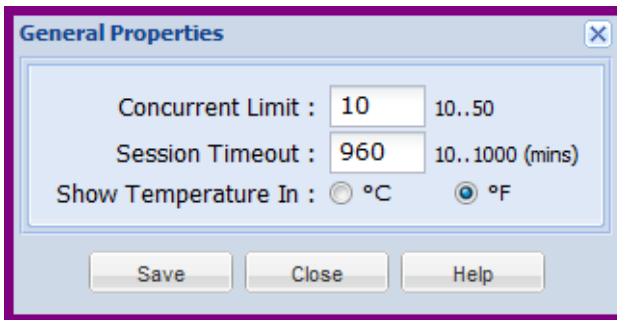


Table 17 General Properties field descriptions

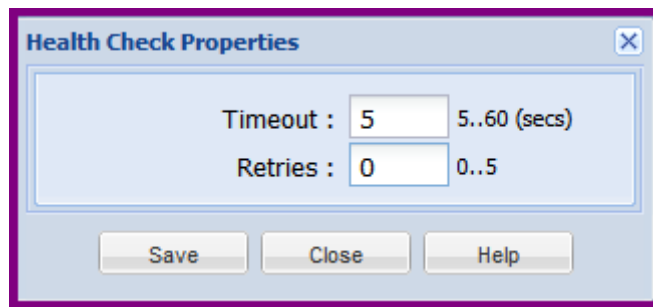
Field	Description
Concurrent Limit	Defines number of concurrent processing to be made while performing group operations. Default value is 10.
Session Timeout	The inactivity timeout in minutes after which SNSC invalidates a logged-in session.
Show Temperature In	Refers to the temperature sensor display in Celsius (°C) or Fahrenheit (°F). Default setting is °F.

Changing the Default Health Check Properties

The health check properties control the timeout and the retries used while performing the periodic health check for the discovered switches. See [Figure 15 on page 102](#) for an example of the Health Check Properties window.

- 1 Choose menu **Options > Health Check Properties**.
- 2 Change the Timeout setting. The value range is 5 to 60 seconds.
- 3 Change the Retries setting. The value range is 0 to 5.
- 4 Click **Save**. The changes take effect during next health check polling.

Figure 15 Health Check Properties Window

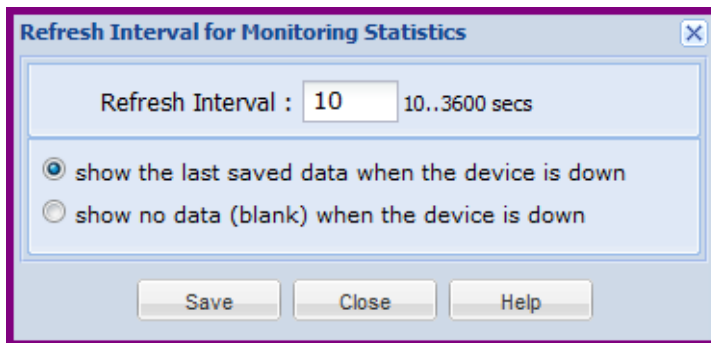


Changing the Default Refresh Configuration Parameters

The refresh configuration parameters control how frequently System Networking Switch Center updates the statistics tables in the user interface. The statistics tables are updated by loading information from the System Networking Switch Center database. For example, if you set the polling configuration parameters to 20 seconds, the switch statistical information is refreshed every 20 seconds. The new parameter takes effect immediately. See [Figure 16 on page 103](#) for an example of the Refresh Configuration parameters window.

- 1 Choose menu **Options > Refresh Configuration**.
- 2 Enter the new value for Refresh Interval between 10 to 3600 seconds.
- 3 Select one of the options that enables System Networking Switch Center to display either the last saved data or no data (blank) when the selected device is down.
- 4 Click **Save**.

Figure 16 Refresh Interval for Monitoring Statistics Window



Changing the Default Data Collection Configuration Parameters

The data collection parameters control how often System Networking Switch Center collects switch data from the database. See [Figure 17 on page 104](#) for an example of the data collection parameter configuration window.

- 1 Choose menu **Options > Data Collection Configuration**.
- 2 Enter new values for HealthCheck Server and Performance Statistics polling intervals. For HealthCheck Server, the value ranges from 10 to 3600 seconds. For Performance Statistics, the value ranges from 5 to 3600 seconds.
- 3 Click **Save**. The new parameter takes effect immediately.

Figure 17 Data Collection Configuration Window

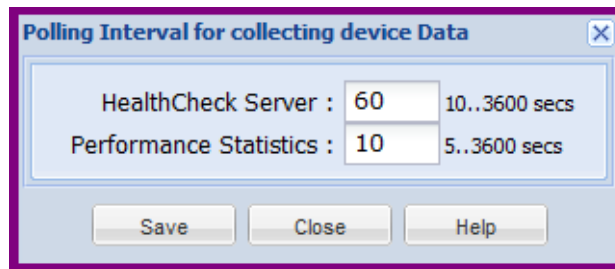


Table 18 Data Collection Properties field descriptions

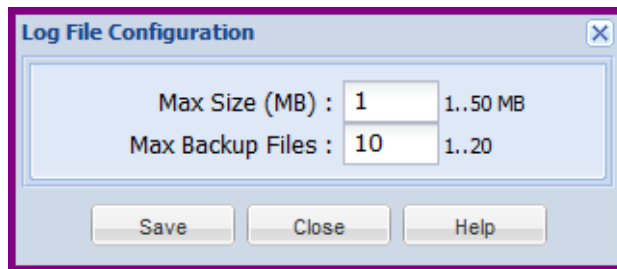
Field	Description
HealthCheck Server	Defines the interval in seconds that SNSC checks the switch status, either up or down.
Performance Statistics	Defines the interval in seconds that SNSC collects and updates performance statistics.

Changing the Default Log File Configuration Parameters

The log file configuration parameters control the log file size and the maximum number of log file backup that System Networking Switch Center can keep at any given time. You can change the log file configuration using the following steps:

- 1 Choose menu **Maintenance > Log File Configuration**.
- 2 Enter the new value for maximum file size in MB (Max Size (MB)) between 1 to 50.
- 3 Enter the new value for maximum number of backup files to keep the log messages (Max Backup Files) between 1 to 20.
- 4 Click **Save**.

Figure 18 Log File Configuration Window



Changing the Default DB Data Purge Configuration Parameters

The database purge parameters control the frequency of database purges. After a database purge, information about events, syslog and performance data are removed. You can select days or events count as the basis for database purge frequency.

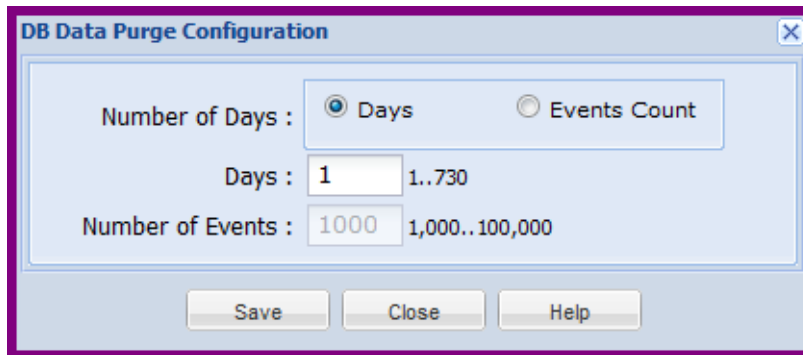
For example, if the purge frequency is set for seven days, then the data older than seven days are purged regularly. The purged data is stored in text form and you can find these files in the following directory: `<SNSC INST DIR>/database/backup`. The purged data files are created using the following notation:

- `events_DDMMYYYY_HHMMSS.txt`
- `syslogs_DDMMYYYY_HHMMSS.txt`

In the above notation, DD stands for day (01-31), MMM stands for month (Jan, Feb, and so on), YYYY stands for year, HH for Hour (00-23), MM for minutes (00-59) and SS for seconds (00-59). However, you can change the purged data location and the format of the timestamp, by editing the DBPurgeDirectory and the TimeStampFormat parameters in the following file: `backup.properties` (see [“Modifying the backup.properties Configuration File” on page 155](#)).

- 1 Choose menu **Maintenance > DB Data Purge Configuration** (see [Figure 19 on page 107](#)).
- 2 Click Days or Events Count as the purge frequency parameter:
- 3 Complete the following steps if you selected Days. If you selected Events Count, go to step 4.
 - a Enter a value between 1 and 730 in the Number of Days field.
 - b Click **Save**.
- 4 If you selected Events Count, complete the following steps.
 - a Enter a value between 1000 and 100,000 in the Number of Events field.
 - b Click **Save**.

The new values take effect immediately.

Figure 19 DB Data Purge Configuration Window

The image shows a 'DB Data Purge Configuration' window with a light blue background and a purple border. At the top, the title bar reads 'DB Data Purge Configuration' with a close button (X) on the right. The main area contains two radio buttons: 'Days' (selected) and 'Events Count'. Below the 'Days' radio button, there is a text input field containing '1' and a range indicator '1..730'. Below the 'Events Count' radio button, there is a text input field containing '1000' and a range indicator '1,000..100,000'. At the bottom of the window, there are three buttons: 'Save', 'Close', and 'Help'.

DB Data Purge Configuration

Number of Days : ☒ Days ☐ Events Count

Days : 1..730

Number of Events : 1,000..100,000

Save Close Help

Configuring Authentication

You can configure System Networking Switch Center to use different authentication mechanisms for authenticating System Networking Switch Center users. The following subsections list different mechanisms supported by System Networking Switch Center:

- [Local Authentication](#)
- [TACACS+ Authentication](#)
- [RADIUS Authentication](#)

Local Authentication

Local authentication is enabled by default in System Networking Switch Center. In this mechanism, the user credentials are stored in System Networking Switch Center database in encrypted format. You can configure System Networking Switch Center to use local authentication (in case, if authentication is set to a different mechanism) using the following steps:

- 1 Choose menu **Options > Authentication Configuration**.
- 2 Select LOCAL as the authentication mechanism.
- 3 If Admin is mapped to root, enter the Admin password in Admin Password field, or enter root password in Root Password field.
- 4 Click **Save**.

TACACS+ Authentication

System Networking Switch Center supports the default and the alternate TACACS+ authorization levels (similar to IBM BLADE switches). The following table shows authorization levels for the default and the alternate TACACS+ settings, one of which must be defined on the TACACS+ server.

Table 19 TACACS+ Authorization Levels

User Access Level	Default TACACS+ Authorization Level	Alternate TACACS+ Authorization Level
user	0	0 - 1
oper	3	6 - 8
admin	6	14 - 15

You can configure System Networking Switch Center to use TACACS+ authentication, using the following steps:

- 1 Choose menu **Options > Authentication Configuration**.
- 2 Select TACACS as the authentication mechanism to bring up TACACS+ specific fields (see [Figure 20 on page 111](#)).
- 3 If Admin is mapped to root, enter the Admin password in Admin Password field, or enter root password in Root Password field.
- 4 Select the authorization level to use – Default or Alternate (see [Table 19](#)).
- 5 Enter the primary server IP address.
- 6 Enter the secondary server IP address.
- 7 Enter the secret for the primary server.
- 8 Enter the secret for the secondary server.
- 9 Enter the port number.
- 10 Enter a value for the timeout.
- 11 Enter a value for retries.
- 12 Click **Save**.

Figure 20 TACACS Authentication Configuration Window

Authentication Configuration

Current Authentication Mechanism: LOCAL

Select Authentication Mechanism: TACACS

Admin Password:

Use Authroization Level

☒ Default (0-6) ☐ Alternate (0-15)

Server Properties Configuration

Primary Server IP Address: 0.0.0.0

Secondary Server IP Address: 0.0.0.0

Secret for Primary IP Address:

Secret for Secondary IP Address:

Port: 49

Timeout: 5

Retries: 3

Save Close Help

You can configure System Networking Switch Center to use local authentication (in case, if authentication is set to a different mechanism) using the following steps:

- 1 Choose menu **Options > Authentication Configuration**.
- 2 Select LOCAL as the authentication mechanism.
- 3 If Admin is mapped to root, enter the Admin password in Admin Password field, or enter root password in Root Password field.
- 4 Click **Save**.

Note: If System Networking Switch Center is unable to contact either Primary or Secondary TACACS+ servers, it uses the local authentication mechanism for validating the user credentials.

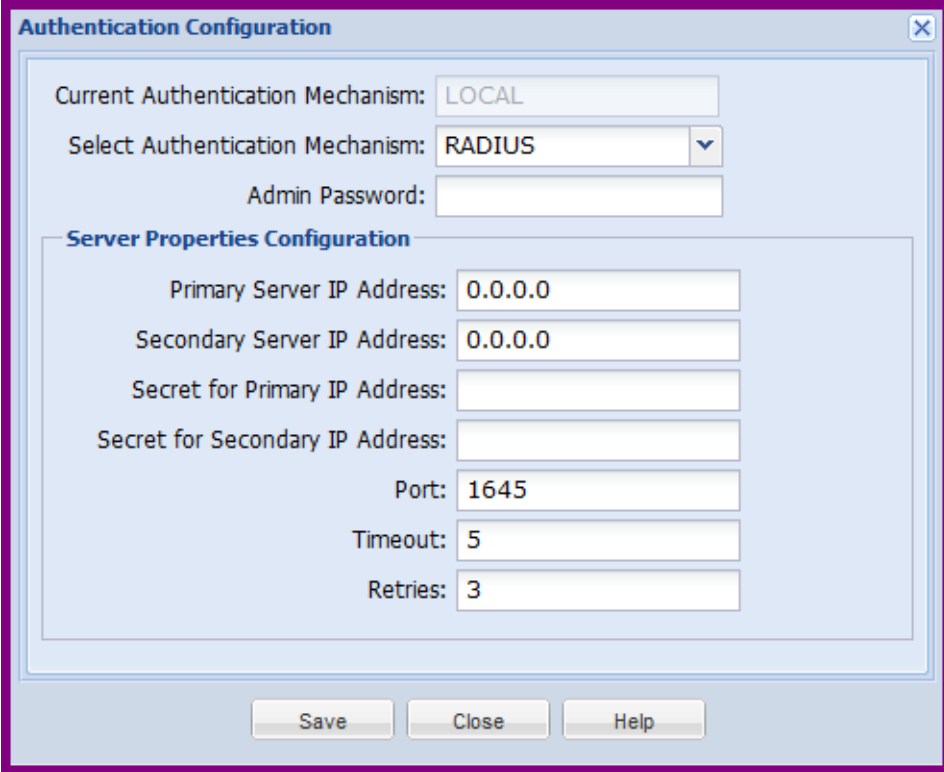
RADIUS Authentication

For RADIUS authentication, similar to those requirements for IBM BLADE switches, System Networking Switch Center requires all user privileges, other than those assigned to the Administrator, have to be defined in the RADIUS dictionary. RADIUS attribute 6 which is built into all RADIUS servers defines the administrator. The file name of the dictionary is RADIUS vendor-dependent. The following RADIUS attributes should be configured on the RADIUS server:

User Name/Access	User Service Type	Value
user	<i>Vendor supplied</i>	255
oper	<i>Vendor supplied</i>	252
admin	<i>Vendor supplied</i>	6

You can configure System Networking Switch Center to use RADIUS authentication using the following steps:

- 1 Choose menu **Options > Authentication Configuration**.
- 2 Select RADIUS as the authentication mechanism to bring up RADIUS specific fields (see [Figure 21 on page 113](#)).
- 3 If Admin is mapped to root, enter the Admin password in Admin Password field, or enter root password in Root Password field.
- 4 Enter the primary server IP address.
- 5 Enter the secondary server IP address.
- 6 Enter the secret for the primary server.
- 7 Enter the secret for the secondary server.
- 8 Enter the port number.
- 9 Enter a value for the timeout.
- 10 Enter a value for retries.
- 11 Click **Save**.

Figure 21 RADIUS Authentication Configuration Window

The image shows a software window titled "Authentication Configuration". It contains several input fields and a section for server properties. At the bottom are "Save", "Close", and "Help" buttons.

Field	Value
Current Authentication Mechanism:	LOCAL
Select Authentication Mechanism:	RADIUS
Admin Password:	
Server Properties Configuration	
Primary Server IP Address:	0.0.0.0
Secondary Server IP Address:	0.0.0.0
Secret for Primary IP Address:	
Secret for Secondary IP Address:	
Port:	1645
Timeout:	5
Retries:	3

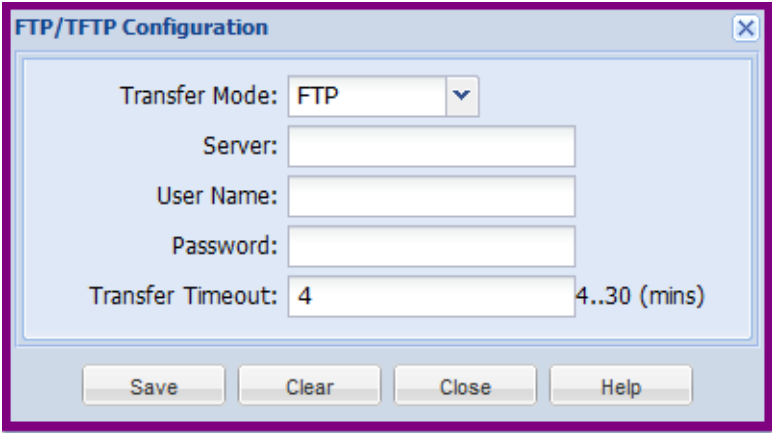
Note: If System Networking Switch Center is unable to contact either Primary or Secondary RADIUS servers, it uses the local authentication mechanism for validating the user credentials.

Configuring FTP/SFTP/TFTP Server Parameters

You must configure an FTP, TFTP, or SFTP server before you can perform switch administration tasks such as image and configuration backup, image download, panic dump and so forth. For information about switch administration tasks, and the role of the FTP/SFTP/TFTP server, see [“Performing Group Operations” on page 179](#).

- 1 Choose menu **Options > FTP/SFTP/TFTP Configuration**.
- 2 Select FTP, TFTP, or SFTP as the transfer mode.
- 3 Enter the IP address of the FTP, TFTP, or SFTP server.
- 4 If you selected FTP as the transfer mode:
 - a Enter the FTP server user name.
 - b Enter the FTP server password.
- 5 Enter the transfer timeout in minutes. This timeout setting is useful for dealing with an FTP/SFTP/TFTP server residing in a slow network.
- 6 If you selected SFTP as the transfer mode:
 - a Enter the SFTP server user name.
 - b Enter the SFTP server password.
 - c Enter the transfer server port (optional).
- 7 Click **Save**.

Figure 22 FTP/SFTP/TFTP Server Configuration Window



The screenshot shows a dialog box titled "FTP/TFTP Configuration". It contains the following fields and controls:

- Transfer Mode:** A dropdown menu currently set to "FTP".
- Server:** An empty text input field.
- User Name:** An empty text input field.
- Password:** An empty text input field.
- Transfer Timeout:** A text input field containing the value "4", followed by the text "4..30 (mins)".

At the bottom of the dialog, there are four buttons: "Save", "Clear", "Close", and "Help".

Modifying Discovery Parameters

You can modify SNMP parameters of a discovered device. This helps System Networking Switch Center continue to manage the device if the SNMP parameters, such as community strings (SNMPv1/v2c) or authentication credentials (SNMPv3), are changed after discovering the device in System Networking Switch Center.

To modify the SNMP parameters:

- 1 In Device List table, select the switch for which you want to change the SNMP parameters used by System Networking Switch Center for managing that switch.
- 2 Choose menu **Device > Change SNMP Parameters** to open Modify dialog (see [Figure 23 on page 116](#)).
- 3 If Root user is enabled, enter the root password in Root Password field (this field is not visible if Root user is disabled).
- 4 If you want to use SNMPv1 or SNMPv2c:
 - a Enter the new read and write community strings in Read Community and Write Community fields respectively.
 - b Click **Save**. System Networking Switch Center begins using the supplied SNMPv1 or SNMPv2c parameters for managing that switch.
- 5 If you want to use as SNMPv3:
 - a Click **Use SNMPv3**.
 - b Enter the new user name in User Name field.
 - c If Authentication is enabled on the switch (switch is configured in AuthNoPriv or AuthPriv), select the authentication protocol (MD5 or SHA1) from Authentication Protocol list and enter the authentication password in Authentication Password field.
 - d If Privacy is enabled on the switch (switch is configured in AuthPriv), select DES in the Privacy Protocol list and enter the privacy password in the Privacy Password field.
 - e Click **Save**. System Networking Switch Center begins using the supplied SNMPv3 parameters for managing that switch.

Figure 23 Modify Discovery Configuration Window

Modify discovery parameters [X]

IP Address: 172.16.2.91

Root Password:

Read Community:

Write Community:

SNMPv3

☐ Use SNMPv3

User Name:

Authentication Protocol: NONE ▼

Authentication Password:

Privacy Protocol: NONE ▼

Privacy Password:

Save Close Help

VM Management Server – Connector Configuration and VMware Infrastructure (VI) Client Integration

System Networking Switch Center provides the following advanced support:

- Viewing the virtual switch information that are available in VMready switch versions.
- Integrating System Networking Switch Center with VMware Infrastructure (VI) Client application so that System Networking Switch Center can be launched inside VMware Infrastructure (VI) Client.

Configuring VM Management Server Connector

In order to retrieve Virtualization information from the VirtualCenter and to integrate System Networking Switch Center with VMware Infrastructure (VI) Client, it is necessary to configure VM Management Server Connector. The VM Management Server Connector retrieves the required information by interacting with the VirtualCenter.

- 1 Choose menu **Options > VM Management Server Connector > Configuration** to launch the VM Management Server Configuration window (see [Figure 24 on page 119](#)).
- 2 Select the protocol to be used for connecting to VirtualCenter. If you are using HTTPs, it is mandatory to generate the keystore.
- 3 In the Port field, enter the port on which VirtualCenter is listening for HTTP or HTTPs requests.
- 4 In the IP Address/Host Name field, enter IP address or host name of the system on which Virtual Center is running.
- 5 Enter the user name in User Name field that should be used for authenticating with VirtualCenter.
- 6 Enter the password in Password field that should be used for authenticating with VirtualCenter.
- 7 If you have selected HTTPS protocol, enter the path of the file containing SSL Certificate. If you select HTTPs protocol, enter the file path that contains the SSL certificate or click Browse to browse for the file.
- 8 (Optional) To check whether the given address and login credentials are valid, click **Test**.
- 9 Click **Add** to save the configuration.

- 10 (Optional) In the Polling Interval field, enter the polling interval in minutes to be used for periodically contacting VirtualCenter to retrieve the information and click **Save** to store the configured value.

Figure 24 VM Management Server Configuration Window

VM Management Server Configuration

General Information

Polling Interval (minutes): 5 Save

VM Management Servers

VM Management Server Information

Protocol: HTTPS ▼

Port: 443

IP Address/Host Name: 172.25.110.4

User Name: Administrator

Password: ●●●●

SSL Certificate File Path: C:/Program Files/BLADE/BLADEHarmc Browse...

Configured VM Management Servers

<input type="checkbox"/>	Protocol	Port	IP Address/Host Name	User Name
<input checked="" type="checkbox"/>	HTTPS	443	172.25.110.4	Administrator

Note: The path should also include the SSL certificate file name

Test Add Delete Register Unregister Refresh Close Help

Integrating IBM System Networking Switch Center with VMware Infrastructure (VI) Client Application

You can integrate System Networking Switch Center UI with VMware Infrastructure (VI) Client Application so that System Networking Switch Center can be conveniently launched within VI Client environment (see [Figure 25 on page 121](#)).

- 1 Choose menu **Options > VM Management Server Connector > Configuration** to launch the VM Management Server Configuration window (see [Figure 24 on page 119](#)).

- 2 Select the VM Management Server to use from the Configured VM Management Servers table (see [“Configuring VM Management Server Connector” on page 117](#) for steps on how to configure VM Management Server connector).
- 3 Click **Register**. If there are any errors, System Networking Switch Center displays that error message.

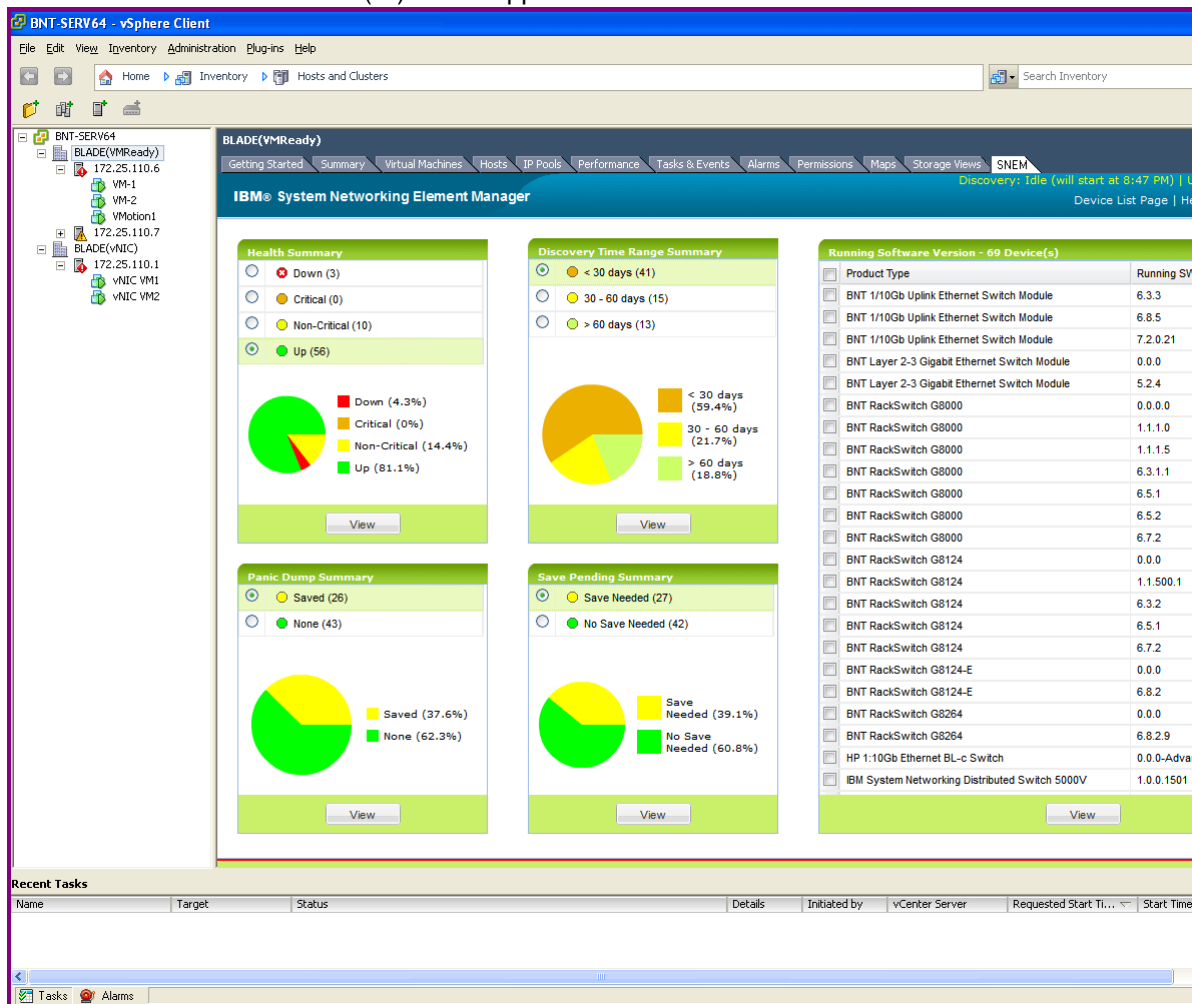
You can also check whether System Networking Switch Center is registered with VMware Infrastructure (VI) Client application or not using the following steps:

- 1 Launch VI client application (if it is already running, then close it and launch it again)
- 2 Choose menu **Plug-ins > Manage Plug-ins** to launch Plug-in Manager window
- 3 If System Networking Switch Center is successfully registered, you will see an entry for IBM System Networking Switch Center under Installed Plug-ins section.

Launching IBM System Networking Switch Center from VMware Infrastructure (VI) Client Application

- 1 Once you have integrated System Networking Switch Center in VM Management Server, launch VMware Infrastructure (VI) client application. Note that if VMware Infrastructure (VI) Client application is already running, you have to close and restart it to enable VI Client to download the newly added plug-in (IBM System Networking Switch Center).
- 2 Select System Networking Switch Center tab in VI Client (see [Figure 25 on page 121](#)) to bring up the System Networking Switch Center login page.

Figure 25 IBM System Networking Switch Center Launched Inside VMware Infrastructure (VI) Client Application



Un-registering IBM System Networking Switch Center from VMware Infrastructure (VI) Client Application

- 1 Choose menu **Options > VM Management Server Connector > Configuration** to launch the VM Management Server Configuration window (see [Figure 25 on page 121](#)).
- 2 In the Configured VM Management Servers table (see [“Configuring VM Management Server Connector” on page 117](#)), select the VM Management Server from which you want to un-register System Networking Switch Center.

3 Click **Unregister**.

Dial Home Configuration

The Dial Home feature offers a round-the-clock device monitoring facility. It enables you to configure System Networking Switch Center to send an email alert to designated recipients upon receiving traps from the switches.

To configure Dial Home:

- Log into SNSC as an Administrator.
- Specify the outgoing email server to use and a list of recipients' email addresses.
- Select the traps for which the email alerts are to be sent.

Configuring Email Parameters

You can configure email parameters, such as Outgoing Mail Server, Email Format, Sender's Mail ID, and Recipient Email Addresses to be used for sending email alerts:

- 1 Choose menu **Options > Dial Home > Email Configuration** to launch the Email Configuration window.

Figure 26 Email Configuration Window

The screenshot shows the 'Email Configuration' window with the following sections:

- General Settings:**
 - Outgoing Mail Server Address: [Text Field]
 - Mail Server Port: 25 [Text Field]
 - Email Format: Plain-text [Dropdown Menu]
 - Sender's Email Address: [Text Field]
- Security and Authentication:**
 - ☐ Use Security Settings
 - User Name: [Text Field]
 - Password: [Text Field]
 - Use Secure Connection: ☒ No ☐ TLS ☐ SSL
- Email Addresses (comma separated):**
 - [Large Text Area]

At the bottom of the window are five buttons: Apply, Refresh, Test, Close, and Help.

- 2 In the **Outgoing Mail Server Address** field, enter the outgoing mail server address .
- 3 Enter the **Mail Server Port** to use. By default, it is set to SMTP port 25.
- 4 From the **Email Format** list, select the format in which the email alert is to be sent. You can send email alerts in plain text or in XML.
- 5 In the **Sender's Email Address** field, enter the address from which the email alerts are to be sent.

- 6 If you are using a POP3 mail server, you can configure additional security and authentication parameters as follows:
 - a Check **Use Security Settings**.
 - b Enter the User Name.
 - c Enter the Password.
 - d Next to **Use Secure Connection**, select either **No**, **TLS**, or **SSL**.
- 7 In the **Recipient Email Address** field, enter the recipients' email addresses, separated by a comma.
- 8 Before saving the configuration, verify whether the outgoing mail server address by clicking **Test**.
- 9 Click **Apply** to save the changes.

Adding Traps for Dial Home

To add traps for Dial Home:

- 1 Choose menu **Options > Dial Home > Traps Configuration** to launch the Traps Configuration window.

Figure 27 Traps Configuration Window

Title Information

Select Devices : ☒ All ☐ IP Address

Device Type : IBM BNT Layer 2/3 Copper Gigabit Ethernet Switch Module f

IP Addresses : (comma separated)

Trap Type : altSwPrimaryPowerSupplyFailure

Description

The primary power supply failed

Configured Traps

Trap Type	Device Type	IP Address	Description
-----------	-------------	------------	-------------

Add Delete Refresh Close Help

- 2 You can add traps applicable to all switches or specific to a list of IP addresses by selecting the **All** or **IP Address** option from **Select Devices**.
- 3 From the **Device Type** list, select the device.
- 4 If you select the **IP Address** option, in the **IP Addresses** field, enter a list of comma-separated IP addresses.
- 5 From the **Trap Type** list, select the traps to add for Dial Home.
- 6 Click **Add** to add the selected traps.

Adding Health Status Messages for Dial Home

To add health status message for Dial Home:

- 1 Choose menu **Options > Dial Home > HealthStatus Configuration** to launch the HealthStatus Configuration window.

Figure 28 HealthStatus Configuration Window

HealthStatus Configuration

Title Information

Select Devices : ☒ All ☐ IP Address

Device Type : IBM BNT Layer 2/3 Copper Gigabit Ethernet Switch Module f ▼

IP Addresses : (comma separated)

HealthStatus Type : Up ▼

Description

HealthStatus is Up

Configured HealthStatus

HealthStatus Type	Device Type	IP Address	Description
-------------------	-------------	------------	-------------

Add Delete Refresh Close Help

- 2 You can add health status messages applicable to all switches or specific to a list of IP addresses by selecting the **All** or **IP Address** option from **Select Devices**.
- 3 From the **Device Type** list, select the device.
- 4 If you select the **IP Address** option, in the **IP Addresses** field, enter a list of comma-separated IP addresses.
- 5 From the **HealthStatus Type** list, select the health status messages to add for Dial Home.
- 6 Click **Add** to add the selected messages.

Email Message Format

When sending out email alerts, the display string OID (xxSwTrapDisplayString) that is normally associated with the trap is used as the Subject line. However, if the display string is missing, the trap description is used instead for the Subject line.

The Subject line also contains the IP address of the switch that emitted the trap, along with the trap type. The format of the Subject line is:

<IP Address>, <Trap Type>, <Variable Binding>

For example, a login failure (altSwLoginFailure) coming from a switch at IP address 192.168.1.10 with xxSwTrapDisplayString variable binding containing the information "Failed login attempt via TELNET from host 192.168.1.50" will be sent with the subject line as:

```
192.168.1.10, altSwLoginFailure, Failed login attempt via
TELNET from host 192.168.1.50
```

In the message body, the information associated with other variable bindings are included. The following example shows a typical message format (by taking various examples of the configurations files shown in the previous sections)

```
From: bhmadmin@foo.com
To: zoneloper@foo.com, zone2oper@foo.com
Subject: 192.168.1.10, altSwLoginFailure, Failed login attempt
via TELNET from host
192.168.1.50
IP Address: 192.168.1.10
Trap Type: altSwLoginFailure
Description: Failed login attempt via TELNET from host
192.168.1.50
Severity: Major
Timestamp: Mon Sep 01, 2008 ...
Variable Bindings Information:
1. Sys Name: XYZ
2. Sys Location: SC
Sys Contact: Foo Admin
```


System Networking Switch Center can be configured to send email messages in either plain text or XML. If using XML, the following schema is used for the message body:

```
<message-body>
<ip-address>...</ip-address>
<trap-type>...</trap-type>
<description>...</description>
<severity>...</severity>
<timestamp>...</timestamp>
<varbind name="XXX" value="..." />
<varbind name="XY" value="..." />
...
</message-body>
```

Configuring Console (SSH/Telnet Client) Application

System Networking Switch Center allows you to use a local console (SSH/Telnet) application residing on the system where the System Networking Switch Center UI is running (browser system) to open up CLI session with the selected device or switch.

The following sections describe various configuration require for launching the local console application:

Configure Web-browser Settings for launching local Telnet/SSH application

For Internet Explorer 7.x and above, ActiveX controls must be enabled as follows:

- 1 Select **Tools > Internet Options**.
- 2 Select the Security tab.
- 3 Click **Customs level...** to open the Security Setting – Internet Zone window.
- 4 Locate “Initialize and script ActiveX controls not marked as safe for scripting” parameter (press the “i” key to locate the parameter).
- 5 Select one of the radio buttons (**Enable (not secure)** or **Prompt**).
- 6 Click **OK**.

For Mozilla Firefox, the signed applet support should be set to true as given below:

- 1 Launch Mozilla Firefox.
- 2 In the Address bar, type the following to display the configurable parameters:
`about:config`
- 3 Locate the following parameter:
`signed.applets.codebase_principal_support`
(Enter the string signed in Filter: bar and press **Enter**).
- 4 If the Value is false, double-click the row to change it to true.

Set the local Telnet/SSH application path in IBM System Networking Switch Center

- 1 Choose menu **Options > Local Console Application** to open the window for setting the local Telnet/SSH application path.
- 2 Enter the telnet/SSH application path as well as any additional parameter required for launching it and click **Save**.

Note: System Networking Switch Center expects the following convention for the application path:

<Application Path> [<parameter 1> <parameter 2> ...] [\$IPADDR]

<Application Path> corresponds to the telnet/ssh application residing on the local system

<parameter 1>, *<parameter 2>*,... are optional parameters that might be required in order to launch the local application.

\$IPADDR parameter is not needed in many cases, but if specified, System Networking Switch Center replaces it with the target switch address while launching the application. If this parameter is not specified, then the target address is implicitly appended to the specified path. The \$IPADDR tag is useful if a local application expects the target IP address to be specified in the middle (for example, *<some application> <target address> <param1> <param2>...*).

Example:

If you are planning to use PuTTY.exe located in the directory `c:\tools`, then the application path is as follows:

```
c:\tools\PuTTY.exe -telnet
```

Note: PuTTY application requires an additional parameter (`telnet`) to be supplied to run in Telnet mode.

Launching the local Telnet/SSH application path in IBM System Networking Switch Center

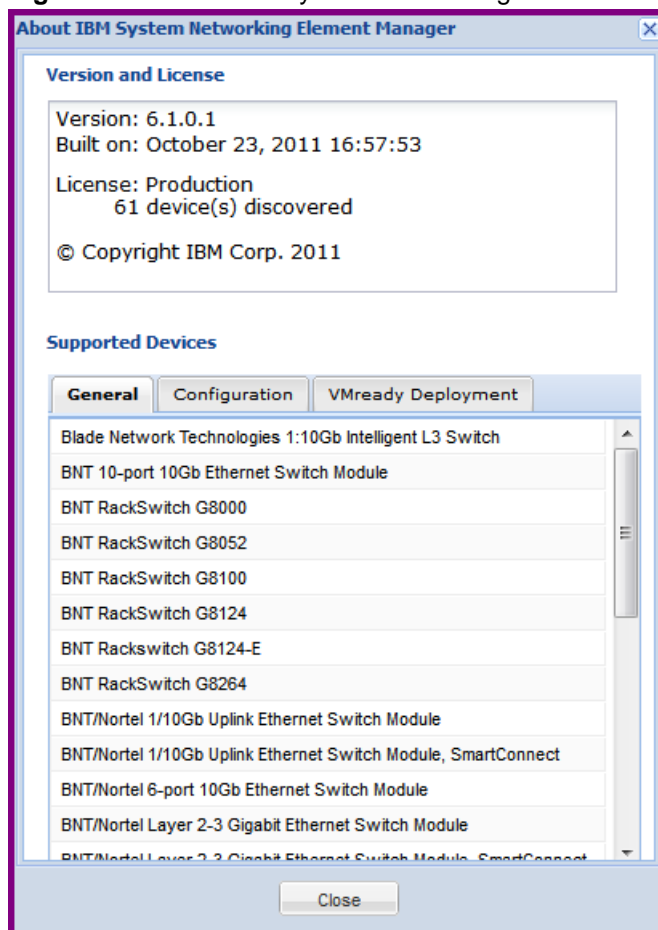
You can launch the local telnet/SSH application after completing the above settings:

- 1 In the Device List table, select the switch for which you want to launch telnet/SSH based CLI session.
- 2 Choose menu **Device > Launch > Console** to launch the application.

How to View Information About IBM System Networking Switch Center

- 1 Choose menu **Help > About** IBM System Networking Switch Center to view information about the software version, supported devices and related data.
- 2 Click **General** tab to view the supported devices.
- 3 Click **Configuration** tab to view those devices for which configuration management is supported. It should be noted that not all devices listed in General tab are found in Configuration tab. This is due to the availability of configuration management feature to selected devices.
- 4 Click the **VMready Deployment** tab to view the devices for which the VMready Across Datacenter Wizard configurations are supported.
- 5 Click **Close** to close the window.

Tip: Choose menu **Help > IBM Systems Networking** to access the IBM's Systems Networking Web site. The IBM Systems Networking Web page opens up in a new browser window and your System Networking Switch Center session remains active.

Figure 29 About IBM System Networking Switch Center Window

How to View Logs

The log viewer feature lets you see specific information logged about actions and scheduled tasks. All information is specific to the System Networking Switch Center application, not to any selected devices. For example, you can view a log of the scheduled backups, or look at the log generated by the most-recent System Networking Switch Center auto discovery process.

System Networking Switch Center has an automatic log archive program. After each log reaches the default size of 1 Mb, System Networking Switch Center starts a new log and saves the previous logfile as *<logfilename>.xx.log*. For example, you might have CMI logs named *cmi.1.log*, *cmi.2.log* and so forth. The current file is always named *<logfilename>.log*. The oldest archive would be *cmi.1.log*.

When the quantity of archived log files reaches the default maximum of ten, the older file is deleted and the others are moved up. For example, *x.1.log* is deleted and *x.2.log* is renamed as *x.1.log* and so forth.

To modify the default log file size and maximum number of backup files, log in to the System Networking Switch Center server and open *log.properties* under *<INSTALLATION DIR>\conf* directory. Edit the *LogFileMaxSizeKB* parameter to modify the maximum log file size. Edit the *MaxBackupFiles* parameter to modify the maximum number of maximum backup files. See [“Modifying the log.properties Configuration File” on page 153](#).

To view the archived log files, log in to the System Networking Switch Center server and open log files residing under the following directory: *<INSTALLATION DIR>/logs*

Navigating the Log Files

This section describes the navigation controls available on each log window.

Tip: Some log files can be more than 100 pages. Use your printer's Page Range feature to avoid printing the entire log.

Figure 30 Log File Navigation Controls

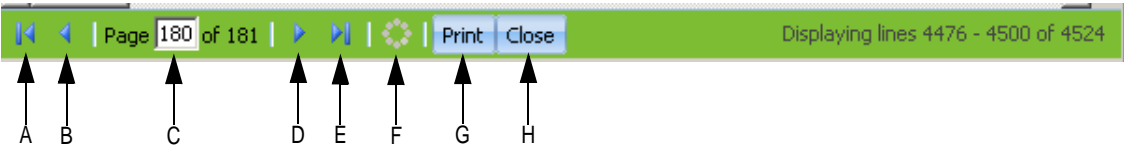


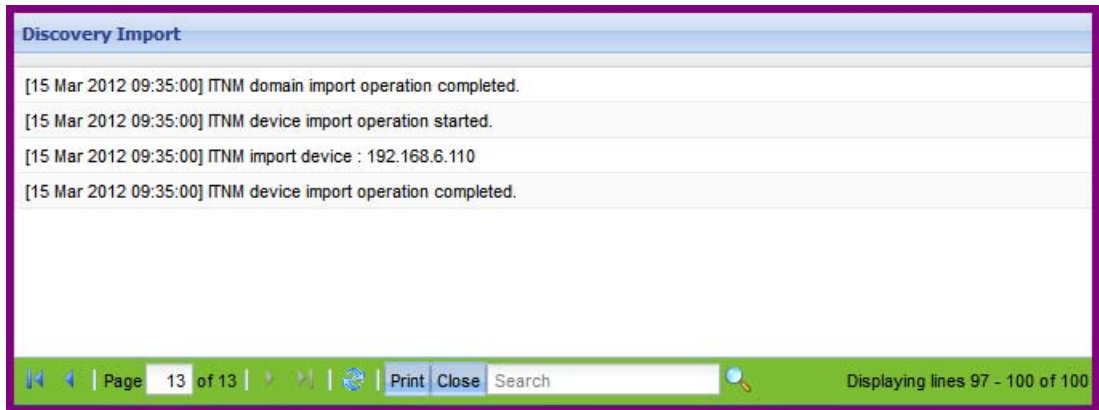
Table 20 Log File Navigation Controls

Control	Description
A	Go to first page of the log.
B	Go to the previous page.
C	Type a page number and click Enter to view the chosen page.
D	Go to the next page.
E	Go to the last page.
F	Refresh the current view of the log file.
G	Print the log.
H	Close the log viewer window.

Viewing the Discovery Import Log

This log captures data about the most recent import of devices and the network domains from Tivoli Network Manager.

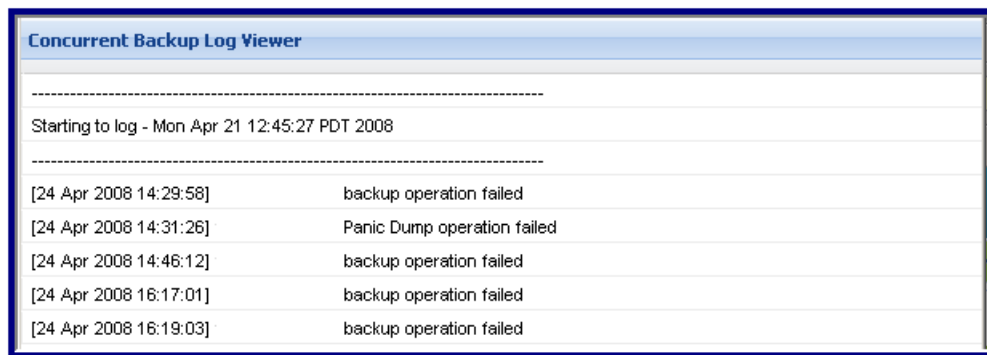
Figure 31 Discovery Import Log Viewer



Viewing the Concurrent Backup Log

This log captures status of concurrent backup tasks.

Figure 32 Concurrent Backup Log Viewer



Concurrent Backup Log Viewer	

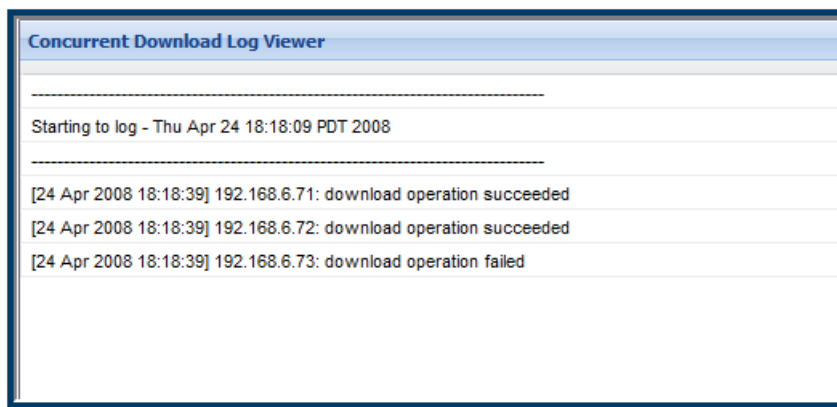
Starting to log - Mon Apr 21 12:45:27 PDT 2008	

[24 Apr 2008 14:29:58]	backup operation failed
[24 Apr 2008 14:31:26]	Panic Dump operation failed
[24 Apr 2008 14:46:12]	backup operation failed
[24 Apr 2008 16:17:01]	backup operation failed
[24 Apr 2008 16:19:03]	backup operation failed

Viewing the Concurrent Download Log

This log displays entries for Image Upgrade, Config Upgrade operations that are not scheduled.

Figure 33 Concurrent Download Log Viewer

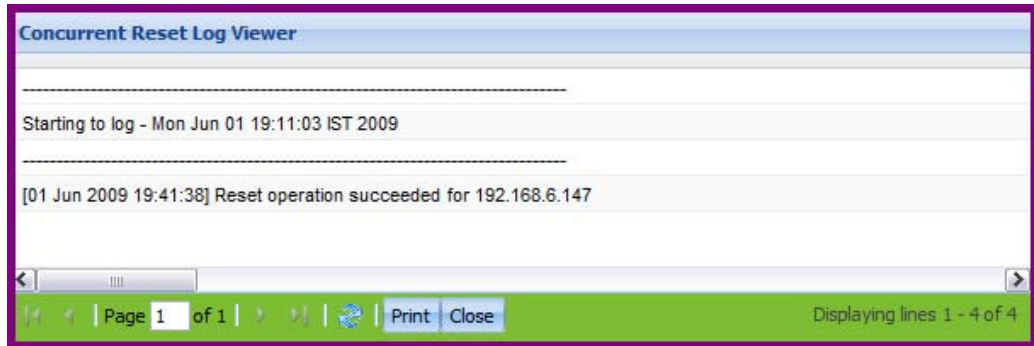


Concurrent Download Log Viewer	
Starting to log - Thu Apr 24 18:18:09 PDT 2008	
[24 Apr 2008 18:18:39]	192.168.6.71: download operation succeeded
[24 Apr 2008 18:18:39]	192.168.6.72: download operation succeeded
[24 Apr 2008 18:18:39]	192.168.6.73: download operation failed

Viewing the Concurrent Reset Log

This log displays entries for switch reset/reboot operations that are not scheduled.

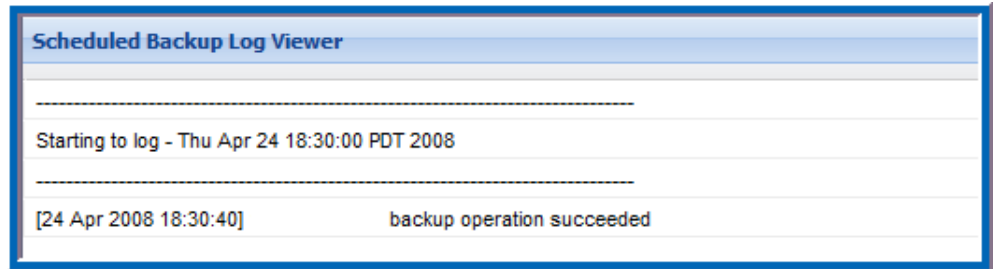
Figure 34 Concurrent Reset Log Viewer



Viewing the Scheduled Backup Log

This log captures status information about log entries for Image Backup, Config Backup, Panic Dump and TSDump operations that are scheduled in a job.

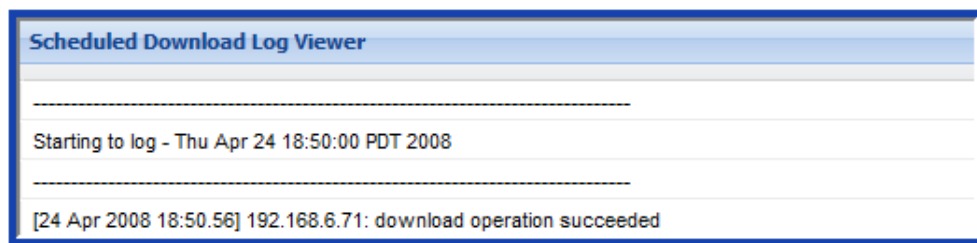
Figure 35 Scheduled Backup Log Viewer



Viewing the Scheduled Download Log

This log displays information about Image Upgrade and Config Upgrade operations that are scheduled in a job.

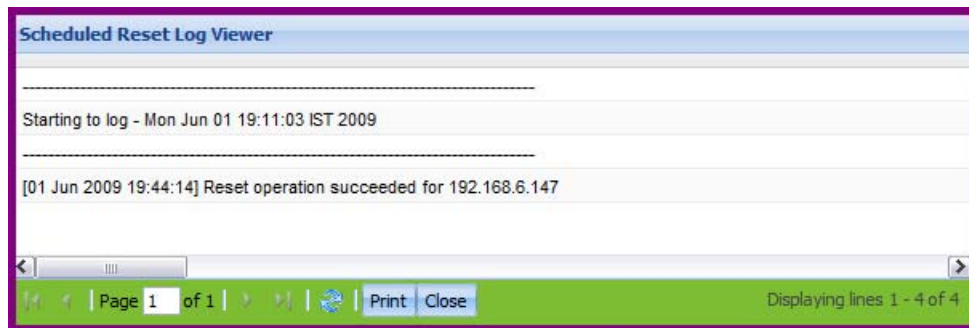
Figure 36 Scheduled Download Log Viewer



Viewing the Scheduled Reset Log

This log displays entries for switch reset/reboot operations that are scheduled in a job.

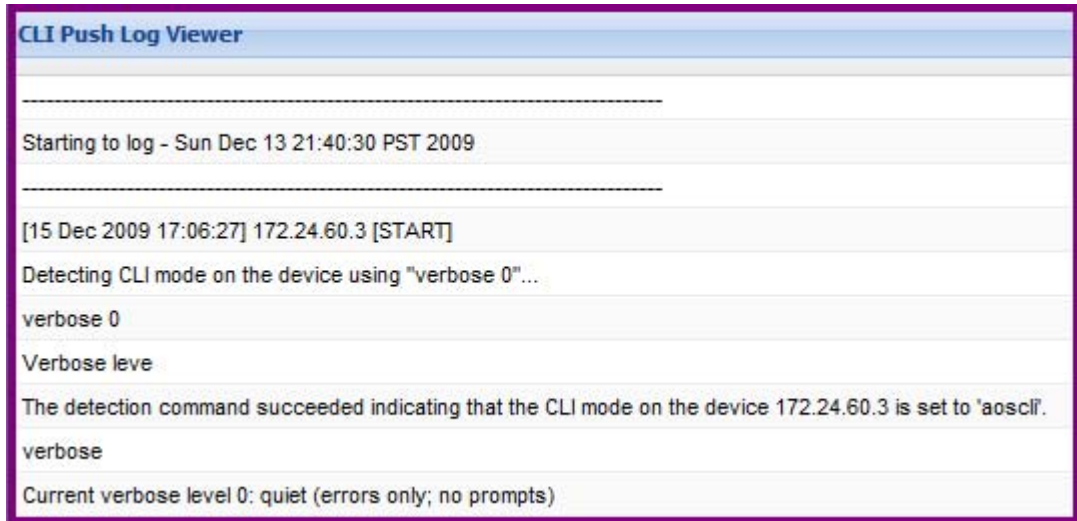
Figure 37 Scheduled Reset Log Viewer



Viewing the CLI Push Log File

This log displays the information dumped while performing the configuration upgrade for a switch using a set of CLI commands (CLI push).

Figure 38 CLI Push Log Viewer



```
CLI Push Log Viewer
-----
Starting to log - Sun Dec 13 21:40:30 PST 2009
-----
[15 Dec 2009 17:06:27] 172.24.60.3 [START]
Detecting CLI mode on the device using "verbose 0"...
verbose 0
Verbose leve
The detection command succeeded indicating that the CLI mode on the device 172.24.60.3 is set to 'aoscli'.
verbose
Current verbose level 0: quiet (errors only; no prompts)
```

Viewing the DB Log File

This log file displays status information about System Networking Switch Center database activities.

Figure 39 DB Log Viewer

DB Log Viewer	
[25 Apr 2008 10:26:48]	Initializing TrapReceiver Server is failed due to some exception.
[25 Apr 2008 10:26:48]	Initializing TrapReceiver Server is failed due to some exception.
[25 Apr 2008 10:26:48]	Initializing TrapReceiver Server is failed due to some exception.
[25 Apr 2008 10:26:58]	Getting latest data from device is failed.

Viewing the CMI Log

This log file captures date, time and status tasks performed by the System Networking Switch Center Common Management Interface (CMI). CMI is the System Networking Switch Center component that communicates with discovered devices. The CMI log viewer shows detailed communication between System Networking Switch Center and a device, including the IP address of the device.

Figure 40 CMI Log Viewer

CMI Log Viewer	
[25 Apr 2008 17:20:07] Sent SNMP TABLE WALK request to	for table PortInterfaceStatistics.
[25 Apr 2008 17:20:07] Sent SNMP GET request to	variables [sysObjectId, sysDescr, sysName, sysUpTime]
[25 Apr 2008 17:20:07] SNMP GET response received from	
[25 Apr 2008 17:20:07] SNMP TABLE WALK request for	completed.
[25 Apr 2008 17:20:07] SNMP TABLE WALK request for	failed due to timeout error.
[25 Apr 2008 17:20:08] Sent SNMP GET request to	for variables [sysObjectId, sysDescr, sysName, sysUpTime]
[25 Apr 2008 17:20:08] Sent SNMP TABLE WALK request to	for table PortInterfaceStatistics.
[25 Apr 2008 17:20:08] SNMP TABLE WALK request for	completed.

Viewing the VSI DB – RESTful Access Log

This log file contains the details of VSI DB access via REST APIs. The information includes the IP address of the client invoking REST API, type of request (GET/PUT/POST/DELETE), and the resource name. It also logs the status of each operation.

Figure 41 VSI Database – RESTful Access Log Viewer

VSI DB RESTful Access Log									
[06 Oct 2011 17:22:11]	192.168.6.72	HTTPS	DELETE	/vsitypes/1/1	200	Success			
[06 Oct 2011 17:22:34]	192.168.6.72	HTTPS	DELETE	/vsitypes/25/16777215	200	Success			
[06 Oct 2011 17:22:57]	192.168.6.72	HTTPS	DELETE	/vsitypes/25/16777215	200	Success			
[06 Oct 2011 17:24:08]	192.168.6.72	HTTPS	DELETE	/vsitypes/25/16777215	200	Success			
[06 Oct 2011 17:24:49]	192.168.6.72	HTTPS	DELETE	/vsitypes/25/16777215	200	Success			
[07 Oct 2011 11:14:55]	192.168.6.72	HTTPS	GET	/vsitypes/10/10	200	Success			
[07 Oct 2011 11:16:04]	192.168.6.72	HTTPS	DELETE	/vsitypes/10/10	200	Success			
[07 Oct 2011 11:17:19]	192.168.6.72	HTTPS	DELETE	/vsitypes/10/10	400	Error: VSI Type (version: 10, index: 10) not configured.			
[07 Oct 2011 11:18:14]	192.168.6.72	HTTPS	GET	/vsitypes/1/1	200	Success			
[07 Oct 2011 11:18:33]	192.168.6.72	HTTPS	DELETE	/vsitypes/1/1	200	Success			
[07 Oct 2011 11:20:02]	192.168.6.72	HTTPS	GET	/vsitypes/1/1	200	Success			

Viewing the Authentication Log

This log provides date, time and a description about authentication activities.

Figure 42 Authentication Log Viewer

Authentication Log Viewer	
[25 Apr 2008 11:57:34]	Local Auth mechanism is used for Authentication and Authorization for this BLADEHarmony Manage
[25 Apr 2008 11:57:34]	Authentication succeeded for admin and the user credential is admin.
[25 Apr 2008 12:08:53]	Local Auth mechanism is used for Authentication and Authorization for this BLADEHarmony Manage
[25 Apr 2008 12:08:53]	Authentication succeeded for admin and the user credential is admin.
[25 Apr 2008 12:27:41]	Local Auth mechanism is used for Authentication and Authorization for this BLADEHarmony Manage
[25 Apr 2008 12:27:41]	Authentication succeeded for admin and the user credential is admin.
[25 Apr 2008 13:13:51]	Local Auth mechanism is used for Authentication and Authorization for this BLADEHarmony Manage
[25 Apr 2008 13:13:51]	Authentication succeeded for admin and the user credential is admin.

Viewing the Sync Config Log File

This log contains date, time and status information about Sync Configuration tasks.

Figure 43 Sync Config Log Viewer

Sync Config Log Viewer.		
Starting to log - Tue Dec 29 15:22:52 IST 2009		
[29 Dec 2009 15:30:12]	Config Sync of VLAN(s) on device	Failed.
[29 Dec 2009 15:32:04]	Config Sync of VLAN(s) on device	Succeeded.

Viewing the VM Server Log

This logs the connectivity of System Networking Switch Center with VirtualCenter and any data collection failures that happen while communicating with VirtualCenter.

Figure 44 VM Server Log Viewer

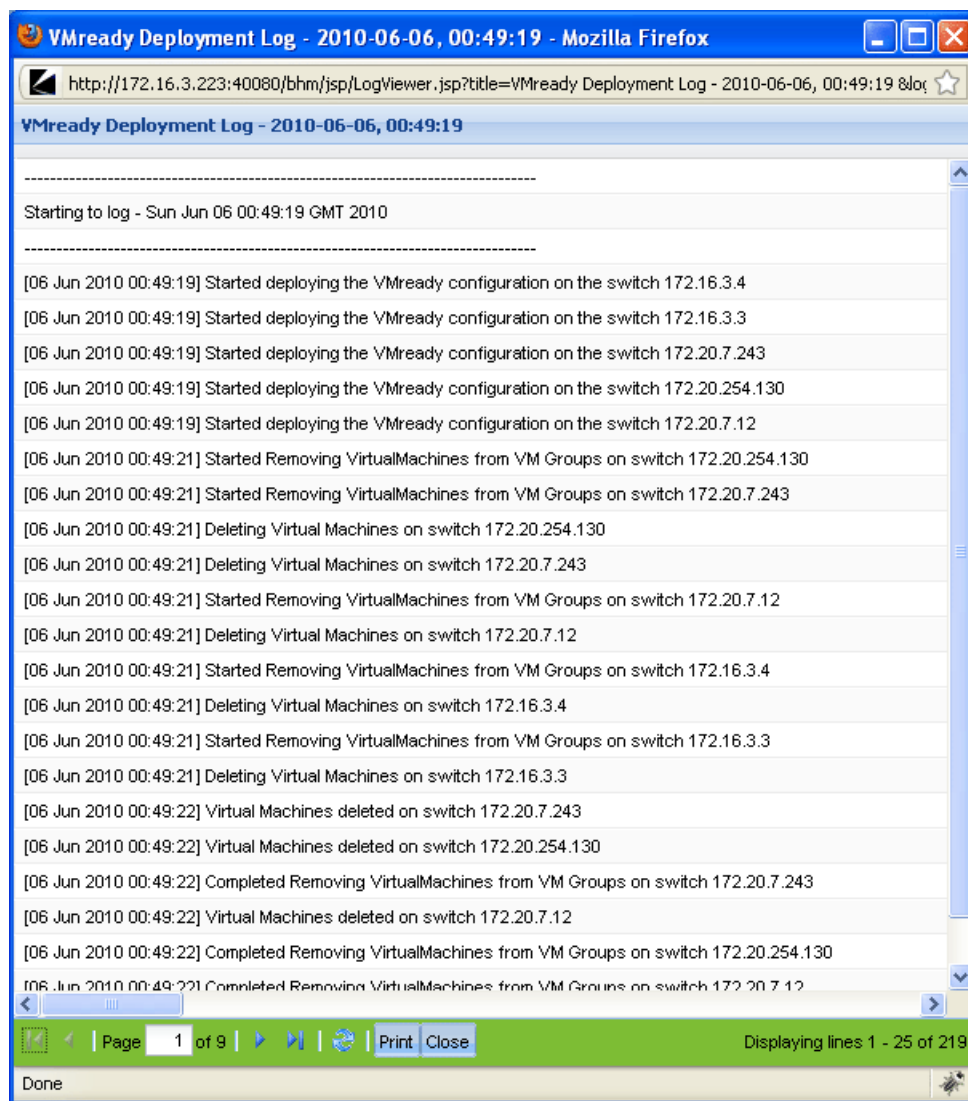
VM Server Log Viewer
Starting to log - Mon Jan 26 09:35:06 PST 2009
[26 Jan 2009 09:35:18] Invalid connection arguments like protocol, port, server address or user credentials
[26 Jan 2009 09:35:18] Failed to initialize vm property collector due to invalid connection arguments like protocol, port, server address or user credentials
[26 Jan 2009 09:44:50] Started vm property collector
[26 Jan 2009 09:44:54] Failed to collect hypervisor properties

Viewing the VMready Deployment Log

This contains logs related to VMAP and VMready configuration deployment initiated from the VMready Across Datacenter wizard.

- **VMAP Log:** Logs details about any VMAP configurations that were deployed on switches from the wizard. **Note:** Each time a VMAP configuration is deployed, the previously stored log is erased.
- **VMready Log:** Logs details about the VMready configuration deployed by the wizard and also provides a means of viewing the snapshot of the configuration deployed.

To view the logs, select the date and time when the particular VMready configuration deployment was initiated and click **View** to view log of operations. See [“VMready Log Viewer” on page 151](#). The configuration that was deployed can be viewed in XML format by clicking **View Deployed Configuration**.

Figure 45 VMready Log Viewer

Advanced Configuration and Tuning

This section provides information about parameters that you can modify in the System Networking Switch Center configuration files. You must connect to the System Networking Switch Center server via Telnet or a similar program. You perform advanced configuration and tuning tasks through a command-line interface.

The configuration files that are described in this section can be found as below:

- The config-substitutions.properties file is under the following directory:
`/opt/ibm/snsc/webserver/var/conf/`
- The rest of the configuration files reside under the following directory:
`/opt/ibm/snsc/conf`

Requirement: You must stop and restart System Networking Switch Center services before any configuration file changes can take effect.

- [“Modifying the log.properties Configuration File” on page 153](#)
- [“Modifying the server_config.properties Configuration File” on page 154](#)
- [“Modifying the backup.properties Configuration File” on page 155](#)
- [“Modifying the config-substitutions.properties Configuration File” on page 156](#)
- [“Modifying the alertseverity.properties Configuration File” on page 157](#)
- [“Modifying the cmi.properties Configuration file” on page 158](#)

Modifying the log.properties Configuration File

The `log.properties` file contains logging-specific properties that you can configure.

Table 21 log.properties file property descriptions

Property Name	Description
TimeStampFormat	This property defines the format of the timestamp used in the log files. To change the timestamp format to different value, see the JDK SimpleDateFormat API document, which provides a list of available formats. Default= <code>dd MMM yyyy HH:mm:ss</code> .
LogFileMaxSizeKB	This parameter defines the maximum log file size in kBytes. If the contents exceed this limit, the file is backed up using a roll number, for example, <code><logfile>.1.log</code> . Default maximum log file size = 1024, which equals 1 MB.
MaxBackupFiles	This parameter defines the maximum number of backup log files that SNSC can store. For example, if this value is ten, then SNSC keeps a maximum of ten backup files. The backup files use the filename format of <code><logfile>.1.log</code> to <code><logfile>.10.log</code> . Ten is the default value for the maximum number of backup files.

Modifying the server_config.properties Configuration File

The `server_conf.properties` file contains System Networking Switch Center server-specific parameters that you can configure.

Table 22 server_conf.properties file property descriptions

Property Name	Description
rmi_port	The <code>rmi_port</code> is the port on which the SNSC server and client exchange information. Default value=40999
cmi_timeout	The <code>cmi_timeout</code> parameter is the timeout, in milliseconds, that SNSC uses to communicate with devices. Default value=5000, which is five seconds.
session_timeout	The <code>session_timeout</code> parameter defines the timeout, in seconds, that SNSC uses to automatically log you out of an inactive browser session when you are connected to SNSC. Default value=57600
snmp_trap_service	When the <code>snmp_trap_service</code> parameter is set to true, SNSC runs the trap listener on the specified trap port. Default value=true
syslog_service	When the <code>syslog_service</code> parameter it is set to true, SNSC runs the syslog listener on the specified syslog port. Default value=true
snmp_trap_port	The <code>snmp_trap_port</code> defines the port on which SNSC listens to receive the traps. The <code>snmp_trap_port</code> only applies if the <code>snmp_trap_service</code> parameter is set to true. Default value=162
syslog_port	The <code>syslog_port</code> parameter defines the port on which SNSC listens to receive the syslog messages. The <code>syslog_port</code> parameter applies only if <code>syslog_service</code> is set to true. Default value=514
Group_operation_status_poll_intr	The polling interval to check the status of group operations like image upgrade or backup that are in progress. Default value = 10s

Modifying the backup.properties Configuration File

The `backup.properties` file contains event backup (DB purge) parameters and Critical Data Backup parameters.

Table 23 backup.properties file property descriptions

Property Name	Description
TimeStampFormat	This parameter defines the format of the timestamp used when SNSC saves purged events in a text file. To change the <code>TimeStampFormat</code> to a different value, see the JDK <code>SimpleDateFormat</code> API document. The API document provides a list of available formats. Default format= <code>ddMMyyyy_HHmmss</code>
DataBackupMaxWaitTime	The maximum time in minutes that Data Backup Operation waits for operation to complete.
DBPurgeDirectory	The directory (NFS or remote mounted) where the purged data files are stored.
DataBackupDirectory	The directory (it could be NFS/Remote mounted) where the data backup file should be stored during data backup operation. Note: This parameter can also be updated using menu Maintenance > Data Backup > Set Data Backup Directory .

Modifying the config-substitutions.properties Configuration File

The config-substitutions.propertiesfile contains System Networking Switch Center Web server configuration parameters that you can modify. The file is installed in the following directory:

```
/opt/ibm/snsc/webserver/var/conf/
```

Table 24 config-substitutions.properties file property descriptions

Property Name	Description
HTTPPort=40080	This parameter defines the HTTP port on which the SNSC Web server listens for HTTP requests. Default value=40080.
HTTPSPort=40443	This parameter defines the HTTPs (SSL) port on which the SNSC Web server listens for HTTPs requests. Default value=40443.

Modifying the alertseverity.properties Configuration File

System Networking Switch Center uses the `alertseverity.properties` file as a reference for assigning severity to generated SNSC Alerts. This property file contains all the alert types generated by System Networking Switch Center, along with severity. If you want to change the default severity, edit this file with the new severity. The severity can be one of the following: CRITICAL, MAJOR, MINOR, WARNING, or INFORMATIONAL.

Modifying the `cmi.properties` Configuration file

System Networking Switch Center uses `cmi.properties` to set the timeout value for handling Table specific responses. You can configure the timeout value to suit the environment depending on the network speed.

How to Manually Set Device Discovery Date

By default, System Networking Switch Center assigns the current date after discovering a device. The discovery date parameter helps you to filter the devices based on date range (see “Discovery Time Range Summary Pane” on page 69). Though System Networking Switch Center assigns the discovery date automatically, but you can override that and specify a different date manually using the following steps:

- 1 Select a switch from the System Networking Switch Center Device List page (see [Figure 9 on page 74](#)).
- 2 Choose **Device > Set Discovery Date**.
- 3 Click the date icon to bring up the date wizard and click the date.
- 4 If Root user is enabled, enter the root password.
- 5 Click **Save**.

You can also set the discovery date on more than one switch at a time using the below steps:

- 1 Select one or more switches from the System Networking Switch Center Device List page (see [Figure 9 on page 74](#)).
- 2 Choose **Group Operations > Set Discovery Date**.
- 3 Click the date icon to bring up the date wizard and click the date.
- 4 If Root user is enabled, enter the root password.
- 5 Click **Save**.

How to Configure Discovery Time Range

The Discovery Time Ranges control how the device counts are shown in Discovery Time Range Summary Page (see [“Discovery Time Range Summary Pane” on page 69](#)) and how the devices are filtered.

- 1** Choose menu **Options > Discovery Time Range Configuration**.
- 2** Change Less Than (<) and Greater Than (>) settings.
- 3** If Root user is enabled, enter the root password.
- 4** Click **Save**.

Viewing Reports

You can view various reports associated with all the discovered switches by choosing the items under the **Reports** menu in System Networking Switch Center (SNSC).

- [“How to View the SNSC Alerts Report” on page 162](#)
- [“How to View the Switch Version Report” on page 164](#)
- [“How to View the Transceiver Information Report” on page 166](#)
- [“How to View the VM Data Center Report” on page 168](#)
- [“How to View the VMready VM Report” on page 170](#)

How to View the SNSC Alerts Report

The SNSC Alerts list is a summary of internal alerts generated by System Networking Switch Center when it detects intra-switch or inter-switch Virtual Machine movements with reference to switches. To view the SNSC Alerts report:

- 1 Click **Reports > SNSC Alerts** (see [Figure 46 on page 162](#)).
- 2 Use the Page text box or associated arrow buttons to navigate through the available pages.
- 3 To view the details of an alert, double-click any alert row or select a row and click **View Details**.
- 4 To delete one or more System Networking Switch Center alerts entries from the System Networking Switch Center database:
 - a Click the box next to Node.
 - b Click **Delete** to remove the selected alerts from the database.
- 5 Click **Close** to return to the System Networking Switch Center home page.

Figure 46 SNSC Alerts Report Window

	IP Address	Time	Severity	Type	Description
<input type="checkbox"/>	192.168.143.6	Wed May 27 13:01...	INFORMATIONAL	Inter-Switch VM Move	VM VM 1 has move...
<input type="checkbox"/>	192.168.143.6	Wed May 27 13:01...	INFORMATIONAL	Inter-Switch VM Move	VM VM 2 has move...
<input type="checkbox"/>	192.168.143.6	Wed May 27 13:01...	INFORMATIONAL	Inter-Switch VM Move	VM VM 3 has move...
<input type="checkbox"/>	192.168.143.6	Wed May 27 13:01...	INFORMATIONAL	Inter-Switch VM Move	VM VM 7 has move...
<input type="checkbox"/>	192.168.143.7	Wed May 27 13:01...	INFORMATIONAL	Inter-Switch VM Move	VM VM 1 has move...
<input type="checkbox"/>	192.168.143.7	Wed May 27 13:01...	INFORMATIONAL	Inter-Switch VM Move	VM VM 3 has move...
<input type="checkbox"/>	192.168.143.7	Wed May 27 13:01...	INFORMATIONAL	Inter-Switch VM Move	VM VM 4 has move...
<input type="checkbox"/>	192.168.144.7	Wed May 27 13:01...	INFORMATIONAL	Intra-Switch VM Move	VM VM 9 has move...

Page 1 of 1 Delete View Details Close Help Displaying 1 - 24 of 24 alerts

Table 25 SNSC Alerts Report field descriptions

Field	Description
IP Address	IP address of the switch that resulted in SNSC Alert
Time	The time that the alert was generated by SNSC.
Severity	The severity of the alert as defined in alertseverity.properties file. See “Advanced Configuration and Tuning” on page 152 for customization.

Table 25 SNSC Alerts Report field descriptions

Field	Description
Type	The alert type
Description	The alert description

Table 26 SNSC Alerts descriptions

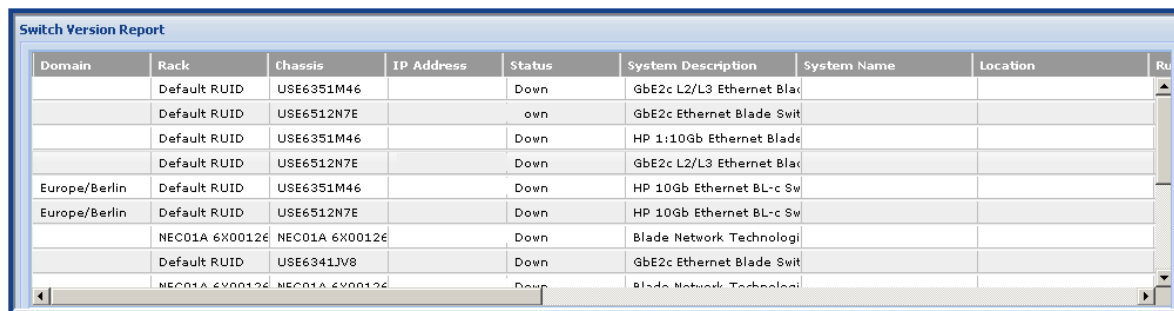
Field	Description
VM <name/MAC address> came online on port <#>	<i>Intra-switch alert</i> When SNSC detects a VM is on a non-zero port that was previously on port 0 of the same switch and not on a non-zero port of another switch.
VM <name/MAC address> came online on port <#> from <switch address>, port <#>	<i>Inter-switch alert</i> When SNSC detects a VM is on a non-zero port on a switch which was previously on a non-zero port of another switch.
VM <name/MAC address> returned to pre-provisioned state from port <#>	<i>Intra-switch alert</i> When SNSC detects a VM is on port 0 that was previously on a non-zero port on the same switch.
VM <name/MAC address> has moved from port <#> to <#>	<i>Intra-switch alert</i> When SNSC detects a VM has moved from one port to another port on the same switch.
VM <name/MAC address> has moved from port <#> to <switch address>, port <#>	<i>Inter-switch alert</i> When SNSC detects a VM has moved from one port to another port on a different switch.

How to View the Switch Version Report

The switch version report is a summary of data about all discovered switches (**Reports > Switch Version Report**) or selected discovered switches (**Group Operations > Switch Version Report**). You can control how the report organizes and presents information (see [“How to Customize Information in Reports” on page 175](#)).

- 1 Click **Reports > Switch Version Report** or **Group Operations > Switch Version Report** (see [Figure 47 on page 164](#)).
- 2 Click **Refresh** to update the version of the report that you are viewing.
- 3 Click **Close** to return to the System Networking Switch Center home page.

Figure 47 Switch Version Report window



The screenshot shows a window titled "Switch Version Report" containing a table with the following columns: Domain, Rack, Chassis, IP Address, Status, System Description, System Name, Location, and Run. The table lists several switches, including those in the "Default RUID" domain and "Europe/Berlin" domain, with various chassis and IP addresses, and their current status (e.g., Down).

Domain	Rack	Chassis	IP Address	Status	System Description	System Name	Location	Run
	Default RUID	USE6351M46		Down	GbE2c L2/L3 Ethernet Blac			
	Default RUID	USE6512N7E		own	GbE2c Ethernet Blade Swit			
	Default RUID	USE6351M46		Down	HP 1:10Gb Ethernet Blade			
	Default RUID	USE6512N7E		Down	GbE2c L2/L3 Ethernet Blac			
Europe/Berlin	Default RUID	USE6351M46		Down	HP 10Gb Ethernet BL-c Sw			
Europe/Berlin	Default RUID	USE6512N7E		Down	HP 10Gb Ethernet BL-c Sw			
	NEC01A 6X00126	NEC01A 6X00126		Down	Blade Network Technologi			
	Default RUID	USE6341JV8		Down	GbE2c Ethernet Blade Swit			
	NEC01A 6X00126	NEC01A 6X00126		Down	Blade Network Technologi			

Table 27 Switch Version Report field descriptions

Field	Description
Domain	Names of all switch domains.
Rack	The Rack name (in the navigation tree) in which the switch is contained
Chassis	The Chassis name (in the navigation tree) in which the switch is contained
IP Address	The IP address of the switch.
Status	Status showing whether the switch is currently up or down.
System Description	Displays the product name of the switch.
System Name	The administrative-assigned name for the switch.
Discovery Date	The date of the switch discovery.
Location	The physical location of the switch.
Image1	The software version of the image stored in the first image storage area.
Image2	The software version of the image stored in the second image storage area.
Boot Version	The software version of the switch boot code.

Table 27 Switch Version Report field descriptions (continued)

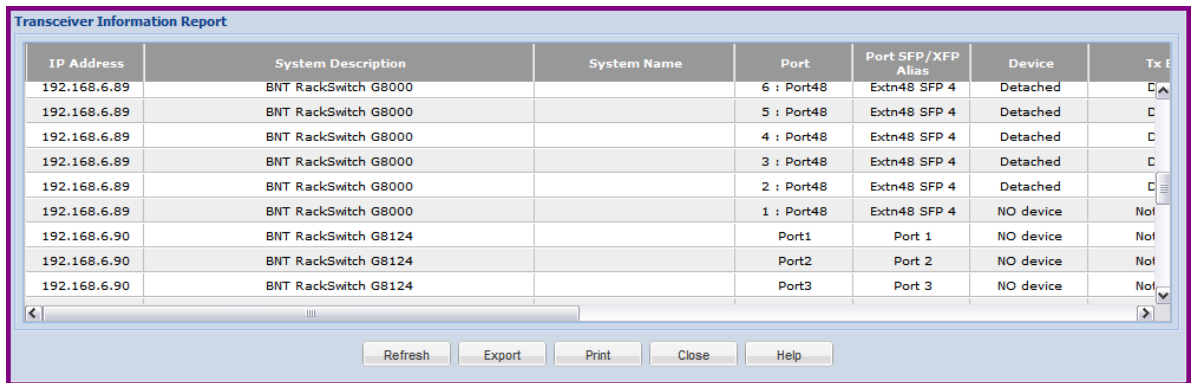
Field	Description
Running Software Version	The version of the software image that is currently running on the system.
Hardware Serial Number	The hardware serial number of the switch.
Config For Next Reset	Gives the configuration to choose for the next switch reset.
Save Pending	Gives information whether any applied changes are not yet saved to FLASH memory on the switch.
Module Bay	The module bay in which the switch is installed.
Manufacture Date	Date the device was manufactured.
Enabled Software Features	Gives information about the enabled software features.
Panic Dump	Gives panic dump status.
Time and Reason for last boot	Gives information about the last reboot cycle. For example, the reason might be power cycle.

How to View the Transceiver Information Report

The transceiver information report is a summary of port transceiver information of switches with 10G ports. To view Transceiver Information report:

- 1 Choose menu **Reports > Transceiver Information Report** to view the report of all discovered switches with 10G ports, or choose menu **Group Operations > Transceiver Information Report** to view the report of the selected switches with 10G ports (see [Figure 48 on page 166](#)).
- 2 Click **Refresh** to update the report that you are viewing.
- 3 Click **Close** to return to the System Networking Switch Center home page.

Figure 48 Transceiver Information Report



The screenshot shows a web-based report titled "Transceiver Information Report". It contains a table with the following columns: IP Address, System Description, System Name, Port, Port SFP/XFP Alias, Device, and Tx Enable. The table lists data for two IP addresses: 192.168.6.89 and 192.168.6.90. For 192.168.6.89, it shows ports 1 through 6, all with "Detached" status. For 192.168.6.90, it shows ports 1 through 3, all with "NO device" status. Below the table are buttons for Refresh, Export, Print, Close, and Help.

IP Address	System Description	System Name	Port	Port SFP/XFP Alias	Device	Tx Enable
192.168.6.89	BNT RackSwitch G8000		6 : Port48	Extn48 SFP 4	Detached	C
192.168.6.89	BNT RackSwitch G8000		5 : Port48	Extn48 SFP 4	Detached	C
192.168.6.89	BNT RackSwitch G8000		4 : Port48	Extn48 SFP 4	Detached	C
192.168.6.89	BNT RackSwitch G8000		3 : Port48	Extn48 SFP 4	Detached	C
192.168.6.89	BNT RackSwitch G8000		2 : Port48	Extn48 SFP 4	Detached	C
192.168.6.89	BNT RackSwitch G8000		1 : Port48	Extn48 SFP 4	NO device	Not
192.168.6.90	BNT RackSwitch G8124		Port1	Port 1	NO device	Not
192.168.6.90	BNT RackSwitch G8124		Port2	Port 2	NO device	Not
192.168.6.90	BNT RackSwitch G8124		Port3	Port 3	NO device	Not

Table 28 Transceiver Information Report field descriptions

Field	Description
IP Address	IP address of the switch.
System Description	Product name of the switch.
System Name	Administrative-assigned name for the switch.
Port	Port index number
Port SFP/XFP Alias	10G SFP/XFP port alias
Device	Device name. "NO device" indicates device/cable is not connected.
Tx Enable	TX-Enable status
Rx Signal	RX-Signal status
Tx Fault	TX-Fault status
Vendor	Vendor name for the device

Table 28 Transceiver Information Report field descriptions (continued)

Field	Description
Serial Number	Serial number of the device
Approval	Approval state for the device: (i) Not Installed (ii) Not Approved (iii) Approved (iv) Detached

How to View the VM Data Center Report

The VM Data Center Report is a list of virtual machines (VMs) that match the following criteria:

- MAC address has been discovered on a server (downlink) port of a switch, and
- MAC address is found in one of the configured VM Management Servers.

At least one VM Management Server must be configured that contains information about the VMs whose MAC addresses will be discovered on the switches.

For RackSwitches (for example, G8124), you must define which ports are server ports in order for the VMs to be reported properly.

To launch the VM Data Center Report, choose menu **Reports > VM Data Center Report** or **Group Operations > VM Data Center Report** (see [Figure 49](#)).

Figure 49 VM Data Center Report

Chassis ID	Bay#	Switch MAC	Switch IP	System Name	Port	VLAN	VM Name	VM IP
2UX8160110	2	00:18:b1:31:a0:00	192.168.6.147	VMTest1	EXT2	5	VM1	172.24.1.10
2UX8160111	3	00:25:03:c6:14:00	192.168.6.148	VMTest2	EXT2	5	VM2	172.24.1.11
2UX8160112	4	fc:cf:62:10:ad:00	192.168.6.149	VMTest3		5	VM3	172.24.1.12

Refresh Export Print Close Help

Table 29 VM Data Center Report field descriptions

Field	Description
Chassis ID	The chassis ID of the switch. This is relevant only in case of stack of switches.
Bay #	The bay number in which the switch is residing. This is relevant only in case of stack of switches.
Switch MAC	MAC Address of the switch on which the VM was discovered.
Switch IP	IP Address of the switch on which the VM was discovered.
System Name	Name of the switch on which the VM was discovered.
Port	Server port on which Virtual Machine was discovered.
VLAN	VLAN to which the Virtual Machine is associated.
VM Name	Name of the discovered virtual machine. This information is retrieved from VMWare vCenter.

Table 29 VM Data Center Report field descriptions

Field	Description
VM IP	IP Address of the Virtual Machine. This information is retrieved from VMWare vCenter.
VM vNIC	vNIC address of the Virtual Machine. This information is retrieved from VMWare vCenter.
PortGroup/VLAN	PortGroup and VLAN of Virtual Machine as configured in the hypervisor. This information is retrieved from VMWare vCenter.
Hypervisor	Name of the Hypervisor on which the VM is running. This information is retrieved from VMWare vCenter.

How to View the VMready VM Report

There are two types of VMready VM Reports, as follows:

- VM Groups: Reports the membership of the Virtual Machine Groups that are configured on each of the discovered VMready capable switches. The VM Groups Report provides a summary of all Virtual Machines discovered by the switches listed in System Networking Switch Center.
- Port Groups: Reports the membership of the Port Groups that are configured on each of the discovered VMready capable switches.

VMready VM Report – VM Groups

To launch the VM Groups Report, choose menu **Reports > VMready VM Report > VM Groups** (see [Figure 50](#)).

Figure 50 VMready VM Report – VM Groups window

Switch IP Address/Name	Group	Chassis UUID	Bay #	Switch MAC	VLAN	Switch #
192.168.130.91	9	G2C1		1a:30:92:a1:b2:91	3089	non-stack
192.168.130.91	25	G2C1		1a:30:92:a1:b2:91	215	non-stack
192.168.130.91	26	G2C1		1a:30:92:a1:b2:91	2140	non-stack
192.168.130.91	27	G2C1		1a:30:92:a1:b2:91	2395	non-stack
192.168.130.91	31	G2C1		1a:30:92:a1:b2:91	1812	non-stack
192.168.130.91	9	G2C1		1a:30:92:a1:b2:91	3767	non-stack
192.168.130.91	18	G2C1		1a:30:92:a1:b2:91	1495	non-stack
192.168.130.91	None	G2C1		1a:30:92:a1:b2:91	3556	non-stack
192.168.130.91	29	G2C1		1a:30:92:a1:b2:91	1485	non-stack
192.168.130.91	13	G2C1		1a:30:92:a1:b2:91	3324	non-stack
192.168.130.91	24	G2C1		1a:30:92:a1:b2:91	3951	non-stack
192.168.130.91	30	G2C1		1a:30:92:a1:b2:91	1681	non-stack
192.168.130.91	15	G2C1		1a:30:92:a1:b2:91	1800	non-stack
192.168.130.91	20	G2C1		1a:30:92:a1:b2:91	1257	non-stack
192.168.130.91	7	G2C1		1a:30:92:a1:b2:91	3588	non-stack
192.168.130.91	19	G2C1		1a:30:92:a1:b2:91	425	non-stack
192.168.130.91	13	G2C1		1a:30:92:a1:b2:91	2936	non-stack
192.168.130.91	18	G2C1		1a:30:92:a1:b2:91	251	non-stack
192.168.130.91	9	G2C1		1a:30:92:a1:b2:91	1518	non-stack
192.168.130.91	28	G2C1		1a:30:92:a1:b2:91	2058	non-stack
192.168.130.111	20	G2C2		2a:30:b2:a1:b2:b1	2951	non-stack
192.168.130.111	18	G2C2		2a:30:b2:a1:b2:b1	1629	non-stack
192.168.130.111	30	G2C2		2a:30:b2:a1:b2:b1	3190	non-stack

Table 30 VMready VM Report – VM Groups field descriptions

Field	Description
Switch IP Address/Name	IP Address/Name of the switch on which the VM was discovered.
Groups	Group number to which the Virtual Machine is associated.
Chassis UUID	The chassis UUID of the switch. This is relevant only in case of stack of switches.
Bay #	The bay number in which the switch is residing. This is relevant only in case of stack of switches.

Table 30 VMready VM Report – VM Groups field descriptions

Field	Description
Switch MAC	MAC address of the switch.
VLAN	VLAN to which the Virtual Machine is associated.
Switch #	Switch number of the corresponding uplink or server ports if the switch is part of a stack. <ul style="list-style-type: none"> • non-stack indicates the switch is not part of a stack. • (Detached) indicates the switch is configured as part of a stack, but is not physically present at the time.
Port	Server port on which Virtual Machine was discovered.
Virtual MAC	MAC address of the Virtual Machine.
VM IP	IP Address of the Virtual Machine.
VM Name	Name of the discovered virtual machine. If the VM Management Server Connector is not configured, this field is blank.
Hypervisor	Name of the Hypervisor on which the VM is running. If the VM Management Server Connector is not configured, this field is blank.

VMready VM Report – Port Groups

To launch the Port Groups Report, choose menu **Reports > VMready VM Report > Port Groups** (see [Figure 51](#)).

Figure 51 VMready VM Report – Port Groups window

Switch IP Address/Name	Group	Chassis UUID	Bay #	Switch MAC	Switch #	Port
192.168.130.91	30	G2C1		1a:30:92:a1:b2: non-stack		EXT1
192.168.130.91	27	G2C1		1a:30:92:a1:b2: non-stack		EXT2, INT11
192.168.130.91	17	G2C1		1a:30:92:a1:b2: non-stack		EXT3, INT9
192.168.130.91	6	G2C1		1a:30:92:a1:b2: non-stack		EXT4, INT4
192.168.130.91	11	G2C1		1a:30:92:a1:b2: non-stack		EXT5
192.168.130.91	8	G2C1		1a:30:92:a1:b2: non-stack		EXT6
192.168.130.91	12	G2C1		1a:30:92:a1:b2: non-stack		EXT7
192.168.130.91	15	G2C1		1a:30:92:a1:b2: non-stack		EXT8
192.168.130.91	21	G2C1		1a:30:92:a1:b2: non-stack		EXT9, INT14
192.168.130.91	32	G2C1		1a:30:92:a1:b2: non-stack		INT1
192.168.130.91	14	G2C1		1a:30:92:a1:b2: non-stack		INT2, INT6
192.168.130.91	28	G2C1		1a:30:92:a1:b2: non-stack		INT3
192.168.130.91	23	G2C1		1a:30:92:a1:b2: non-stack		INT5
192.168.130.91	22	G2C1		1a:30:92:a1:b2: non-stack		INT7
192.168.130.91	24	G2C1		1a:30:92:a1:b2: non-stack		INT8
192.168.130.91	19	G2C1		1a:30:92:a1:b2: non-stack		INT10
192.168.130.91	1	G2C1		1a:30:92:a1:b2: non-stack		INT12
192.168.130.91	26	G2C1		1a:30:92:a1:b2: non-stack		INT13
192.168.130.111	13	G2C2		2a:30:b2:a1:b2: non-stack		EXT1
192.168.130.111	29	G2C2		2a:30:b2:a1:b2: non-stack		EXT2, EXT5, EXT6
192.168.130.111	7	G2C2		2a:30:b2:a1:b2: non-stack		EXT3
192.168.130.111	25	G2C2		2a:30:b2:a1:b2: non-stack		EXT4
192.168.130.111	8	G2C2		2a:30:b2:a1:b2: non-stack		EXT7

Table 31 VMready VM Report — Port Groups field descriptions

Field	Description
Switch IP Address/ Name	IP Address/Name of the switch.
Groups	Group number to which the uplink or server ports are associated.
Chassis UUID	The chassis UUID of the switch. This is relevant only in case of stack of switches.
Bay #	The bay number in which the switch is residing. This is relevant only in case of stack of switches.

Table 31 VMready VM Report — Port Groups field descriptions

Field	Description
Switch MAC	MAC address of the switch.
Switch #	Switch number of the corresponding uplink or server ports if the switch is part of a stack. <ul style="list-style-type: none">• non-stack indicates the switch is not part of a stack.• (Detached) indicates the switch is configured as part of a stack, but is not physically present at the time.
Port	Alias of uplink or server ports.

How to Customize Information in Reports

This section explains how to customize information displayed in the Switch Version Report and Event List window.

- [“Changing the Column Sort Order” on page 176](#)
- [“Displaying or Hiding Columns” on page 177](#)

Changing the Column Sort Order

- 1 Click a column heading.
- 2 Click **Sort Ascending** to sort information in ascending order.
- 3 Click **Sort Descending** to sort information in descending order.

Displaying or Hiding Columns

- 1 Click a column heading.
- 2 Click **Columns**.
- 3 Clear column names to hide one or more columns.
- 4 Click column names to display one or more columns.

Performing Group Operations

You typically perform group operations on multiple switches of the same type.

- [“How to Deploy Switch Image and Configuration on One or More Switches” on page 180](#)
- [“How to Run CLI Commands on One or More Switches” on page 191](#)
- [“How to Collect Data from One or More Switches on Demand” on page 193](#)
- [“How to Retrieve Switch Version Report from One or More Switches” on page 194](#)
- [“How to Retrieve Transceiver Information Report from One or More Switches” on page 195](#)
- [“How to Retrieve VM Data Center Report from One or More Switches” on page 196](#)
- [“How to Invoke Actions on One or More Switches” on page 197](#)
- [“How to Manually Set Discovery Date on One or More Switches” on page 198](#)
- [“How to Add/Remove Notes to/from One or More Switches” on page 199](#)

Restriction: The Concurrent Limit setting (see **Options > General Properties**) controls the number of switches on which System Networking Switch Center (SNSC) can simultaneously perform group operations. For example, if the Concurrent Limit parameter is set to 10, System Networking Switch Center can perform actions on a maximum of 10 switches at the same time. See [“Changing the Default General Properties” on page 101](#) to change the general properties.

How to Deploy Switch Image and Configuration on One or More Switches

You can deploy switch image (firmware) or configuration on one or more selected switches through group operations. In addition to deploying them, you can backup firmware and/or configuration from multiple switches and download panic dump, tech support dump from multiple switches. These group operations can be initiated to take effect immediately or can be configured to occur at a scheduled time.

- [“How to Upgrade Switch Image on One or More Switches” on page 182](#)
- [“How to Backup Switch Image from One or More Switches” on page 184](#)
- [“How to Upgrade Switch Configuration on One or More Switches” on page 185](#)
- [“How to Backup Switch Configuration from One or More Switches” on page 186](#)
- [“How to Download Panic Dump from One or More Switches” on page 187](#)
- [“How to Download Tech Support Dump from One or More Switches” on page 188](#)
- [“How to View Scheduled Jobs” on page 189](#)

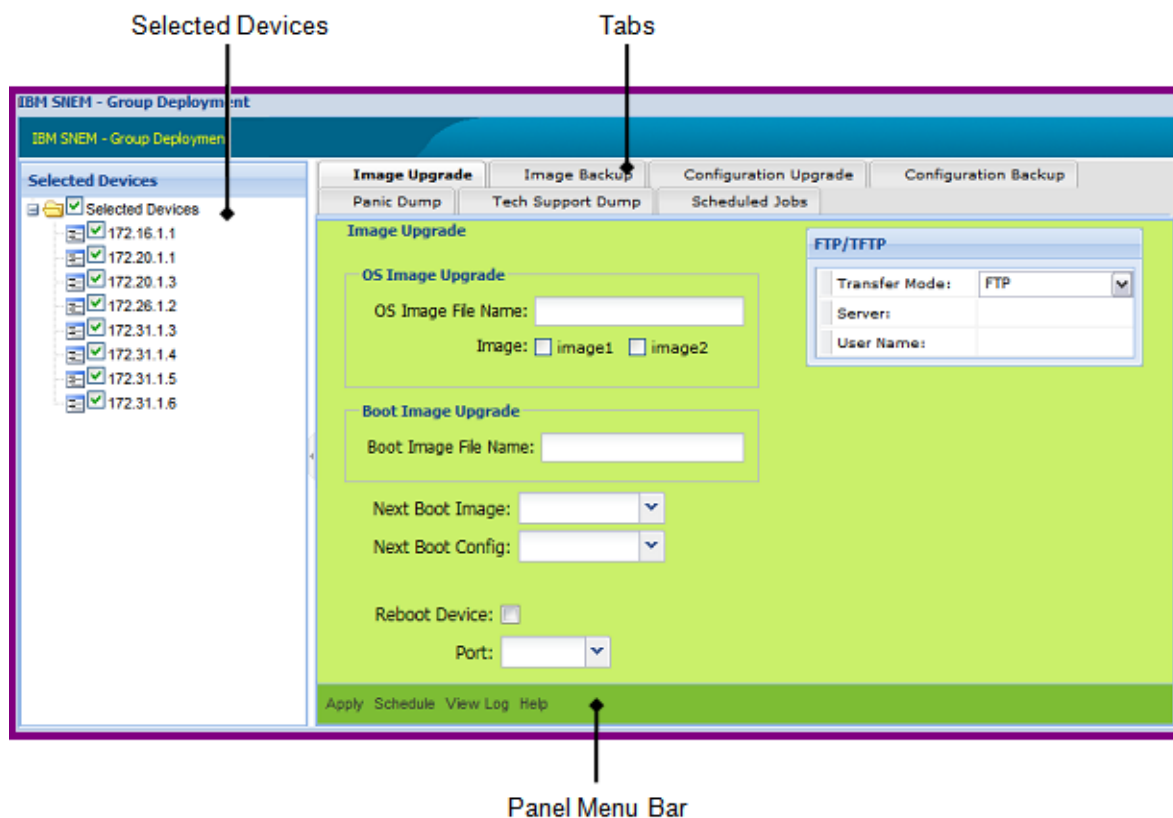
Prerequisite: You must configure an FTP, TFTP, or SFTP server before you can perform most group operations. When you perform a task that involves an FTP, TFTP, or SFTP server, System Networking Switch Center displays information about the server, such as transfer mode and IP address. See [“Configuring FTP/SFTP/TFTP Server Parameters” on page 114](#) to set up the server.

To launch Group Deployment page:

- Select one or more switches in the device list (see [Figure 6 on page 63](#)).
- Choose any one option under menu **Group Operations > Deployment**.

The Group Deployment page (see [Figure 52 on page 181](#)) consists of two framed windows: the Selected Devices frame (left) and the Content Frame (right).

The Selected Devices frame lists the selected switches for which the group operation is going to be performed. It also allows you to deselect any switches from the selection list. The Content frame shows the sub-features in the form of tabs and the corresponding details in a panel along with panel specific menu bar at the bottom.

Figure 52 IBM System Networking Switch Center – Group Deployment Page

How to Upgrade Switch Image on One or More Switches

You can upgrade the switch image (firmware) on one or more switches of the same type by using this feature.

- 1 Log in to System Networking Switch Center as an administrator.
- 2 Select one or more switches of the same type from the System Networking Switch Center Device List page. You can make use of List Device(s) filter in the Device List page to select a particular type of switch.
- 3 Choose menu **Group Operations > Deployment > Image Upgrade** to launch Image Upgrade window.
- 4 Enter the name of the switch OS image in the OS Image File Name field. This switch OS image must reside on the FTP/SFTP/TFTP Server.
 - a Choose `image1` if you want the switch OS image in image 1 slot on the switch.
 - b Choose `image2` if you want the switch OS image in image 2 slot on the switch.
- 5 Enter the name of the switch boot image in Boot Image File Name field. This switch boot image must reside on the FTP/SFTP/TFTP Server.
- 6 (Optional) Choose **Next Boot Image** if you want to load a different OS image during next boot.
- 7 (Optional) Choose **Next Boot Config** if you want to load a different configuration during next boot.
- 8 Choose **Reboot Device** if you want the new image files to take effect. If you select **Reboot Device**, then Image Upgrade operation will reset the switch after upgrading the switch images. This operation interrupts service on the selected switches.
- 9 Choose **Port** through which the operation should be performed. Note that this field may not be available for the selected switch. Please disregard this step if it does not apply to your switch.
- 10 Click **Apply** to immediately copy the image file to the selected switches.
- 11 (Optional) Click **Schedule** to set the parameters required to copy the image file to the selected switches at a later time.
 - a Enter the schedule name of the job.
 - b Select a job type.
 - c Enter the date to start the job.
 - d Enter the hour and minute to start the job.
 - e Click **Schedule**.

- f To review job parameters, choose menu **Group Operations > Deployment > Scheduled Jobs**.

12 Click **View Log** to open a window that displays information about the procedure.

Note: If you are using SFTP as the transfer protocol, you can configure a server port to which your SFTP server is listening.

How to Backup Switch Image from One or More Switches


You can backup the switch image (firmware) from one or more switches by using this feature.

- 1 Log in to System Networking Switch Center as an administrator.
- 2 Select one or more switches from the System Networking Switch Center Device List page.
- 3 Choose menu **Group Operations > Deployment > Image Backup** to launch Image Backup window.
- 4 Select the image type to backup from Image list.
- 5 Choose **Port** through which the operation should be performed. Note that this field may not be available for the selected switch. Please disregard this step if it does not apply to your switch.
- 6 Select the transfer mode – FTP, TFTP, or SFTP.
- 7 Click **Apply** to immediately start the image backup process.
- 8 (Optional) Click **Schedule** to set the parameters required to backup the image file from the selected switches at a later time.
 - a Enter the schedule name of the job.
 - b Select a job type.
 - c Enter the date to start the job.
 - d Enter the hour and minute to start the job.
 - e Click **Schedule**.
 - f To review job parameters, choose menu **Group Operations > Deployment > Scheduled Jobs**.
- 9 Click **View Log** to open a window that displays information about the procedure.

The default image backup file stored on FTP/SFTP/TFTP server is in the following format:

```
<IPAddress>_ddMMMyyyy_HHmms
```

For example, the image backed up from the switch 192.168.1.1 on 7th March 2008 at 23:59:01 hours will be named as follows:

```
192.168.1.1_07Mar2008_235901
```

Note: If you are using SFTP as the transfer protocol, you can configure a server port to which your SFTP server is listening.

How to Upgrade Switch Configuration on One or More Switches

You can upgrade the switch configuration on one or more switches of the same type by using this feature.

- 1 Log in to System Networking Switch Center as an administrator.
- 2 Select one or more switches of the same type from the System Networking Switch Center Device List page. You can make use of List Device(s) filter in the Device List page to select a particular type of switch.
- 3 Choose menu **Group Operations > Deployment > Configuration Upgrade** to launch Configuration Upgrade window.
- 4 Enter the name of the configuration file in Configuration File Name. This configuration file should be residing on the FTP/SFTP/TFTP Server.
- 5 Choose **Port** through which the operation should be performed. Note that this field may not be available for the selected switch. Please disregard this step if it does not apply to your switch.
- 6 Select the transfer mode – FTP, TFTP, or SFTP.
- 7 Click **Apply** to immediately copy the configuration file to the selected switches.
- 8 (Optional) Click **Schedule** to set the parameters required to copy the configuration file to the selected switches at a later time.
 - a Enter the schedule name of the job.
 - b Select a job type.
 - c Enter the date to start the job.
 - d Enter the hour and minute to start the job.
 - e Click **Schedule**.
 - f To review job parameters, choose menu **Group Operations > Deployment > Scheduled Jobs**.
- 9 Click **View Log** to open a window that displays information about the procedure.

Note: If you are using SFTP as the transfer protocol, you can configure a server port to which your SFTP server is listening.

How to Backup Switch Configuration from One or More Switches

You can backup the switch configuration from one or more switches by using this feature.

- 1 Log in to System Networking Switch Center as an administrator.
- 2 Select one or more switches from the System Networking Switch Center Device List page.
- 3 Choose menu **Group Operations > Deployment > Configuration Backup** to launch Configuration Backup window.
- 4 Choose **Port** through which the operation should be performed. Note that this field may not be available for the selected switch. Please disregard this step if it does not apply to your switch.
- 5 Select the transfer mode – FTP, TFTP, or SFTP.
- 6 Click **Apply** to immediately start the configuration backup process.
- 7 (Optional) Click **Schedule** to set the parameters required to backup the configuration from the selected switches at a later time.
 - a Enter the schedule name of the job.
 - b Select a job type.
 - c Enter the date to start the job.
 - d Enter the hour and minute to start the job.
 - e Click **Schedule**.
 - f To review job parameters, choose menu **Group Operations > Deployment > Scheduled Jobs**.
- 8 Click **View Log** to open a window that displays information about the procedure.

The configuration file that you backed up is stored on FTP/SFTP/TFTP server in the following format:

```
config_<IPAddress>_ddMMMyyyy_HHmmsstxt
```

For example, the configuration file backed up from the switch 192.168.1.1 on 7th March 2008 at 23:59:01 hours will be named as follows:

```
config_192.168.1.1_07Mar2008_235901.txt
```

Note: If you are using SFTP as the transfer protocol, you can configure a server port to which your SFTP server is listening.

How to Download Panic Dump from One or More Switches

When a switch encounters a fatal condition during runtime, it captures the current hardware and software state information into a panic dump. You can download the panic dump from one or more switches by using this feature.

- 1 Log in to System Networking Switch Center as an administrator.
- 2 Select one or more switches from the System Networking Switch Center Device List page.
- 3 Choose menu **Group Operations > Deployment > Panic Dump** to launch Panic Dump window.
- 4 Choose **Port** through which the operation should be performed. Note that this field may not be available for the selected switch. Please disregard this step if it does not apply to your switch.
- 5 Select the transfer mode – FTP, TFTP, or SFTP.
- 6 Click **Apply** to immediately start downloading the panic dump.
- 7 (Optional) Click **Schedule** to set the parameters required to download the panic dump from the selected switches at a later time.
 - a Enter the schedule name of the job.
 - b Select a job type.
 - c Enter the date to start the job.
 - d Enter the hour and minute to start the job.
 - e Click **Schedule**.
 - f To review job parameters, choose menu **Group Operations > Deployment > Scheduled Jobs**.
- 8 Click **View Log** to open a window that displays information about the procedure.

The panic dump is stored on FTP/SFTP/TFTP server in the following format:

```
panicdump_<IPAddress>_ddMMMyyyy_HHmms
```

For example, the panic dump saved from the switch 192.168.1.1 on 7th March 2008 at 23:59:01 hours will be named as follows:

```
panicdump_192.168.1.1_07Mar2008_235901
```

Note: If you are using SFTP as the transfer protocol, you can configure a server port to which your SFTP server is listening.

How to Download Tech Support Dump from One or More Switches

You can download the tech support dump from one or more switches by using this feature.

- 1 Log in to System Networking Switch Center as an administrator.
- 2 Select one or more switches from the System Networking Switch Center Device List page.
- 3 Choose menu **Group Operations > Deployment > Tech Support Dump** to launch Tech Support Dump window.
- 4 Choose **Port** through which the operation should be performed. Note that this field may not be available for the selected switch. Please disregard this step if it does not apply to your switch.
- 5 Select the transfer mode – FTP, TFTP, or SFTP.
- 6 Click **Apply** to immediately start downloading the tech support dump.
- 7 (Optional) Click **Schedule** to set the parameters required to download the tech support dump from the selected switches at a later time.
 - a Enter the schedule name of the job.
 - b Select a job type.
 - c Enter the date to start the job.
 - d Enter the hour and minute to start the job.
 - e Click **Schedule**.
 - f To review job parameters, choose menu **Group Operations > Deployment > Scheduled Jobs**.
- 8 Click **View Log** to open a window that displays information about the procedure.

The tech support dump is stored on FTP/SFTP/TFTP server in the following format:

```
tsdump_<IPAddress>_ddMMMyyy_HHmss
```

For example, the tech support dump saved from the switch 192.168.1.1 on 7th March 2008 at 23:59:01 hours will be named as follows:

```
tsdump_192.168.1.1_07Mar2008_235901
```

Note: If you are using SFTP as the transfer protocol, you can configure a server port to which your SFTP server is listening.

How to View Scheduled Jobs

You can view and refresh the list of scheduled jobs and you can cancel one or more scheduled jobs. You can see information about the job type, scheduled start date, ID of the person who scheduled the job and the job name.

- 1 Choose menu **Group Operations > Deployment > Scheduled Jobs** (see [Figure 53 on page 189](#)). The window displays all currently scheduled jobs.
- 2 Click **View Details** to bring up the window showing the details of the selected scheduled job.
- 3 To cancel one or more jobs:
 - a Select the job or jobs that you want to cancel.
 - b Click **Cancel Jobs**.
 - c Click **Refresh** to verify that the scheduled jobs list does not displayed the cancelled jobs.

Figure 53 Scheduled Jobs pane

Image Upgrade	Image Backup	Configuration Upgrade	Configuration Backup	Panic Dump	
Tech Support Dump	Scheduled Jobs				
Schedule Name	Operation Type	Selected Device(s)	Job Type	Date	User
image_upgrade	Image Upgrade	192.168.6.81...	One-time	Sat Mar 19 00:00	admin
config_upgrade	Configuration Upgrade	192.168.6.81...	One-time	Sat Mar 19 00:00	admin
Refresh View Details Cancel Jobs Help					

Table 32 Scheduled Jobs field descriptions

Field	Description
Schedule Name	Name of the scheduled job as created by the user.
Operation Type	The operation type, such as Image Upgrade, Image Backup, Configuration Upgrade, that is going to be performed by the scheduled job.
Selected Devices	The list of selected devices. Due to limited space, ellipsis is employed in case of multiple devices. But the list of all the selected devices can be seen by clicking View Details to open a window showing the details of the selected scheduled job.

Table 32 Scheduled Jobs field descriptions

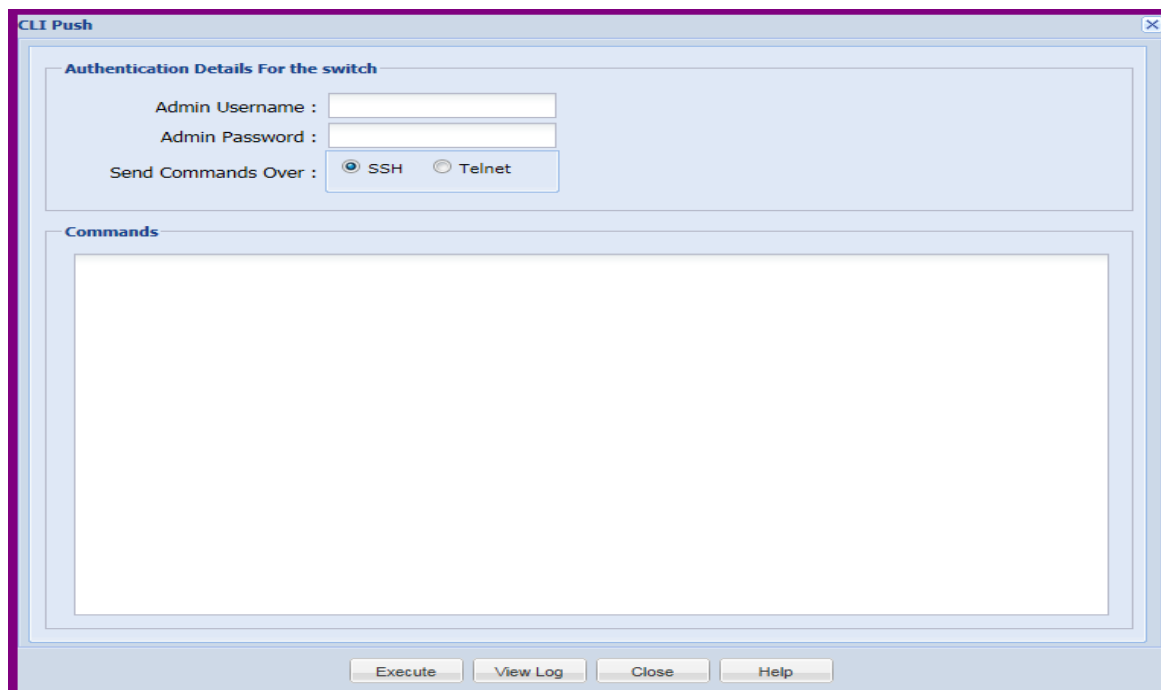
Field	Description
Job Type	The type of the job. It can be: <ul style="list-style-type: none">• One-time – Meaning it is executed once as scheduled• Recurrent – Recurring job occurring at regular interval
Date	The scheduled date and time information. In case of Recurrent type of jobs, a different tag such as Daily, Weekly and Monthly is used along with the time and/or date.
User	User who created the scheduled job.

How to Run CLI Commands on One or More Switches

Using this facility, you can make changes to the switch configuration on multiple switches by executing one or more CLI commands. When you perform this operation, you must save the changes so that they are retained beyond the next time the switch is reset. When you execute the save command, your new configuration changes are placed in the active configuration block. The previous configuration is copied into the backup configuration block.

Note: Make sure that you enter complete commands, so no prompting for further user input is required.

- 1 Log in to System Networking Switch Center as an administrator.
- 2 Select one or more switches of the same type from the System Networking Switch Center Device List page. You can make use of List Device(s) filter in the Device List page to select a particular type of switch.
- 3 Choose menu **Group Operations > CLI Push** to launch the window (see [Figure 54 on page 192](#)).
- 4 Enter the Admin Username and Password of the switch.
- 5 Choose the protocol (SSH or Telnet) over which the CLI commands should be sent.
- 6 Enter one or more CLI commands.
- 7 (Optional) Click **View Log** to open the window to view the messages logged while performing CLI Push operation.
- 8 Click **Execute** to run the CLI commands on the selected switches.

Figure 54 CLI Push window

The image shows a software window titled "CLI Push" with a standard Windows-style title bar (minimize, maximize, close buttons). The window is divided into two main sections. The top section, titled "Authentication Details For the switch", contains three input fields: "Admin Username :", "Admin Password :", and "Send Commands Over :". The "Send Commands Over :" field has two radio buttons, "SSH" (which is selected) and "Telnet". The bottom section, titled "Commands", is a large, empty rectangular area for entering commands. At the bottom of the window, there is a horizontal bar containing four buttons: "Execute", "View Log", "Close", and "Help".

CLI Push

Authentication Details For the switch

Admin Username :

Admin Password :

Send Commands Over : ☒ SSH ☐ Telnet

Commands

How to Collect Data from One or More Switches on Demand

You can asynchronously refresh the data of the selected switches.

- 1 Log in to System Networking Switch Center as an administrator.
- 2 Select one or more switches from the System Networking Switch Center Device List page.
- 3 Choose menu **Group Operations > Collect Data From Device**.

How to Retrieve Switch Version Report from One or More Switches

You can retrieve the switch version report from one or more switches.

- 1 Log in to System Networking Switch Center as an administrator.
- 2 Select one or more switches from the System Networking Switch Center Device List page.
- 3 Choose menu **Group Operations > Switch Version Report**.
- 4 For more information, refer to [“How to View the Switch Version Report” on page 164](#).

How to Retrieve Transceiver Information Report from One or More Switches

You can retrieve the Transceiver Information report from one or more switches.

- 1 Log in to System Networking Switch Center as an administrator.
- 2 Select one or more switches from the System Networking Switch Center Device List page.
- 3 Choose menu **Group Operations > Transceiver Information Report**.
- 4 For more information, refer to [“How to View the Transceiver Information Report” on page 166](#).

How to Retrieve VM Data Center Report from One or More Switches

You can retrieve the VM Data Center report from one or more switches.

- 1 Log in to System Networking Switch Center as an administrator.
- 2 Select one or more switches from the System Networking Switch Center Device List page.
- 3 Choose menu **Group Operations > VM Data Center Report**.
- 4 For more information, refer to [“How to View the VM Data Center Report” on page 168](#).

How to Invoke Actions on One or More Switches

You can use this facility to invoke action commands such as **Apply**, **Save** on one or more switches.

- 1 Log in to System Networking Switch Center as an administrator.
- 2 Select one or more switches from the System Networking Switch Center Device List page.
- 3 To apply any pending configuration changes on the selected switches:
 - a Choose **Group Operations > Group Actions > Apply**.
 - b Click **Yes** to confirm that you want to apply the configuration on the selected switch(es).
- 4 To save the current configuration to the flash memory on the selected switches:
 - a Choose **Group Operations > Group Actions > Save**.
 - b Click **Yes** to confirm that you want to save the configuration on the selected switch(es).
- 5 To reboot the selected switches:
 - a Choose **Group Operations > Group Actions > Reboot Switch**.
 - b Click **Yes** to confirm that you want to reboot the selected switch(es).
- 6 To delete the selected switch entries from System Networking Switch Center device list:
 - a Choose **Group Operations > Group Actions > Delete**.
 - b Click **Yes** to confirm that you want to delete the selected switch(es).

Note: While invoking **Delete** operation, if you select one or members of a stack of switches, the entire stack will be deleted.

How to Manually Set Discovery Date on One or More Switches

You can manually set the discovery date on one or more switches.

- 1 Log in to System Networking Switch Center as an administrator.
- 2 Select one or more switches from the System Networking Switch Center Device List page.
- 3 Choose menu **Group Operations > Set Discovery Date**.
- 4 Click the date icon to open the Date wizard and click the date.
- 5 If Root user is enabled, enter the root password.
- 6 Click **Save**.

How to Add/Remove Notes to/from One or More Switches

You can add notes or remove notes from on one or more switches.

- 1** Log in to System Networking Switch Center as any valid user.
- 2** Select one or more switches from the System Networking Switch Center Device List page.
- 3** To add Notes:
 - a** Choose menu **Group Operations > Notes > Add**.
 - b** Type the text that you want to add.
 - c** Click **OK**.
- 4** To remove Notes:
 - a** Choose menu **Group Operations > Notes > Remove**.
 - b** Click **Yes** in the confirmation dialog to remove notes.

Monitoring a Switch

The monitoring feature provides real-time information and statistics about various components of a selected switch. The monitoring facility is provided as part of the Device Console page in (see [Figure 11 on page 88](#)).

Choose menu **Options > Data Collection Configuration** to view or change the Performance Statistics interval parameter. The parameter determines how often performance statistics are collected from a device and written to the System Networking Switch Center (SNSC) database. Performance Statistics collection only occurs on a device when a user opens a monitoring page for that device. If no users have selected a monitor page, no performance statistics collection occurs on any discovered device.

Choose menu **Options > Refresh Configuration** to view or change the interval that determines how often the user interface is updated with new performance statistics from the database.

- [“How to Monitor the Switch” on page 203](#)
- [“How to Modify a Statistical Monitoring Page” on page 206](#)
- [“How to View Switch Summary” on page 209](#)
- [“How to Monitor Switch Statistics” on page 217](#)
- [“How to Monitor a Port” on page 231](#)
- [“How to Monitor Bridge Statistics” on page 246](#)
- [“How to Monitor LLDP Information” on page 253](#)
- [“How to Monitor Failover Information” on page 257](#)
- [“How to Monitor vLAG Information” on page 262](#)
- [“How to Monitor Hotlinks Statistics” on page 268](#)
- [“How to Monitor 802.1x/p Information” on page 272](#)
- [“How to Monitor IP Routing” on page 278](#)
- [“How to Monitor BGP Routing” on page 297](#)
- [“How to Monitor RIP Routing” on page 301](#)
- [“How to Monitor OSPF Routing” on page 304](#)
- [“How to Monitor IGMP Routing” on page 326](#)
- [“How to Monitor Virtual Routing” on page 330](#)
- [“How to Monitor Access Control Lists” on page 333](#)
- [“How to Monitor Fiber Channel over Ethernet \(FCoE\)” on page 338](#)
- [“How to Monitor Virtualization” on page 347](#)
- [“How to Monitor Edge Virtual Bridging \(EVB\)” on page 350](#)
- [“How to Monitor Unified Fabric Port Information” on page 356](#)
- [“How to Monitor iSwitch Information” on page 363](#)
- [“How to Launch a Chart” on page 366](#)
- [“How to Export a Statistical Summary” on page 368](#)
- [“How to Print a Statistical Summary” on page 370](#)

How to Monitor the Switch

You can launch **Device Console – Monitoring** page by choosing one of the following ways after you log in to System Networking Switch Center:

- 1 Log in to System Networking Switch Center.
- 2 Launch Device Console page. You can launch this page using one of the following approaches:
 - a Select a switch from the System Networking Switch Center Home page (see [Figure 6 on page 63](#)) and choose menu **Device > Monitor**.
 - b Click the IP address link of the switch you want to manage in device list table in the Home page.
 - c In Home page's Go To: text field, enter the IP address of the switch you want to manage and click the **Search** (Magnifying Glass) icon.
- 3 Select the category from Monitor's tab in the left frame.

When you select a category, it results in the display of tab associated content pane. For example, if you select Summary, the content pane shows the following sub-category in the form of tabs:

- Health Status
- Information
- Port Status
- Port Summary

You can select one of the sub-category tabs to view the specific details.

Using the Monitoring Buttons

Table 33 Button descriptions

Button	Description
Refresh	Statistics are refreshed automatically on a regular basis. Click Refresh to display updated values between the regular refresh intervals. Choose menu Options > Refresh Configuration to change the refresh intervals.
Export	You can export monitoring statistics to a spreadsheet in CSV (comma separated value) format. Choose menu Export > Save to create a .csv file that you can open in Microsoft Excel. See “How to Export a Statistical Summary” on page 368 for more information.
Print	Click to send the statistics to the printer. See “How to Print a Statistical Summary” on page 370 for more information.
Chart	This button is available for all statistics related pages, enabling you to launch a chart and plot values in real-time. See “How to Launch a Chart” on page 366 for more information.
Help	Click to launch context-sensitive help for the page that you are viewing.
Port	This button is only available when you monitor ports. Click to change the port that is being monitored. See “How to Monitor a Port” on page 231 for more information.
Clear Counter	Select this option to clear the counter values only on the user interface.
Clear Statistics	Select this option to clear the statistics on the switch and reset them to zero.

About Various Monitor Tabs

Some **Device Console > Monitor** tabs might not be available for the selected switch. Please disregard the corresponding information if it does not apply to your switch.

How to Modify a Statistical Monitoring Page

You can customize information displayed by the monitoring pages.

- [“Changing the Column Sort Order” on page 207](#)
- [“Displaying or Hiding Columns” on page 208](#)

Changing the Column Sort Order

- 1 Click a column heading.
- 2 Click **Sort Ascending** to sort information in ascending order.
- 3 Click **Sort Descending** to sort information in descending order.

Displaying or Hiding Columns

- 1 Click a column heading.
- 2 Click **Columns**.
- 3 Clear column names to hide one or more columns.
- 4 Click column names to display one or more columns.

How to View Switch Summary

Select Monitor's **Summary** category to view Switch Summary information. This section covers the following switch summary topics:

- [“Viewing Health Status” on page 210](#)
- [“Viewing Information” on page 211](#)
- [“Viewing Port Status” on page 212](#)
- [“Viewing Port Summary” on page 214](#)
- [“Viewing Events” on page 215](#)
- [“Viewing Syslog” on page 216](#)

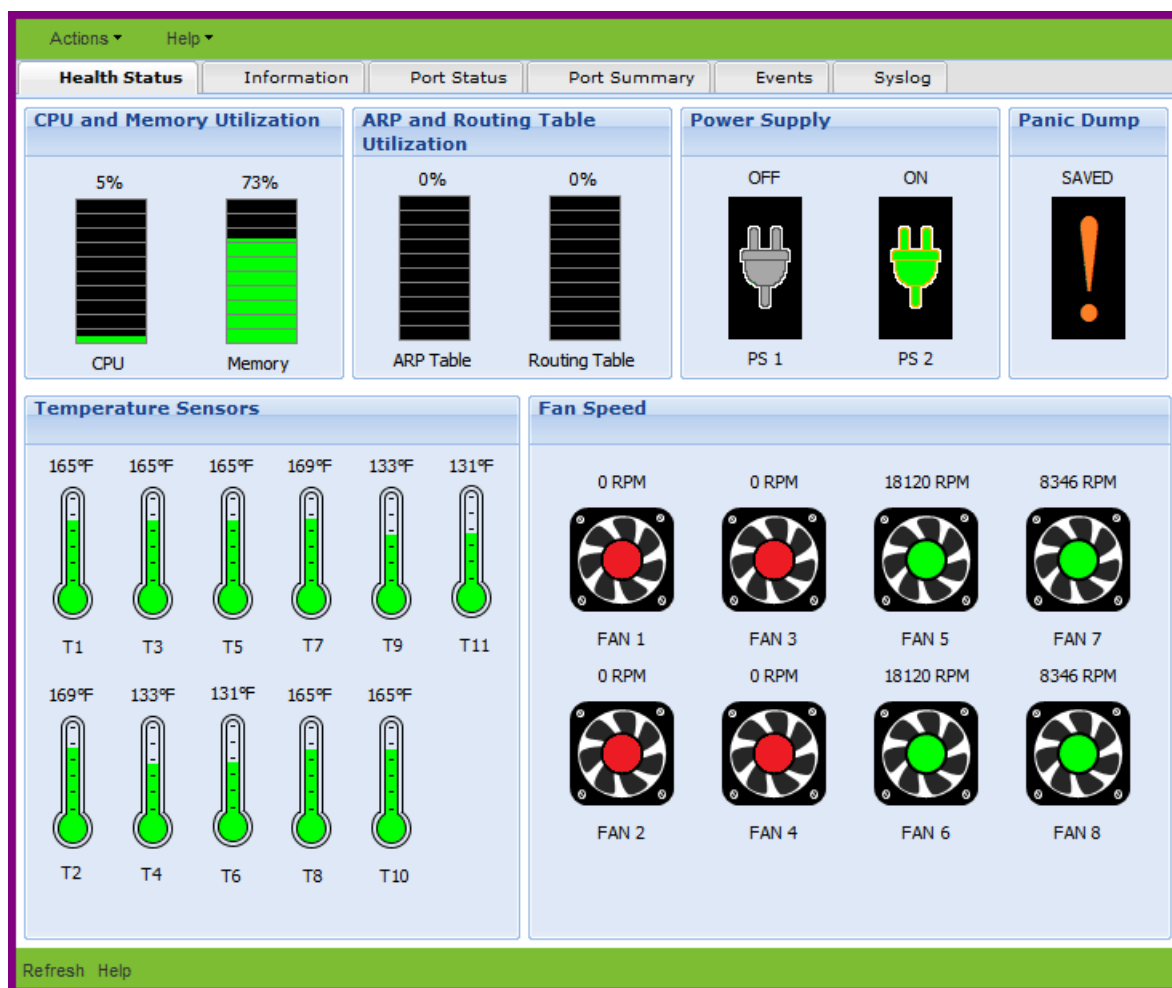
Viewing Health Status

Device Console > Monitor > Summary > Health Status

The Health Status page pictorially shows CPU and Memory Utilization, ARP and Routing Table Utilization, Power Supply Status, Panic Dump Status, Temperature Sensors reading and Fan Speed (see [Figure 55 on page 210](#)).

Note: The utilization, power supply status, temperature sensors and fan speed might not be available for the selected switch. Please disregard this information if it does not apply to your switch.

Figure 55 Health Status Window



Viewing Information

Device Console > Monitor > Summary > Information

Note: This tab or some of its fields might not be available for the selected switch. Please disregard this information if it does not apply to your switch.

Table 34 Switch Information field descriptions

Field	Description
System Description	Displays the product name of the switch.
MAC Address	MAC address of the switch.
System Up Since	Displays the date and time when the switch was last booted.
Location	The physical location of the node, such as telephone closet, third floor.
Contact	Information about the contact person for this managed node.
Boot Code Version	The software version of the switch boot code.
Image 1 Software Version	The software version of the image stored in the first image storage area.
Image 2 Software Version	The software version of the image stored in the second image storage area.
Current Image	The software image that is active (image1 or image2).
Current Config	The current configuration block (active, backup, factory).
Primary Server Key	The NTP Authentication primary server key.
Secondary Server Key	The NTP Authentication secondary server key.
NTP Authentication State	The NTP Authentication state. A value of 1 means Enabled; a value of 0 means Disabled.

Viewing Port Status

Device Console > Monitor > Summary > Port Status

The Port Status displays the state, speed and transmit and receive utilization corresponding to all the ports of the selected switch (see [Figure 56 on page 212](#)).

Figure 56 Port Status Window

Actions ▾ Help ▾

Health Status	Information	Port Status	Port Summary	Events	Syslog
Port Name	Port State	Speed	Transmit Utilization(%)	Receive Utilization(%)	
Downlink1	down	100 Mb	<div><div></div></div> 0%	<div><div></div></div> 0%	
Downlink2	down	100 Mb	<div><div></div></div> 0%	<div><div></div></div> 0%	
Downlink3	down	100 Mb	<div><div></div></div> 0%	<div><div></div></div> 0%	
Downlink4	inoperative	1000 Mb	<div><div></div></div> 0%	<div><div></div></div> 0%	
Downlink5	up	1000 Mb	<div><div></div></div> 51%	<div><div></div></div> 72%	
Downlink6	disabled	any	<div><div></div></div> 0%	<div><div></div></div> 0%	
Downlink7	down	100 Mb	<div><div></div></div> 0%	<div><div></div></div> 0%	
Downlink8	inoperative	10000 Mb	<div><div></div></div> 0%	<div><div></div></div> 0%	
Downlink9	inoperative	100 Mb	<div><div></div></div> 0%	<div><div></div></div> 0%	
Downlink10	down	10000 Mb	<div><div></div></div> 0%	<div><div></div></div> 0%	
Downlink11	down	10 Mb	<div><div></div></div> 0%	<div><div></div></div> 0%	
Downlink12	disabled	10 Mb	<div><div></div></div> 0%	<div><div></div></div> 0%	
Downlink13	up	10000 Mb	<div><div></div></div> 24%	<div><div></div></div> 22%	
Downlink14	disabled	100 Mb	<div><div></div></div> 0%	<div><div></div></div> 0%	
Downlink15	down	1000 Mb	<div><div></div></div> 0%	<div><div></div></div> 0%	
Downlink16	disabled	10000 Mb	<div><div></div></div> 0%	<div><div></div></div> 0%	
Xconnect1	disabled	10 Mb	<div><div></div></div> 0%	<div><div></div></div> 0%	
Mgmt	disabled	10 Mb	<div><div></div></div> 0%	<div><div></div></div> 0%	
Uplink1	inoperative	any	<div><div></div></div> 0%	<div><div></div></div> 0%	

Refresh Export Print Chart Transmit Utilization(%) ▾ Help

Table 35 Port Status field descriptions

Field	Description
Port Name	The physical port of the switch
Port State	The port status

Table 35 Port Status field descriptions (continued)

Field	Description
Speed	The port speed
Transmit Utilization (%)	Transmission utilization in percentage (number of bytes sent out per speed)
Receive Utilization (%)	Receive utilization in percentage (number of bytes taken in per speed)

Viewing Port Summary

Device Console > Monitor > Summary > *Port Summary*

Table 36 Port Summary field descriptions

Field	Description
Port	Displays the port number. Note: The value will be in the following format if switch is connected to a stack: <Switch#> : <Port#/Port Alias>
Port Name	The port name defined by the administrator.
Speed	Displays the link speed.
Port State	Displays the current enabled or disabled value for the port link.
VLAN	A virtual local area network.
Tag PVID	Displays state of VLAN tag persistence. The default value is enabled, or "tagged". When disabled, or untagged, the VLAN tag is removed from packets whose VLAN tag matches the port PVID. The default value is enabled.
PVID	Displays the default VLAN number that is used to forward frames that are not VLAN tagged. The default number is 1.

Viewing Events

Device Console > Monitor > Summary > *Events*

Table 37 Events field descriptions

Field	Description
Node	IP address of the device that sent the event.
DB Time	The time that the event was received at the server and placed into the SNSC database.
Severity	The severity of the trap as defined in trapseverity.properties file. See “Advanced Configuration and Tuning” on page 152 for customization information.
Type	The trap type, which is included in the event from the device. The type is defined by the device.
Description	The text that was included in the event from the sending device.

Note 1: You can remove events from the System Networking Switch Center database by selecting the event(s) and by clicking **Delete**.

Note 2: You can view the details of an event including the SNMP variable bindings either by double-clicking any event row or by selecting a row and clicking **View Details**.

Viewing Syslog

Device Console > Monitor > Summary > Syslog

Table 38 Syslog field descriptions

Field	Description
Node	IP address of the device that sent the message.
Node Time	The time the message was generated by the device that sent it.
DB Time	The time that the message was received at the server and placed into the SNSC database.
Severity	Severity level, as follows: EMERG - indicates the system is unusable. ALERT - indicates action should be taken immediately. CRIT - indicates critical conditions. ERR - indicates error conditions or eroded operations. WARNING - indicates warning conditions. NOTICE - indicates a normal but significant condition. INFO - indicates an information message. DEBUG - indicates a debug-level message.
Description	The text that was included in the event from the sending device.

Note: To remove syslog messages from the System Networking Switch Center database, select the message(s) and click **Delete**.

Note: To view the details of a Syslog message, either double-click any event row or select a row and click **View Details**.

How to Monitor Switch Statistics

Select Monitor's **Switch** category to monitor Switch Statistics. This section covers the following switch statistics topics:

- [“Monitoring SNMP Statistics” on page 218](#)
- [“Viewing Information Summary” on page 220](#)
- [“Monitoring Packet Statistics” on page 221](#)
- [“Monitoring MP CPU Statistics” on page 222](#)
- [“Monitoring STP Statistics” on page 223](#)
- [“Monitoring UFD Statistics” on page 224](#)
- [“Monitoring UFD Information” on page 225](#)
- [“Monitoring NTP Statistics” on page 226](#)
- [“Monitoring Trunk Groups” on page 227](#)
- [“Monitoring Trunk Group Ports” on page 228](#)
- [“Monitoring TACACS+ Authentication Statistics” on page 229](#)

Note: Some of the monitor pages display Absolute Value, Average/sec, Minimum/sec, Maximum/sec and LastVal/sec. The following table describes how those values are calculated.

Table 39 Statistics field descriptions

Field	Description
AbsoluteValue	The current value retrieved from the device.
Average/sec	The average value calculated over time.
Minimum/sec	<p>The value is calculated over time using one of the following formula:</p> <ul style="list-style-type: none"> • $\text{AbsoluteValue} / \langle \text{polling interval} \rangle$ in case of Counter type variables. • $(\text{AbsoluteValue} - \text{Previous value}) / \langle \text{polling interval} \rangle$ in case of Integer type variables. <p>However, the table value is updated only if the new Minimum/sec value is less than the previous Minimum/sec.</p>
Maximum/sec	<p>The value is calculated over time using one of the following formula:</p> <ul style="list-style-type: none"> • $\text{AbsoluteValue} / \langle \text{polling interval} \rangle$ in case of Counter type variables. • $(\text{AbsoluteValue} - \text{Previous value}) / \langle \text{polling interval} \rangle$ in case of Integer type variables. <p>However, the table value is updated only if the new Maximum/sec value is greater than the previous Maximum/sec.</p>
LastVal/sec	<p>The value is calculated over time using one of the following formula:</p> <ul style="list-style-type: none"> • $\text{AbsoluteValue} / \langle \text{polling interval} \rangle$ in case of Counter type variables. • $(\text{AbsoluteValue} - \text{Previous value}) / \langle \text{polling interval} \rangle$ in case of Integer type variables.

Monitoring SNMP Statistics

Device Console > Monitor > Switch > *SNMP Statistics*

Table 40 SNMP Statistics field descriptions

Field	Description
Packets In	The number of messages delivered to the SNMP switch from the transport service.
Packets Out	The number of SNMP Messages passed from the SNMP switch to the transport service.
Packets Using Unsupported SNMP Version	The number of SNMP messages that were received for an unsupported SNMP version.
Packets with Unknown Community String	The number of SNMP messages received that used an unknown SNMP community name.
Packets with Wrong Community String	The number of SNMP messages that represented an SNMP operation that was not allowed by the SNMP community named in the message.
ASN1 Decode Errors	The number of Abstract Syntax Notation One (ASN.1) or BER errors that occurred while the SNMP was decoding received SNMP messages. Note: OSI's method of specifying abstract objects is called ASN.1 (Abstract Syntax Notation One, defined in X.208), and one set of rules for representing such objects as strings of ones and zeros is called the BER (Basic Encoding Rules, defined in X.209). ASN.1 is a flexible notation that lets you define a variety of data types, from simple types such as integers and bit strings to structured types such as sets and sequences. BER describes how to represent or encode values of each ASN.1 type as a string of eight-bit octets.
Too Big Errors In	The number of SNMP PDUs that were delivered to the SNMP entity when Too Big Errors In occurred
No Such Name Errors In	The number of SNMP PDUs that were delivered to the SNMP entity when the No Such Names In error occurred.
Bad Value Errors In	The number of SNMP PDUs that were delivered to the SNMP entity when Bad Value Errors occurred.
Read Only Errors In	The number of valid SNMP PDUs that were delivered to the SNMP entity when the Read Only Errors In occurred. Note: This is a protocol error that generates an SNMP PDU that contains readOnly in the error status field. This method detects incorrect implementations of the SNMP.
Generic Errors In	The number of SNMP PDUs that were delivered to the SNMP entity when Generic Errors In occurred.

Table 40 SNMP Statistics field descriptions (continued)

Field	Description
MIB Variables Retrieved	The number of MIB objects successfully retrieved by the SNMP switch after valid SNMP get-request and get-next Protocol Data Units (PDU).
MIB Variables Modified	The number of MIB objects that were successfully altered by the SNMP stack after valid SNMP set-request PDUs.
GET Requests In	The number of SNMP get-request PDUs that were accepted and processed by the SNMP stack.
GET NEXT Requests In	The number of SNMP get-next PDUs that were accepted and processed by the SNMP stack.
SET Requests In	The number of SNMP set-request PDUs that were accepted and processed by the SNMP stack.
GET Responses In	The total number of SNMP Get-Response PDUs accepted and processed by the SNMP agent.
Traps Received	The total number of SNMP Trap Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
Too Big Errors Out	The number of SNMP PDUs that were generated by the SNMP entity when Too Big Errors Out occurred.
No Such Names Out	The number of SNMP PDUs that were generated by the SNMP entity when No Such Names Out error occurred.
Bad Value Errors Out	The number of SNMP PDUs that were generated by the SNMP entity when Bad Value Errors Out occurred.
Generic Errors Out	The number of SNMP PDUs that were generated by the SNMP when Generic Errors Out occurred.
GET Requests Out	The total number of SNMP Get-Request Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
GET NEXT Requests Out	The total number of SNMP Get-Next Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
SET Requests Out	The total number of SNMP Set-Request Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
GET Responses Out	The total number of SNMP Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
Traps Out	The total number of SNMP Trap Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.

Viewing Information Summary

Device Console > Monitor > Switch > Information

Note: This tab might not be available for the selected switch. Please disregard this information if it does not apply to your switch.

Table 41 Information Summary field descriptions

Field	Description
Config Save Status	Shows the configuration save status: saveInProgress, saveSuccessful, saveFailed, notInitiated, saveNotRequired
Config Restore Status	Shows the configuration restoration status: restoreInProgress, restoreSuccessful, restoreFailed, notInitiated
Config Restore Version	Shows the restored version of the configuration.
Last Boot Time	The time the switch was last rebooted.
Alloc Count	Total number of packet allocations from the packet buffer pool by the TCP/IP protocol stack.
Release Count	Total number of times the packet buffers are freed (released) to the packet buffer pool by the TCP/IP protocol stack.
Fail Count	Total number of packet allocation failures from the packet buffer pool by the TCP/IP protocol stack.
Peak Usage Count	The highest number of packet allocations with size greater than 128 bytes and less than or equal to 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.

Monitoring Packet Statistics

Device Console > Monitor > Switch > *Packet Statistics*

Table 42 Packet Statistics field descriptions

Field	Description
Packets Allocated	The total number of allocated packets.
Packets Freed	The total number of freed allocated packets.
Failed Packet Allocations	The total number of failed allocated packets.
Medium Packet Allocations	The current number of allocated medium size packets. A medium packet contains between 129 and 1,536 bytes.
Jumbo Packet Allocations	The current number of allocated jumbo size packets. A jumbo packet contains between 1537 and 9,216 bytes.
Small Packet Allocations	The number of allocated small size packets. A small packet contains 128 bytes or less.
Medium Packet Allocations High Water Mark	The maximum number of allocated medium size packets. A medium packet contains between 129 and 1,536 bytes.
Jumbo Packet Allocations High Water Mark	The maximum number of allocated jumbo size packets. A jumbo packet contains between 1,537 and 9,216 bytes.
Small Packet Allocations High Water Mark	The maximum number of allocated small size packets. A small packet contains 128 bytes or less.

Monitoring MP CPU Statistics

Device Console > Monitor > Switch > *MP CPU Statistics*

Table 43 MP CPU Statistics field descriptions

Field	Description
MP Cpu Utilization (1 Second Avg)	The percentage of CPU utilization as measured over the last one-second interval.
MP Cpu Utilization (4 Second Avg)	The percentage of CPU utilization as measured over the last four-second interval.
MP Cpu Utilization (64 Second Avg)	The percentage of CPU utilization as measured over the last 64-second interval.

Monitoring STP Statistics

Device Console > Monitor > Switch > STP Statistics

Table 44 Spanning Tree Protocol field descriptions

Field	Description
STG	Shows the Spanning Tree Group number. MIF TEST
Port	Shows the port number.
Receive Cfg	Shows the number of configuration BPDUs received.
Receive TCN	Shows the number of TCN (Topology Change Notification) messages received.
Transmit Cfg	Shows the number of configuration BPDUs transmitted.
Transmit TCN	Shows the number of TCN (Topology Change Notification) messages transmitted.

Monitoring UFD Statistics

Device Console > Monitor > Switch > *UFD Statistics*

Note: This tab might not be available for the selected switch. Please disregard this information if it does not apply to your switch.

Table 45 Uplink Failure Detection Statistics field descriptions

Field	Description
Number of times LTM link failure	The total numbers of times that link failures were detected on the uplink ports in the Link to Monitor group.
Number of times LTM Link in Blocking State	The total number of times that Spanning Tree Blocking state was detected on the uplink ports in the Link to Monitor group.
Number of times LTD got auto disabled	The total numbers of times that downlink ports in the Link to Disable group were automatically disabled because of a failure in the Link to Monitor group.

Monitoring UFD Information

Device Console > Monitor > Switch > UFD Information

Note: This tab might not be available for the selected switch. Please disregard this information if it does not apply to your switch.

Table 46 Uplink Failure Detection Information field descriptions

Field	Description
UFD State	Shows the operational status of UFD: enabled or disabled.
Link to Monitor Status	Shows the current status of the Link to Monitor (LtM).
Link to Monitor Ports	Shows the ports in the assigned to the LtM.
Link to Monitor Trunks	Shows the trunks assigned to the LtM.
Link to Disable Status	Shows the current status of the Link to Disable (LtD).
Link to Disable Ports	Shows the ports assigned to the LtD.
Link to Disable Trunks	Shows the trunks assigned to the LtD.

Monitoring NTP Statistics

Device Console > Monitor > Switch > NTP Statistics

Table 47 NTP Statistics field descriptions

Field	Description
NTP Requests Sent to Primary NTP Server	The total number of Network Time Protocol (NTP) requests the switch sent to the primary NTP server to synchronize time.
NTP Responses received from Primary NTP Server	The total number of NTP responses received from the primary NTP server.
Update Clock Using Primary NTP Server Response	The total number of times the switch updated its time based on the NTP responses received from the primary NTP server.
NTP Requests sent to Secondary NTP Server	The total number of NTP requests the switch sent to the secondary NTP server to synchronize time.
NTP Responses received from Secondary NTP Server	The total number of NTP responses received from the secondary NTP server.
Update clock using Secondary NTP Server Response	The total number of times the switch updated its time based on the NTP responses received from the secondary NTP server.
Last Update NTP Server	Last update of time on the switch based on either primary or secondary NTP response received.
Last Update NTP Time	The time stamp showing the time when the switch was last updated

Monitoring Trunk Groups

Device Console > Monitor > Switch > *Trunk Groups*

Table 48 Trunk Groups field descriptions

Field	Description
Index	The switch Trunk Groups, by number.
State	The current operational state of the Trunk Group.
Ports	The member ports within each Trunk Group.

Monitoring Trunk Group Ports

Device Console > Monitor > Switch > *Trunk Group Ports*

Table 49 Trunk Groups field descriptions

Field	Description
Trunk Group	The Trunk Group number.
Port	The port number.
Port State	The link status of the port.

Monitoring TACACS+ Authentication Statistics

Device Console > Monitor > Switch > *TACACS Authentication Statistics*

Table 50 TACACS Authentication Statistics field descriptions

Field	Description
Start Requests	Number of authentication start requests sent to server.
Continue Requests	Number of authentication continue requests sent to server.
Enable Requests	Number of authentication enable requests sent to server.
Abort Requests	Number of authentication abort requests sent to server.
Pass Received	Number of authentication pass received from server.
Fail Received	Number of authentication fails received from server.
Get User Received	Number of authentication get users received from server.
Get Password Received	Number of authentication get passwords received from server.
Get Data Received	Number of authentication get data received from server.
Error Received	Number of authentication errors received from server.
Follow Received	Number of authentication follows received from server.
Restart Received	Number of authentication re starts received from server.
Session Timeout	Number of authentication session time outs.
Auth Requests	Number of authorization requests sent to server.
Auth Pass Adds Received	Number of authorization pass adds received from server.
Auth Pass Replace Received	Number of authorization pass replaces received from server.
Auth Fails Received	Number of authorization fails received from server.
Auth Error Received	Number of authorization errors received from server.
Auth Follows Received	Number of authorization follows received from server.
Auth Session Timeouts	Number of authorization session time outs.
Acct Start Requests	Number of accounting start requests sent to server.
Acct Wd Requests	Number of accounting watchdog requests sent to server.
Acct Stop Requests	Number of accounting stop requests sent to server.
Acct Success Received	Number of accounting success received from server.
Acct Error Received	Number of accounting errors received from server.

Table 50 TACACS Authentication Statistics field descriptions (continued)

Field	Description
Acct Follow Received	Number of accounting follow received from server.
Acct Session Timeouts	Number of accounting session time outs.
Malformed Pkt Received	Number of Malformed packets received from server.
Socket Failure	Number of socket failures occurred.
Connection Failure	Number of connection failures occurred.

How to Monitor a Port

Select Monitor's **Port** category to monitor Port Statistics and Information. This section covers the following port statistics and information topics:

- [“Monitoring Port—Summary” on page 232](#)
- [“Monitoring Port—Interface Statistics” on page 233](#)
- [“Monitoring Port—802.1x Statistics” on page 235](#)
- [“Monitoring Port—LACP Statistics” on page 236](#)
- [“Monitoring Port—LACP Aggregator Information” on page 237](#)
- [“Monitoring Port—LACP Port Aggregator Information” on page 238](#)
- [“Monitoring Port—IP Statistics” on page 239](#)
- [“Monitoring Port—Authenticator Diagnostics Statistics” on page 240](#)
- [“Monitoring Port—Bridge Statistics” on page 242](#)
- [“Monitoring Port—Ethernet Error Statistics” on page 243](#)

Monitoring Port—Summary

Device Console > Monitor > Ports > *Summary*

Table 51 Port Summary field descriptions

Field	Description
Port	The physical port.
Speed	The port speed.
Bytes In	The number of bytes per second that are being received by the port.
Unicast Packets In	The number of unicast packets per second that are being received by the port.
Bytes Out	The number of bytes per second that are being transmitted by the port.
Unicast Packets Out	The number of unicast packets per second that are being transmitted by the port.

Monitoring Port—Interface Statistics

Device Console > Monitor > Ports > *Interface Statistics*

Table 52 Port Interface field descriptions

Field	Description
Bytes In	The number of bytes received on the interface, including framing characters.
Unicast Packets In	The number of packets, delivered by this sublayer to a higher layer that were not addressed to a multicast or a broadcast address at this sublayer.
Non-Unicast Packets In	The number of packets, delivered by this sublayer to a higher layer that were addressed to a multicast or a broadcast address at this sublayer.
Discarded Packets	The number of inbound packets that were discarded, although no errors had been detected to prevent their delivery to a higher-layer protocol. This can occur to free up buffer space.
Error Packets	For packet-oriented interfaces, the number of inbound packets with errors that prevented their delivery to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units with errors that prevented their delivery to a higher-layer protocol.
Unknown Protocol Packets	For packet-oriented interfaces, the number of packets received via the interface that were discarded because of an unknown or unsupported protocol. For character-oriented or fixed-length interfaces that support protocol multiplexing, the number of transmission units received via the interface that were discarded because of an unknown or unsupported protocol. Note: If the interface does not support protocol multiplexing, Unknown Protocol Packets will be zero (0).
Bytes Out	The number of bytes transmitted out of the interface, including framing characters.
Unicast Packets Out	The number of packets that higher-level protocols requested to transmit that were not addressed to a multicast or broadcast address at this sublayer. The count includes the packets that were discarded or not delivered.
Non-Unicast Packets Out	The number of packets that higher-level protocols requested to transmit that were addressed to a multicast or broadcast address at this sublayer. The count includes the packets that were discarded or not delivered.
Outbound Discards	The number of outbound packets that were discarded, although no errors had been detected that would prevent their transmission. This can occur to free up buffer space.

Table 52 Port Interface field descriptions (continued)

Field	Description
Not Sent Due to Error	For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors.
Outbound Packet Queue Length	The number of packets in the output queue.
Broadcasts In	The number of packets, delivered by this sublayer to a higher layer, that were addressed to a broadcast address at this sublayer.
Broadcasts Out	The number of packets that higher-level protocols requested to transmit that were addressed to a broadcast address at this sublayer. The count includes the packets that were discarded or not delivered.
Multicasts In	The number of packets, delivered by this sublayer to a higher layer that were addressed to a multicast address at this sublayer. For a MAC layer protocol, this includes Group and Functional addresses.
Multicasts Out	The number of packets that higher-level protocols requested to transmit that were addressed to a multicast address at this sublayer. The count includes the packets that were discarded or not sent. For a MAC layer protocol, this count includes Group and Functional addresses.

Monitoring Port—802.1x Statistics

Device Console > Monitor > Ports > *802.1x Statistics*

Table 53 Port 802.1x field descriptions

Field	Description
EAPOL Frames Received	Total number of EAPOL frames received.
EAPOL Frames Transmitted	Total number of EAPOL frames transmitted.
EAPOL Start Frames Received	Total number of EAPOL start frames received.
EAPOL Logoff Frames Received	Total number of EAPOL logoff frames received.
EAPOL Response Id Frames Received	Total number of EAPOL response ID frames received.
EAPOL Response Frames Received	Total number of EAPOL response frames received.
EAPOL Request Id Frames Transmitted	Total number of EAPOL request ID frames transmitted.
EAPOL Request Frames Transmitted	Total number of EAPOL request frames transmitted.
Invalid EAPOL Frames Received	Total number of invalid EAPOL frames received.

Monitoring Port—LACP Statistics

Device Console > Monitor > Ports > *LACP Statistics*

Table 54 Port LACP Statistics field descriptions

Field	Description
Valid LACPDUs Received	Total number of valid LACP data units received.
Valid Marker PDUs Received	Total number of valid LACP marker data units received.
Valid Marker Rsp PDUs Received	Total number of valid LACP marker response data units received.
Unknown Version/TLV Type	Total number of LACP data units with an unknown version or type, length, and value (TLV) received.
Illegal Subtype Received	Total number of LACP data units with an illegal subtype received.
LACPDUs Transmitted	Total number of LACP data units transmitted.
Marker PDUs Transmitted	Total number of LACP marker data units transmitted.
Marker Rsp PDUs Transmitted	Total number of LACP marker response data units transmitted.

Monitoring Port—LACP Aggregator Information

Device Console > Monitor > Ports > LACP Aggregator

Table 55 Port LACP Aggregator Information field descriptions

Field	Description
MAC Address	MAC address assigned to the aggregator.
Actor System Priority	Priority value associated with the Actor's System ID.
Actor System ID	Unique identifier for the System where this aggregator resides.
Individual State	Indicates whether the aggregator represents an Individual link (true) or an Aggregate (false).
Actor Oper Key	Current value of the operational key for the aggregator.
Partner System Priority	Priority value associated with the Partner's System ID.
Partner System ID	Unique identifier for the current protocol Partner of this aggregator.
Partner Oper Key	Current value of the operational key for the aggregator's current protocol partner
Ready State	Indicates whether the aggregator is ready or not.
Number of Ports in	Total number of member ports within this aggregator.

Monitoring Port—LACP Port Aggregator Information

Device Console > Monitor > Ports > *LACP Port Aggregator*

Table 56 Port LACP Port Aggregator Information field descriptions

Field	Description
LACP Status	Current LACP status for the port: true or false
LACP Admin Status	Current LACP admin status: true or false
Actor System ID	Unique identifier for the System where this aggregator resides.
Actor System Priority	Priority value associated with the Actor's System ID.
Actor Admin Key	Current value of the administration key for the Aggregation Port.
Actor Oper Key	Current value of the operational key for the Aggregation Port.
Actor Port Number	Port number locally assigned to the Aggregation Port.
Actor Port Priority	Priority value assigned to this Aggregation Port.
Individual State	Indicates whether the Aggregation Port operates only as an Individual link (<i>true</i>) or is able to aggregate (<i>false</i>).
Selected Aggregator ID	Identifier of the aggregator that this Aggregation Port has currently selected.
Attached Aggregator ID	Identifier of the aggregator to which this Aggregation Port is currently attached.
Ready_N Flag	Indicates whether or not the timer has expired while waiting to attach to an aggregator.
Need to Transmit Flag	Displays the new protocol information to be transmitted on the link.
Selection Logic	Indicates the selection logic. A value of selected indicates the selection of an appropriate aggregator. A value of unselected indicates that no aggregator is currently selected and standby indicates a restriction on the selected aggregator.
Port Moved	Indicates whether or not if receive machine for a port is in the <i>port_disabled</i> state, and the combination of partner oper system and partner oper port number in use by the port, has been received in an incoming LACPDU on a different port.
Collision and Detection State	State of Collision Detection: <i>on</i> or <i>off</i>
Rx Machine State	State of the Rx Machine.
Mux Machine State	State of the Mux Machine.
Periodic Machine State	State of the Periodic Machine.

Monitoring Port—IP Statistics

Device Console > Monitor > Ports > *IP Statistics*

Table 57 Port IP Statistics field descriptions

Field	Description
Good Packets In	Number of good packets received.
Header Error Packets In	Number of header error packets received.
Inbound Discard Packets	Number of discarded inbound packets.

Monitoring Port—Authenticator Diagnostics Statistics

Device Console > Monitor > Ports > *Authenticator Diagnostics Statistics*

Table 58 Port Authenticator Diagnostics Statistics field descriptions

Field	Description
Authentication Enters Connecting	Total number of times that the state machine transitions to the CONNECTING state from any other state.
Authentication Logoffs	Total number of times that the state machine transitions from CONNECTING to DISCONNECTED as a result of receiving an EAPOLLogoff message.
Authentication Enter Authenticating	Total number of times that the state machine transitions from CONNECTING to AUTHENTICATING, as a result of an EAPResponse/Identity message being received from the Supplicant.
Authentication Success	Total number of times that the state machine transitions from AUTHENTICATING to AUTHENTICATED, as a result of the Backend Authentication state machine indicating successful authentication of the Supplicant.
Authentication Timeout	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of the Backend Authentication state machine indicating authentication timeout.
Authentication Failure	Total number of times that the state machine transitions from AUTHENTICATING to HELD, as a result of the Backend Authentication state machine indicating authentication failure.
Reauthentications	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of a re-authentication request.
EAP Starts while Authenticating	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Start message being received from the Supplicant.
EAP Logoff while Authenticating	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Logoff message being received from the Supplicant.
Reauthentications after Authentication	Total number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of a re-authentication request.
EAP Starts after Authentication	Total number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of an EAPOL-Start message being received from the Supplicant.
EAP Logoff after Authentication	Total number of times that the state machine transitions from AUTHENTICATED to DISCONNECTED, as a result of an EAPOLLogoff message being received from the Supplicant.

Table 58 Port Authenticator Diagnostics Statistics field descriptions (continued)

Field	Description
Backend Responses	Total number of times that the state machine sends an initial Access-Request packet to the Authentication server. Indicates that the Authenticator attempted communication with the Authentication Server.
Backend Access Challenges	Total number of times that the state machine receives an initial Access-Challenge packet from the Authentication server. Indicates that the Authentication Server has communication with the Authenticator.
Other Backend Requests	Total number of times that the state machine sends an EAP-Request packet (other than an Identity, Notification, Failure, or Success message) to the Supplicant. Indicates that the Authenticator chose an EAP-method.
Backend Non Nak Responses	Total number of times that the state machine receives a response from the Supplicant to an initial EAP-Request, and the response is something other than EAP-NAK. Indicates that the Supplicant can respond to the Authenticators chosen EAP-method.
Backend Authentication Success	Total number of times that the state machine receives an Accept message from the Authentication Server. Indicates that the Supplicant has successfully authenticated to the Authentication Server.
Backend Authentication Failures	Total number of times that the state machine receives a Reject message from the Authentication Server. Indicates that the Supplicant has not authenticated to the Authentication Server.

Monitoring Port—Bridge Statistics

Device Console > Monitor > Ports > *Bridge Statistics*

Table 59 Port bridge field descriptions

Field	Description
Maximum size of INFO	The maximum size of the INFO (non-MAC) field that this port will receive or transmit.
Frames In	The number of frames that have been received by this port from its segment. Note: Packets In only counts frames that are for a protocol being processed by the local bridging function, including bridge management frames.
Frames Out	The number of frames that have been transmitted by this port to its segment. Note: Packets Out only counts frames that are for a protocol being processed by the local bridging function, including bridge management frames.
Discarded Frames In	The number of valid received frames that were discarded (filtered) by the forwarding process.

Monitoring Port—Ethernet Error Statistics

Device Console > Monitor > Ports > *Ethernet Error Statistics*

Table 60 Port Ethernet Error Statistics field descriptions

Field	Description
Alignment Errors	The number of frames received on a particular interface that were not of integral length and did not pass the FCS check. The count is incremented when the Alignment Error status is returned by the MAC service to the LLC, or other MAC user. Frames with multiple errors are counted exclusively.
FCS Errors	The number of frames received on a particular interface that failed the FCS health check because of length. The count is incremented when the Frame Check Error status is returned by the MAC service to the LLC, or other MAC user. Frames with multiple errors are counted exclusively.
Single Collision Frames	The number successfully transmitted frames on a particular interface where transmission was inhibited by a single collision. Note: A frame that is counted by Single Collision Frames can also be counted by the occurrences of the Unicast Packets Out, Multicasts Out, or Broadcast Out, but not recorded by the event of Multiple Collision Frames.
Multiple Collision Frames	A count of successfully transmitted frames on a particular interface where transmission was inhibited by more than one collision. Note: A frame that is counted by Multiple Collision Frames can also be counted by Unicast Packets Out, Multicasts Out, or Broadcast Out, but not recorded by Single Collision Frames.
SQE Test Errors	The number of times the SQE TEST ERROR message was generated by the PLS sublayer for a particular interface.
Deferred Transmissions	A number of frames where the first transmission attempt, on a particular interface, is delayed because the medium is busy. Note: The count represented by an instance of this object does not include frames involved in collisions.
Late Collisions	The number of times that a collision is detected, on a particular interface, later than 512 bit-times into the transmission of a packet. A late collision, included in the count of Late Collisions, can be considered as a generic collision for other statistics. Note: bit-times vary per system. Example: On a 10Mbps system, 512 bit-times represents 51.2 microseconds.
Excessive Collisions	A number of frames on a particular interface in which transmission failed because of excessive collisions.

Table 60 Port Ethernet Error Statistics field descriptions (continued)

Field	Description
Internal MAC Transmission Errors	<p>The number of frames transmitted on a particular interface that failed because of an internal MAC sublayer transmit error. This frame error is only counted if it was not recorded under Late Collisions, Excessive Collisions, or Carrier Sense Errors.</p> <p>Note: Internal Mac Transmit Errors may represent a number of transmission errors that were not otherwise recorded.</p>
Carrier Sense Errors	<p>The number of times the carrier sense condition was lost or was never asserted while attempting to transmit a frame on a particular interface. The count, represented by an instance of this object, is incremented once per transmission attempt.</p>
Received Frames > Maximum Length	<p>A number of frames received on a specific interface that exceeded the allowed maximum frame size. The count is incremented when the Received Frames > Maximum Length status is returned by the MAC service to the LLC, or other MAC user. Received frames that have multiple errors are counted exclusively.</p>
Internal MAC Receive Errors	<p>The number of frames on a specific interface that could not be accepted because of an internal MAC sublayer error. This frame error is only counted if it was not recorded under Received Frames > Maximum Length, Alignment Errors, or FCS Errors.</p> <p>Note: Internal Mac Receive Errors may represent a number of receive errors that were not otherwise recorded.</p>

Monitoring Port – Transceiver Information

Device Console > Monitor > Ports > *Transceiver Info*

Note: This tab is available only for switches with 10G ports. Please disregard this information if it does not apply to your switch.

Table 61 Port Transceiver Information field descriptions

Field	Description
Port	10G port index
Port SFP/XFP Alias	10G SFP/XFP port alias
Device	Device name. "NO device" indicates device/cable is not connected.
Tx Enable	TX-Enable status. It can be (i) Not Installed (ii) Enabled (iii) Disabled (iv) Detached (v) Not Available
Rx Signal	RX-Signal status, as follows: e (i) Not Installed (ii) Down (iii) Link (iv) Detached (v) Not Available
Tx Fault	TX-Fault status, as follows: (i) Not Installed (ii) Fault (iii) None (iv) Detached (v) Not Available
Vendor	Vendor name of the device
Serial Number	Serial number of the device
Approval	Approval state for the device, as follows: (i) Not Installed (ii) Not Approved (iii) Approved (iv) Detached
Device Part Number	External Port SFP/XFP device part number.
Device Revision	External Port SFP/XFP device revision.
Device Voltage	External Port SFP/XFP device voltage.
Device Temperature	External Port SFP/XFP device temperature.
Device Laser Wave Length	External Port SFP/XFP device laser wave length.

How to Monitor Bridge Statistics

Select Monitor's **Bridge** category to monitor Bridge Statistics and Information. This section covers the following bridge statistics and information topics:

- [“Monitoring Bridge—Forwarding Database Information” on page 247](#)
- [“Monitoring Bridge—Forwarding Statistics” on page 248](#)
- [“Monitoring Bridge—Base Port Information” on page 249](#)
- [“Monitoring Bridge—CIST Bridge Information” on page 250](#)
- [“Monitoring Bridge—CIST Port Information” on page 251](#)
- [“Monitoring Bridge—STP Information” on page 252](#)

Monitoring Bridge—Forwarding Database Information

Device Console > Monitor > Layer 2 > Bridge > Forwarding Database Information

Table 62 Forwarding Database field descriptions

Field	Description
MAC Address	The MAC address of the FDB entry.
VLAN/Group	The VLAN number or Group number of the FDB entry.
Port	The physical port on which the MAC address is located
State	The status of the bridge: forwarding or unknown. An address that is in the forwarding state means that it has been learned by the switch. If the state for the port is listed as unknown, the MAC address has not yet been learned by the switch, but has only been seen as a destination address.
Trunk	Shows all FDB entries on a single trunk. When trunk groups are configured, you can view the state of each port in the various trunk groups.

Monitoring Bridge—Forwarding Statistics

Device Console > Monitor > Layer 2 > Bridge > *Forwarding Statistics*

Table 63 Monitoring Forwarding Statistics field descriptions

Field	Description
Current Entries	Current number of entries in the Forwarding Database.
Highest Number of Entries	Highest number of entries recorded at any given time in the Forwarding Database.

Monitoring Bridge—Base Port Information

Device Console > Monitor > Layer 2 > Bridge > Base Port Information

Table 64 Monitoring Base Port field descriptions

Field	Description
STP	The index for Spanning Tree Protocol groups.
Port	The port number for Spanning Tree Protocol groups.
State	The current state of the port as defined by Spanning Tree Protocol, as follows: disabled, blocking, listening, learning, forwarding, discarding, or broken.
Designated Root	The unique Bridge Identifier of the Bridge recorded as the Root in the Configuration BPDUs transmitted by the Designated Bridge for the segment to which the port is attached.
Designated Cost	The path cost of the Designated Port of the segment connected to this port. This value is compared to the Root Path Cost field in received bridge PDUs.
Designated Bridge	The designated bridge resides closest to the root bridge and is responsible for forwarding packets from the LAN towards the root bridge. This bridge is displayed as character string starting with the bridge priority (1-65535) followed by a hyphen and six byte MAC address of that switch.
Designated Port	The designated port identifies the physical ports.
Forward Transitions	The number of times this port has transitioned from the Learning state to the Forwarding state.
Path Cost	The port path cost parameter is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. A setting of 0 indicates that the cost will be set to the appropriate default after the link speed has been auto negotiated

Monitoring Bridge—CIST Bridge Information

Device Console > Monitor > Layer 2 > Bridge > CIST Bridge Information

Table 65 CIST Bridge field descriptions

Field	Description
Bridge	The bridge identifier.
Path Cost	The port path cost parameter is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. A setting of 0 indicates that the cost will be set to the appropriate default after the link speed has been auto negotiated.
Port	The port number.
Hello Time	The Hello interval in seconds.
Forward Delay	The time (in seconds) for a CIST bridge root forward delay.
Regional Root	The regional root.
Regional Path Cost	The regional path cost.

Monitoring Bridge—CIST Port Information

Device Console > Monitor > Layer 2 > Bridge > *CIST Port Information*

Table 66 CIST Port field descriptions

Field	Description
Port	Specifies the CIST bridge port being configured.
Priority	The port priority helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment.
Path Cost	The port path cost parameter is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. A setting of 0 indicates that the cost will be set to the appropriate default after the link speed has been auto negotiated.
State	Specifies if the CIST Bridge port is enabled or disabled.
Role	Specifies the role of the CIST Bridge port.
Designated Bridge	The designated bridge resides closest to the root bridge and is responsible for forwarding packets from the LAN towards the root bridge. This bridge is displayed as character string starting with the bridge priority (1-65535) followed by a hyphen and six byte MAC address of that switch.
Designated Port	The designated port identifies a physical port. This is a number that is the numerical sum of bridge priority and the actual physical port number. For example, a physical port number four with bridge priority 32768 will be displayed as 32678+4=32772.
Link Type	The port link type.

Monitoring Bridge—STP Information

Device Console > Monitor > Layer 2 > Bridge > STP

Table 67 STP Information field descriptions

Field	Description
STG	Spanning Tree Group index.
Time Since Topology Change	Time since the last time a topology change was detected by the bridge entity, in milliseconds.
Topology Changes	Total number of topology changes detected by this bridge since the management entity was last reset or initialized.
Designated Root	Bridge identifier of the root of the spanning tree, as determined by the Spanning Tree Protocol executed by this node. This value is used as the Root Identifier in all Configuration Bridge PDUs originated by this node.
Root Cost	Cost of the path to the root, as seen from this bridge.
Root Port	Port number of the port which offers the lowest cost path from this bridge to the root bridge.
Maximum Age	Maximum age of Spanning Tree Protocol information learned from the network on any port before it is discarded, in hundredths of a second. This is the actual value that currently is in use on this bridge.
Hello Time	Amount of time between the transmission of Configuration Bridge PDUs by this node on any port when it is the root of the spanning tree or trying to become so, in hundredths of a second. This is the actual value that currently is in use on this bridge.
Forward Delay	Time value that controls how fast a port changes its spanning state when moving towards the Forwarding state, in hundredths of a second. The Forward Delay value determines how long the port stays in each of the Listening and Learning states, which precede the Forwarding state. The Forward Delay value is also used to age all dynamic entries in the Forwarding Database, after a topology change has been detected.
Hold Time	Time interval during which no more than two Configuration Bridge PDUs are transmitted by this node, in hundredths of a second.

How to Monitor LLDP Information

Select Monitor's **Layer 2 > LLDP** category to monitor Link Layer Detection Protocol (LLDP) information. This section covers the following topics:

- [“Monitoring LLDP Port Information” on page 254](#)
- [“Viewing EVB \(Edge Virtual Bridging\) Local Information” on page 255](#)
- [“Viewing EVB \(Edge Virtual Bridging\) Remote Information” on page 256](#)

Monitoring LLDP Port Information

Device Console > Monitor > Layer 2 > LLDP > *LLDP Port Info*

Note: This tab might not be available for the selected switch. Please disregard this information if it does not apply to your switch.

Table 68 LLDP Port Information field descriptions

Field	Description
Port	The port alias or number.
EVB TLV State	Shows whether EVB TLV state is enabled or disabled.

Viewing EVB (Edge Virtual Bridging) Local Information

Device Console > Monitor > Layer 2 > LLDP > *EVB Local Info*

Note: This tab is available only for EVB capable switches. Please disregard this information if it does not apply to your switch.

Table 69 EVB Local Information field descriptions

Field	Description
Index	EVB index number.
Port	Port associated with the local EVB.
Capability	Supported capabilities.
Current	Current capabilities.
RTE Value	Local ECP RTE value.

Viewing EVB (Edge Virtual Bridging) Remote Information

Device Console > Monitor > Layer 2 > LLDP > EVB Remote Info

Note: This tab is available only for EVB capable switches. Please disregard this information if it does not apply to your switch.

Table 70 EVB Remote Information field descriptions

Field	Description
Index	EVB index number.
Port	Port associated with the remote EVB.
Capability	Supported capabilities.
Current	Current capabilities.
RTE Value	Remote ECP RTE value.

How to Monitor Failover Information

Select Monitor's **Layer 2 > Failover** category to monitor Failover information. This section covers the following Failover topics:

- [“Monitoring General Trigger Status” on page 258](#)
- [“Monitoring Trigger Information” on page 259](#)
- [“Monitoring Monitored Port Status” on page 260](#)
- [“Monitoring Controlled Port Status” on page 261](#)

Monitoring General Trigger Status

Device Console > Monitor > Layer 2 > Failover > *General*

Note: This tab might not be available for the selected switch. Please disregard this information if it does not apply to your switch.

Table 71 Failover General field descriptions

Field	Description
Failover State	Failover state (on or off)

Monitoring Trigger Information

Device Console > Monitor > Layer 2 > Failover > *Trigger Information*

Note: This tab might not be available for the selected switch. Please disregard this information if it does not apply to your switch.

Table 72 Failover Trigger Information field descriptions

Field	Description
Trigger ID	Trigger identifier
Trigger State	Trigger state (enabled or disabled)
Operational Links Limit	Limit on number of operational links
Monitor State	Runtime monitor state (up or down)
Monitored Ports	List of monitored ports
Control State	Runtime controlled state (auto-controlled or auto-disabled)
Controlled Ports	List of controlled ports

Monitoring Monitored Port Status

Device Console > Monitor > Layer 2 > Failover > *Monitor Port Status*

Note: This tab might not be available for the selected switch. Please disregard this information if it does not apply to your switch.

Table 73 Failover Monitor Port Status field descriptions

Field	Description
Trigger ID	Trigger identifier
Monitored Port	Port number of the monitored port.
Port Status	Port status (operational or failed)

Monitoring Controlled Port Status

Device Console > Monitor > Layer 2 > Failover > *Control Port Status*

Note: This tab might not be available for the selected switch. Please disregard this information if it does not apply to your switch.

Table 74 Failover Control Port Status field descriptions

Field	Description
Trigger ID	Trigger identifier
Controlled Port	Port number of the controlled port.
Port Status	Port status (operational or failed)

How to Monitor vLAG Information

Select Monitor's **Layer 2 > VLAG** category to monitor vLAG information. This section covers the following vLAG information topics:

- ["Monitoring vLAG General Information" on page 263](#)
- ["Monitoring vLAG PDU Statistics" on page 264](#)
- ["Monitoring vLAG IGMP Statistics" on page 266](#)
- ["Monitoring vLAG ISL Statistics" on page 267](#)

Monitoring vLAG General Information

Device Console > Monitor > Layer 2 > VLAG > General

Note: This tab or some of its fields might not be available for the selected switch. Please disregard this information if it does not apply to your switch.

Table 75 vLAG General field descriptions

Field	Description
State	The current running state of vLAG.
Admin Role	The current running role of the switch. The role can be Primary (1), Secondary (2), or Unselected (3).
Operational Role	The vLAG switch operational role.
ISL Trunk Id	The vLAG ISL Trunk ID.
Local MAC	The local vLAG MAC address.
Local Priority	The local vLAG priority.
Peer MAC	The peer vLAG MAC address.
Peer Priority	The peer vLAG priority.
Health Check Status	The current health check running status.
Startup Delay Interval	The startup delay timer interval.
Startup Delay Status	The startup delay timer status.
System MAC	The system vLAG MAC address.
Auto Recovery Status	The system auto recovery status.

Monitoring vLAG PDU Statistics

Device Console > Monitor > Layer 2 > VLAG > PDU

Use the **PDU** tab to view the VLAG PDU statistics.

Note: This tab or some of its fields might not be available for the selected switch. Please disregard this information if it does not apply to your switch.

Table 76 vLAG PDU statistics field descriptions

Field	Description
Sent for Role Election	The total number of vLAG PDUs sent for role elections.
Sent for System Info	The total number of vLAG PDUs sent for role system info.
Sent for Peer Instance Enable	The total number of vLAG PDUs sent for peer instance enable.
Sent for Peer Instance Disable	The total number of vLAG PDUs sent for peer instance disable.
Sent for FDB Dynamic Add	The total number of vLAG PDUs sent for addition of FDB dynamic entry.
Sent for FDB Dynamic Delete	The total number of vLAG PDUs sent for deletion of FDB dynamic entry.
Sent for FDB Inactive Add	The total number of vLAG PDUs sent for addition of FDB inactive entry.
Sent for FDB Inactive Delete	The total number of vLAG PDUs sent for deletion of FDB inactive entry.
Sent for Health Check	The total number of vLAG PDUs sent for health check.
Sent for ISL Hello	The total number of vLAG PDUs sent for ISL hello.
Sent for Other	The total number of vLAG PDUs sent for others.
Sent for Unknown	The total number of vLAG PDUs sent for unknowns.
Received for Role Election	The total number of vLAG PDUs received for role elections.
Received for System Info	The total number of vLAG PDUs received for role system info.
Received for Peer Instance Enable	The total number of vLAG PDUs received for peer instance enable.
Received for Peer Instance Disable	The total number of vLAG PDUs received for peer instance disable.

Table 76 vLAG PDU statistics field descriptions (continued)

Field	Description
Received for FDB Dynamic Add	The total number of vLAG PDUs received for addition of FDB dynamic entry.
Received for FDB Dynamic Delete	The total number of vLAG PDUs received for deletion of FDB dynamic entry.
Received for FDB Inactive Add	The total number of vLAG PDUs received for addition of FDB inactive entry.
Received for FDB Inactive Delete	The total number of vLAG PDUs received for deletion of FDB inactive entry.
Received for Health Check	The total number of vLAG PDUs received for health check.
Received for ISL Hello	The total number of vLAG PDUs received for ISL Hello.
Received for Other	The total number of vLAG PDUs received for others.
Received for Unknown	The total number of vLAG PDUs received for unknowns.

Monitoring vLAG IGMP Statistics

Device Console > Monitor > Layer 2 > VLAG > IGMP

Use the **IGMP** tab to view the vLAG IGMP statistics.

Note: This tab or some of its fields might not be available for the selected switch. Please disregard this information if it does not apply to your switch.

Table 77 vLAG IGMP field descriptions

Field	Description
Reports Forwarded	The total number of IGMP reports forwarded to the peer.
Leaves Forwarded	The total number of IGMP leaves forwarded to the peer.

Monitoring vLAG ISL Statistics

Device Console > Monitor > Layer 2 > VLAG > ISL

Use the **ISL** tab to view the vLAG ISL statistics.

Note: This tab or some of its fields might not be available for the selected switch. Please disregard this information if it does not apply to your switch.

Table 78 vLAG ISL field descriptions

Field	Description
In Octets	The total number of vLAG ISL octets received.
In Packets	The total number of vLAG ISL packets received.
Out Octets	The total number of vLAG ISL octets sent.
Out Packets	The total number of vLAG ISL packets sent.

How to Monitor Hotlinks Statistics

Select Monitor's **Hotlinks** category to monitor Hotlinks statistics. This section covers the following Hotlinks statistics topics:

- [“Monitoring Hotlinks Summary” on page 269](#)
- [“Monitoring Hotlinks Statistics” on page 270](#)
- [“Monitoring Hotlinks Information” on page 271](#)

Monitoring Hotlinks Summary

Device Console > Monitor > Layer 2 > Hotlinks > Summary

Note: This tab might not be available for the selected switch. Please disregard this information if it does not apply to your switch.

Table 79 Hotlinks Summary field descriptions

Field	Description
ID	The trigger identifier
Name	The trigger name
State	Trigger state – enable or disable
Preempt State	Preempt State – enable or disable
Forward Delay	Forward Delay setting in seconds
Active	The active interface information

Monitoring Hotlinks Statistics

Device Console > Monitor > Layer 2 > Hotlinks > Statistics

Note: This tab might not be available for the selected switch. Please disregard this information if it does not apply to your switch.

Table 80 Hotlinks Statistics field descriptions

Field	Description
Trigger ID	Trigger ID number.
Master Active	Total number of times the Master interface transitioned to the Active state.
Backup Active	Total number of times the Backup interface transitioned to the Active state.
FDB Update	Total number of FDB update requests sent.
FDB Failed	Total number of FDB update requests that failed.

Monitoring Hotlinks Information

Device Console > Monitor > Layer 2 > Hotlinks > Info

Note: This tab might not be available for the selected switch. Please disregard this information if it does not apply to your switch.

Table 81 Hotlinks Info field descriptions

Field	Description
Hotlinks Setting	Hotlinks on/off setting
Hotlinks FDB Update Setting	Hotlinks FDB update enabled/disabled setting
Hotlinks BPDU Flood Setting	Hotlinks BPDU Flood enabled/disabled setting

How to Monitor 802.1x/p Information

Select Monitor's **802.1x/p** category to monitor 802.1x/p information. This section covers the following 802.1x/p information topics:

- [“Monitoring 802.1x General Information” on page 273](#)
- [“Monitoring 802.1p—Priority COSq Information” on page 274](#)
- [“Monitoring Port Priority Information” on page 275](#)

Monitoring 802.1x General Information

Device Console > Monitor > Layer 2 > 802.1x/p > 802.1x General

Table 82 802.1X General Information field descriptions

Field	Description
System Capability	The capability of the switch as an 802.1x Authenticator. It cannot be used as an Authentication Server or a Supplicant.
System Status	The operational status of 802.1x: enabled or disabled
Protocol Version	The protocol version in use.

Monitoring 802.1p—Priority COSq Information

Device Console > Monitor > Layer 2 > 802.1x/p > 802.1p Priority COSq

Table 83 802.1p Priority COSq Information field descriptions

Field	Description
Priority	The 802.1p priority level.
COSq	The Class of Service queue number.
Weight	The scheduling weight of the COS queue.

Monitoring Port Priority Information

Device Console > Monitor > Layer 2 > 802.1x/p > *Port Priority*

Table 84 802.1p Port Priority Information field descriptions

Field	Description
Port	The port number.
Priority	The 802.1p priority level for the port.
COSq	The Class-of-Service (COS) queue number.
Weight	The scheduling weight of the COS queue.

How to Monitor ECP (Edge Control Protocol) Information

Select Monitor's **Layer 2 > ECP** category to view ECP information. This section covers the following topics:

- [“Viewing ECP \(Edge Control Protocol\) Channel Information” on page 277](#)

Viewing ECP (Edge Control Protocol) Channel Information

Device Console > Monitor > Layer 2 > ECP > ECP Channel Info

Note: This tab is available only for EVB capable switches. Please disregard this information if it does not apply to your switch.

Table 85 ECP Channel Information field descriptions

Field	Description
Index	ECP index number.
Port	Port associated with the ECP channel.
S-Tag	VLAN tag with a Tag Protocol Identification value allocated for "802.1Q Service Tag Type."
Send Length	Send length value.
Send Next	Index number associated with the next send.
Receive Last Sequence	Sequence number associated with the last received.
State Machine	State machine index.
Rx Count	Received packets count.
Tx Count	Transmitted packets count.
Rx Drop	Number of packets dropped during receive.
Tx Drop	Number of packets dropped while transmitting.
State	State (enabled or disabled).

How to Monitor IP Routing

Select Monitor's **Routing > IP** category to monitor IP Routing Statistics and Information. This section covers the following IP Routing statistics and information topics:

- [“Monitoring IP Routing—IP Interface Statistics” on page 279](#)
- [“Monitoring IP Routing—Interface Information” on page 280](#)
- [“Monitoring IP Routing—TCP Statistics” on page 281](#)
- [“Monitoring IP Routing—TCP Connections” on page 282](#)
- [“Monitoring IP Routing—UDP Statistics” on page 283](#)
- [“Monitoring IP Routing—UDP Information” on page 284](#)
- [“Monitoring IP Routing—IP Statistics” on page 285](#)
- [“Monitoring IP Routing—ICMP In Statistics” on page 287](#)
- [“Monitoring IP Routing—ICMP Out Statistics” on page 288](#)
- [“Monitoring IP Routing—DNS Statistics” on page 289](#)
- [“Monitoring IP Routing—Routes” on page 290](#)
- [“Monitoring IP Routing—Routes Standard” on page 291](#)
- [“Monitoring IP Routing—Routes Statistics” on page 292](#)
- [“Monitoring IP Routing—ARP” on page 293](#)
- [“Monitoring IP Routing—ARP Statistics” on page 294](#)
- [“Monitoring IP Routing—Gateway Information” on page 295](#)
- [“Monitoring IP Routing—IP Address Information” on page 296](#)

Monitoring IP Routing—IP Interface Statistics

Device Console > Monitor > Layer 3 > IP > *IP Interface Statistics*

Table 86 Routing IP Interface Statistics field descriptions

Field	Description
Interface	The number of the interface. The interface number is either one of the 256 IP interfaces or one of the physical ports.
Bytes In	The number of bytes received on the interface, including framing characters.
Bytes Out	The number of bytes transmitted out of the interface, including framing characters.
Unicast Packets In	The number of packets, delivered by this sublayer to a higher layer that were not addressed to a multicast or a broadcast address at this sublayer.
Unicast Packets Out	The number of packets that higher-level protocols requested to transmit that were not addressed to a multicast or broadcast address at this sublayer. The count includes the packets that were discarded or not delivered.
Multicasts In	The number of packets, delivered by this sublayer to a higher layer that were addressed to a multicast address at this sublayer. For a MAC layer protocol, this includes Group and Functional addresses.
Multicasts Out	The number of packets that higher-level protocols requested to transmit that were addressed to a multicast address at this sublayer. The count includes the packets that were discarded or not sent. For a MAC layer protocol, this includes Group and Functional addresses.
Discarded Packets	The number of inbound packets that were discarded, although no errors had been detected to prevent their delivery to a higher-layer protocol. This can occur to free up buffer space.
Outbound Discards	The number of outbound packets that were discarded, although no errors had been detected that would prevent their transmission. This can occur to free up buffer space.
Error Packets	For packet-oriented interfaces, the number of inbound packets with errors that prevented their delivery to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units with errors that prevented their delivery to a higher-layer protocol.
Not Sent Due to Error	For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors.

Monitoring IP Routing—Interface Information

Device Console > Monitor > Layer 3 > IP > Interface Information

Table 87 Routing IP Interface Information field descriptions

Field	Description
Interface	The interface type: <ul style="list-style-type: none"> An IP interface; for example <i>IP 10</i>. A physical (port) number depending on the switch; for example <i>Downlink2</i>.
Description	A text string containing information about the interface. <ul style="list-style-type: none"> A logical interface is described as <i>net0</i>, <i>net1</i>, etc. A Fast Ethernet physical (port) interface is described as <i>utp ethernet (10/100)</i> A Gigabit Ethernet physical (port) interface is described as <i>fiber ethernet (1000)</i>
Type	The type of interface. A virtual interface (<code>propVirtual</code>) or a physical interface that is assigned to a switch port (e.g. <code>ethernetCsmacd</code>).
MTU (Largest Packet)	The size of the largest datagram which can be sent or received on the interface, specified in octets
Speed	The speed of the physical interface: 10 Mbps, 100 Mbps, 1000Mbps, 10000Mbps, 40000Mbps, any or other.
MAC Address	The MAC address of the physical interface.
Admin State	The administrative state of the Interface: up, down or testing
Operational Status	The status of the Interface: up, down, testing, unknown, dormant, notPresent or lowerLayerDown.
Last Change	Lists the date of the last change to the interface.
MIB Specification	A reference to MIB definitions those are specific to the media that realizes the interface. Example: if the interface is realized by Ethernet, then MIB Specific refers to a document that defines Ethernet objects.

Monitoring IP Routing—TCP Statistics

Device Console > Monitor > Layer 3 > IP > *TCP Statistics*

Table 88 Routing IP TCP field descriptions

Field	Description
Active Opens	The number of TCP connections that were a direct transition to the SYN-SENT state from the CLOSED state.
Passive Opens	The number of TCP connections that were a direct transition to the SYN-RCVD state from the LISTEN state.
Failed Attempts	The number of TCP connections that were a direct transition to the CLOSED state from the SYN-SENT state or the SYN-RCVD state, and a direct transition to the LISTEN state from the SYN-RCVD state.
Resets In	The number of TCP connections that made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
Segments In	The total number of segments received, including those received in error. This count includes segments received on currently established connections.
Segments Out	The total number of transmitted segments, including those on current connections, but excluding those that contain only retransmitted bytes.
Retransmitted Segments	The total number of retransmitted segments: the number of TCP segments transmitted that contain one or more previously transmitted bytes.
Segments Received with Errors	The total number of received segments, including errors. This count includes segments received on currently established connections.
Resets Out	The number of transmitted TCP segments that contain the RST flag.

Monitoring IP Routing—TCP Connections

Device Console > Monitor > Layer 3 > IP > TCP Connections

Table 89 Routing TCP Connections field descriptions

Field	Description
Connection State	TCP connection state
Local IP Address	The local IP Address
Local TCP Port	The local port number
Remote IP Address	The remote IP address
Remote TCP Port	The remote port number

Monitoring IP Routing—UDP Statistics

Device Console > Monitor > Layer 3 > IP > UDP Statistics

Table 90 Routing IP UDP field descriptions

Field	Description
Datagrams In	The total number of UDP datagrams delivered to UDP users.
No Application at Port	The total number of received UDP datagrams when no application was at the destination port.
Dropped Datagrams	The number of received UDP datagrams that could not be delivered for reasons other than the absence of an application at the destination port.
Datagrams Out	The total number of delivered UDP datagrams.

Monitoring IP Routing—UDP Information

Device Console > Monitor > Layer 3 > IP > *UDP Information*

Table 91 Routing UDP Information field descriptions

Field	Description
Local IP Address	The local IP address for the UDP listener. When the UDP listener accepts datagrams for any IP interface associated with the node, the address is 0.0.0.0.
Local UDP Port	The local port number for the UDP listener.

Monitoring IP Routing—IP Statistics

Device Console > Monitor > Layer 3 > IP > *IP Statistics*

Table 92 Routing IP Statistics field descriptions

Field	Description
Good Packets In	The number of input datagrams received from interfaces, including those received in error.
Header Error Packets In	The number of input datagrams that were discarded because of errors in the IP headers. Errors: bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so on.
Address Errors In	The number of input datagrams that were discarded because the IP address in the IP header's destination field was not a valid address at this switch. Invalid addresses: 0.0.0.0, addresses of unsupported Classes such as Class E, and so forth. For entities that are not IP Gateways that do not forward datagrams, the count includes datagrams that were discarded because the destination address was not a local address.
Packets Routed	The number of input datagrams for which this entity was not their final IP destination. An attempt was made to find a route to forward them to that final destination. In entities that do not act as IP Gateways, the count only includes packets that were Source-Routed via this entity, and that the Source-Route option processing was successful.
Packets In with Unknown Protocol	The number of locally-addressed datagrams that were received successfully, but were discarded because of an unknown or an unsupported protocol.
Inbound Dropped Packets	The number of input IP datagrams that were discarded, although no errors were identified. This can occur because of insufficient buffer space. Note: This counter does not include any datagrams that were discarded while waiting for reassembly.
Packets Consumed	The total number of input datagrams successfully delivered to IP user-protocols, including ICMP.
Packets Out	The total number of IP datagrams that local IP user-protocols, including ICMP, supplied to IP in requests for transmission. Note: This counter does not include any datagrams that were counted in Packets Routed.
Outbound Dropped Packets	The number of output IP datagrams that were discarded, although no problems were noted. This can occur because of insufficient buffer space. Note: This counter includes datagrams that were counted in Packets Routed if the packets met this discard criterion.

Table 92 Routing IP Statistics field descriptions (continued)

Field	Description
Non-Routable Dropped Packets	The number of IP datagrams discarded because no route was available for transmitting them to their destinations. Note: This counter includes any packets counted in Packets Routed that meet this no-route criterion. Also included, are any datagrams that a host cannot route because all of the default gateways are down.
IP Fragments Reassembled	The number of received IP fragments that needed to be reassembled.
Packet Reassembly Successes	The number of IP datagrams successfully reassembled.
Packet Reassembly Failures	The number of failures detected by the IP reassembly algorithm. Possible failures include timed out, errors, and so on. Note: This is not necessarily a count of discarded IP fragments. Some algorithms, notably the algorithm in RFC 815, can lose track of the number of fragments by combining them as they are received.
Successful Packet Fragmentation	The number of IP datagrams that have been successfully fragmented.
Failed Packet Fragmentation	The number of IP datagrams that have been discarded because they could not be fragmented, such as when the Don't Fragment flag has been set.
Fragments Created	The number of IP datagrams that have been fragmented.
Routing Discards	The number of dropped packets.

Monitoring IP Routing—ICMP In Statistics

Device Console > Monitor > Layer 3 > IP > *ICMP In Statistics*

Table 93 Routing IP ICMP In field descriptions

Field	Description
Packets In	The number of received ICMP messages.
Error Packets In	The number of received ICMP Time error messages.
Destination Unreachable Packets In	The number of received ICMP Destination Unreachable messages.
Time Exceeded Packets In	The number of received ICMP Time Exceeded messages.
Parameter Problem Packets In	The number of received ICMP Parameter Problem messages.
Source Quench Packets In	The number of received Internet Control Message Protocol (ICMP) Source Quench messages.
Redirect Packets In	The number of received ICMP Redirect messages.
Echo (Ping) Request Packets In	The number of received ICMP Echo (request) messages.
Echo (Ping) Reply Packets In	The number of received ICMP Echo Reply messages.
Timestamp Request Packets In	The number of received ICMP Timestamp (request) messages.
Timestamp Reply Packets In	The number of received ICMP Timestamp Reply messages.
Address Mask Request Packets In	The number of received ICMP Address Mask Request messages.
Address Mask Reply Packets In	The number of received ICMP Address Mask Reply messages.

Monitoring IP Routing—ICMP Out Statistics

Device Console > Monitor > Layer 3 > IP > *ICMP Out Statistics*

Table 94 Routing IP ICMP Out field descriptions

Field	Description
Packets Out	The total number of delivered ICMP packets.
Error Packets Out	The number of ICMP packets delivered with error messages.
Destination Unreachable Packets Out	The number of transmitted ICMP Destination Unreachable messages.
Time Exceeded Packets Out	The number of transmitted ICMP Time Exceeded messages.
Parameter Problem Packets Out	The number of transmitted ICMP Parameter Problem messages.
Source Quench Packets Out	The number of Internet Control Message Protocol (ICMP) Source Quench messages sent.
Redirect Packets Out	The number of ICMP Redirect messages sent. Note: For a host, this object will always be 0 (zero) since hosts do not send redirects.
Echo (Ping) Request Packets Out	The number of transmitted ICMP Echo request messages.
Echo (Ping) Reply Packets Out	The number of transmitted ICMP Echo Reply messages.
Timestamp Request Packets Out	The number of transmitted ICMP Timestamp request messages.
Timestamp Reply Packets Out	The number of transmitted ICMP Timestamp Reply messages.
Address Mask Request Packets Out	The number of transmitted ICMP Address Mask Request messages.
Address Mask Reply Packets Out	The number of transmitted ICMP Address Mask Reply messages.

Monitoring IP Routing—DNS Statistics

Device Console > Monitor > Layer 3 > IP > *DNS Statistics*

Table 95 Routing IP DNS Statistics field descriptions

Field	Description
Good DNS Requests In	The number of DNS request packets that have been received.
DNS Requests Out	The number of DNS request packets that have been transmitted.
Bad DNS Requests In	The number of DNS request packets received that were dropped.

Monitoring IP Routing—Routes

Device Console > Monitor > Layer 3 > IP > Routes

Table 96 Routing Routes Information field descriptions

Field	Description
Route	The index number of the routing table.
Destination IP Address	The destination IP address of this route.
Destination IP Mask	The IP mask of this route.
Next-Hop Router 1	The gateway of this route.
Tag Type	The tag type: ICMP, static, SNMP, addr, RIP, broadcast, martian, or multicast.
Route Type	The type of route: indirect, direct, local, broadcast, martian, multicast, or other.
Interface	The IP interface of this route that is used as the source IP for routing.
Route Metric	The routing metric for the route.

Monitoring IP Routing—Routes Standard

Device Console > Monitor > Layer 3 > IP > *Routes Standard*

Table 97 Routing Routes Standard Information field descriptions

Field	Description
Local Interface Index	The index value identifying the local interface through which the next hop of this route should be reached.
Destination IP Address	The destination IP address of this route. Note: Multiple routes to a single destination can appear in the table if the Destination IP Address has been defined by the Network Management Protocol.
Next Hop	The IP address of the next hop of this route. Note: If a route bound to an interface is through a broadcast media, Next Hop Address is the agent's IP address on that interface.
Route Type	The type of route: direct, indirect, invalid, or other. Note: The type invalid disassociates both the destination and the route entry that are identified with this entry. Management stations must be prepared to receive information from agents that correspond to entries that are not currently in use.
Route Protocol	The route protocol/mechanism via which this route was learned: other, local, netmgmt, icmp, egp, ggp, hello, rip, is-is, es-is, ciscoIgrp, bbnSpfIgp, ospf, bgp
Route Age	The number of seconds since this route was last updated or otherwise determined to be correct.
Route Mask	The mask that must be logically Ended with the destination address before it is compared to the destination address of the router. If the value of the destination address is 0.0.0.0 (default value), the mask value is also 0.0.0.0. If the system does not support arbitrary subnet masks, an agent constructs the router mask based on the class of the network of the destination address: <ul style="list-style-type: none"> • 255.0.0.0 for class A • 255.255.0.0 for class B • 255.255.255.0 for class C

Monitoring IP Routing—Routes Statistics

Device Console > Monitor > Layer 3 > IP > *Routes Statistics*

Table 98 Routing Routes Statistics Information field descriptions

Field	Description
IP Routes	The current number of IP routes.
Most IP Routes	The highest number of IP routes.
Maximum IP Routes	The maximum number of IP routes.

Monitoring IP Routing—ARP

Device Console > Monitor > Layer 3 > IP > ARP

Table 99 Routing ARP Table field descriptions

Field	Description
Destination IP Address	The destination IP address of the address resolution.
MAC Address	The MAC address for the Address Resolution Protocol (ARP) entry.
VLAN ID	The VLAN identifier for the ARP.
Source Port	The port number.
Flag	<p>The flag status of this ARP: <i>clear</i>, <i>unresolved</i> (U), <i>permanent</i> (P), <i>indirect</i> (R), or <i>layer4</i> (p 4) (in 20.1.1.0 and higher). These flags are defined as follows:</p> <ul style="list-style-type: none">• U: Unresolved or unknown ARP entry. The MAC address of the client has not yet been learned.• P: Permanent entry created for switch IP interface. This entry never ages out.• P 4: Permanent entry created for Layer 4 proxy IP address or virtual server IP address.• R: Indirect ARP cache entry. This entry is used for faster forwarding the next time the packet comes for the same destination.

Monitoring IP Routing—ARP Statistics

Device Console > Monitor > Layer 3 > IP > ARP Statistics

Table 100 Routing ARP Statistics field descriptions

Field	Description
ARP Entries	The current number of ARP entries.
Most ARP Entries	The highest number of ARP entries.
Max ARP Entries	The maximum number of ARP entries.

Monitoring IP Routing—Gateway Information

Device Console > Monitor > Layer 3 > IP > *Gateway Information*

Table 101 Routing Gateway Information field descriptions

Field	Description
Gateway	The gateway index
Address	The gateway IP address
Status	The status of the gateway

Monitoring IP Routing—IP Address Information

Device Console > Monitor > Layer 3 > IP > IP Address Information

Table 102 Routing IP Address Information field descriptions

Field	Description
IP Address	The IP address
Interface	The index number of the interface.
IP Subnet Mask	The subnet mask of the IP address. The subnet mask is an IP address with all the network bits set to 1 and all the hosts bits set to 0.
Broadcast LSB	The broadcast address of the interface.
Maximum Reassembly Size	The size of the largest IP datagram that can be re-assembled from fragmented IP datagrams.

How to Monitor BGP Routing

Select Monitor's **Routing > BGP** category to monitor BGP Routing Statistics and Information. This section covers the following BGP Routing statistics and information topics:

- [“Monitoring BGP Routing—BGP Peers Summary” on page 298](#)
- [“Monitoring BGP Routing—BGP Routing Table” on page 300](#)

Monitoring BGP Routing—BGP Peers Summary

Device Console > Monitor > Layer 3 > BGP > *Peers Summary*

Table 103 Routing BGP Peers Summary Information field descriptions

Field	Description
Remote Address	The remote IP address of this entry's BGP peer.
Peer	The BGP Identifier of this entry's BGP peer.
State	The BGP peer connection state: idle, connect, active, opensent, openconfirm or established.
Status	The BGP status: stop or start
Version	The negotiated version of BGP running between the two peers.
Local Address	The local IP address of this entry's BGP connection.
Local Port	The local port for the TCP connection between the BGP peers.
Local Autonomous System	The Local Autonomous System number.
Remote Port	The remote port for the TCP connection between the BGP peers. Note that the objects <code>bgpPeerLocalAddr</code> , <code>bgpPeerLocalPort</code> , <code>bgpPeerRemoteAddr</code> and <code>bgpPeerRemotePort</code> provide the appropriate reference to the standard MIB TCP connection table.
Remote Autonomous System	The remote autonomous system number.
Received Updates	The number of BGP UPDATE messages received on this connection. This object should be initialized to zero (0) when the connection is established.
Sent Updates	The number of BGP UPDATE messages transmitted on this connection. This object should be initialized to zero (0) when the connection is established.
Received Messages	The total number of messages received from the remote peer on this connection. This object should be initialized to zero when the connection is established.
Sent Messages	The total number of messages transmitted to the remote peer on this connection. This object should be initialized to zero when the connection is established.
Last Error	The last error code and subcode seen by this peer on this connection. If no error has occurred, this field is zero. Otherwise, the first byte of this two byte OCTET STRING contains the error code, and the second byte contains the subcode.
FSM Established	The total number of times the BGP FSM transitioned into the established state.

Table 103 Routing BGP Peers Summary Information field descriptions

Field	Description
FSM Time	This timer indicates how long (in seconds) this peer has been in the Established state or how long since this peer was last in the Established state. It is set to zero when a new peer is configured or the router is booted.
Hold Time	Time interval in seconds for the Hold Timer established with the peer.
Keep Alive	Time interval in seconds for the KeepAlive timer established with the peer.
Time Since Last Update	Elapsed time in seconds since the last BGP UPDATE message was received from the peer. Each time the <code>bgpPeerInUpdates</code> is incremented, the value of this object is set to zero (0).

Monitoring BGP Routing—BGP Routing Table

Device Console > Monitor > Layer 3 > BGP > *Routing Table*

Table 104 Routing BGP Routing Table field descriptions

Field	Description
Index	BGP router index.
Network	BGP network address.
Next Hop	BGP NextHop addresses from this network.
Metric	BGP metric from this network.
Local Preference	BGP local preference from this network.
Weight	Total weight of AS paths from this network.
Path	AS paths from this network.
Origin	BGP route origin from this network.

How to Monitor RIP Routing

Select Monitor's **Routing > RIP** category to monitor RIP Routing Statistics and Information. This section covers the following RIP Routing statistics and information topics:

- [“Monitoring RIP Routing—RIP V2 Statistics” on page 302](#)
- [“Monitoring RIP Routing—RIP Route Information” on page 303](#)

Monitoring RIP Routing—RIP V2 Statistics

Device Console > Monitor > Layer 3 > RIP > *RIP V2 Statistics*

Table 105 Routing RIP V2 field descriptions

Field	Description
Packets Received	The number of RIPv2 packets received.
Packets Sent	The number of RIPv2 packets sent.
Requests Received	The number of RIPv2 requests received.
Responses Received	The number of RIPv2 responses received.
Requests Sent	The number of RIPv2 requests sent.
Responses Sent	The number of RIPv2 responses sent.
Route Timeouts	The number of RIPv2 route timeouts.
Bad Size Received	The number of RIPv2 packets with a bad size received.
Bad Version Received	The number of RIPv2 packets with a bad version received.
Bad Zero Received	The number of RIPv2 packets with a bad zero received.
Bad Source Port Received	The number of RIPv2 packets with a bad source port received.
Bad Source IP Received	The number of RIPv2 packets with a bad source IP received.
From Self Received	The number of RIPv2 packets received from the originating switch.

Monitoring RIP Routing—RIP Route Information

Device Console > Monitor > Layer 3 > RIP > *RIP Route Information*

Table 106 Routing RIP Route Information field descriptions

Field	Description
RIP Route Index	Index number of the RIP route.
Destination IP Address	Destination IP address for the route.
RIP Route Mask	Destination IP mask for the route
RIP Route Gateway	IP address for the next-hop router.
RIP Route Metric	Metric value for the route.

How to Monitor OSPF Routing

Select Monitor's **Routing > OSPF** category to monitor OSPF Routing Statistics and Information. This section covers the following OSPF Routing statistics and information topics:

- [“Monitoring OSPF Routing—General OSPF Statistics” on page 305](#)
- [“Monitoring OSPF Routing—OSPF Area Statistics” on page 308](#)
- [“Monitoring OSPF Routing—OSPF Area Neighbor Statistics” on page 309](#)
- [“Monitoring OSPF Routing—OSPF Area Interface Statistics” on page 310](#)
- [“Monitoring OSPF Routing—OSPF Area Receive Error Statistics” on page 311](#)
- [“Monitoring OSPF Routing—OSPF Area Interface Receive Error Statistics” on page 312](#)
- [“Monitoring OSPF Routing—OSPF Interface Change Statistics” on page 313](#)
- [“Monitoring OSPF Routing—OSPF Interface Transmission Statistics” on page 314](#)
- [“Monitoring OSPF Routing—OSPF Interface Neighbor Statistics” on page 315](#)
- [“Monitoring OSPF Routing—OSPF Area Information” on page 317](#)
- [“Monitoring OSPF Routing—OSPF Interface Information” on page 318](#)
- [“Monitoring OSPF Routing—OSPF Neighbor Interface Information” on page 319](#)
- [“Monitoring OSPF Routing—OSPF Virtual Interface Information” on page 320](#)
- [“Monitoring OSPF Routing—OSPF Stats2 Information” on page 321](#)
- [“Monitoring OSPF Routing—OSPF Link-State DB Information” on page 322](#)
- [“Monitoring OSPF Routing—OSPF External Link-State DB Information” on page 323](#)
- [“Monitoring OSPF Routing—OSPF Summary Range Information” on page 324](#)
- [“Monitoring OSPF Routing—OSPF Routes Information” on page 325](#)

Monitoring OSPF Routing—General OSPF Statistics

Device Console > Monitor > Layer 3 > OSPF > *General OSPF Statistics*

Table 107 Routing General OSPF field descriptions

Field	Description
Packets In	The total number of OSPF packets received for this OSPF interface.
Packets Out	The total number of OSPF packets transmitted for this OSPF interface.
Hello In	The total number of Hello packets received for this OSPF interface.
Hello Out	The total number of Hello packets transmitted for this OSPF interface.
Database Description In	The total number of Database Description packets received for this OSPF interface.
Database Description Out	The total number of Database Description packets transmitted for this OSPF interface.
Link State Request In	The total number of Link State Request packets received for this OSPF interface.
Link State Request out	The total number of Link State Request packets transmitted for this OSPF interface.
Link State Acks In	The total number of Link State Acknowledgement packets received for this OSPF interface.
Link State Acks Out	The total number of Link State Acknowledgement packets transmitted for this OSPF interface.
Link State Updates In	The total number of Link State Update packets received for this OSPF interface.
Link State Updates Out	The total number of Link State Update packets transmitted for this OSPF interface.
Neighbor Hello In	The sum total of all Hello packets received from neighbors on all OSPF areas and interfaces.
Neighbor State	The sum total number of neighbors in this state (i.e. an indication that Hello packets should now be sent to the neighbor at intervals of HelloInterval seconds), across all OSPF areas and interfaces.
Neighbor Adjoint Ok	The sum total number of decisions to be made (again) as to whether an adjacency should be established/maintained with the Neighbor across all OSPF areas and interfaces.
Neighbor Negotiation Done	The sum total number of neighbors in this state wherein the Master/slave relationship has been negotiated, and sequence numbers have been exchanged, across all OSPF areas and interfaces.

Table 107 Routing General OSPF field descriptions (continued)

Field	Description
Neighbor Exchange Done	The sum total number of neighbors in this state (i.e. in an adjacency's final state) having transmitted a full sequence of Database Description packets, across all OSPF areas and interfaces.
Neighbor Bad Link State Request	The sum total number of Link State Requests that have been received for a link state advertisement that is not contained in the database across all interfaces and OSPF areas.
Neighbor Bad Sequences	<p>The sum total number of Database Description packets which have been received that either:</p> <ul style="list-style-type: none"> • has an unexpected DD sequence number, or • has had the init bit set unexpectedly, or • has an options field differing from the last Options field received in a Database Description packet. <p>Any of these conditions indicate that some error has occurred during adjacency establishment for all OSPF areas and interfaces.</p>
Neighbor Loading Done	The sum total number of link state updates received for all out-of-date portions of the database across all OSPF areas and interfaces.
Neighbor Hello 1 way	The sum total number of Hello packets received from neighbors, in which this router is not mentioned across all OSPF interfaces and areas.
Neighbor Reset Adjacency	The sum total number of times the Neighbor adjacency has been reset across all OSPF areas and interfaces.
Neighbor Down	The total number of Neighboring routers down (i.e. in the initial state of a neighbor conversation) across all OSPF areas and interfaces.
Interface Up	The sum total number of interfaces up in all OSPF areas.
Interface Down	The sum total number of interfaces down in all OSPF areas.
Interface Not Connected	The sum total of interfaces no longer connected to the attached network across all OSPF areas and interfaces.
Interface Connected	The sum total number of interfaces, connected to the attached network in all OSPF areas.
Interface Wait Timer Fired	The sum total number of times the Wait Timer has been fired, (indicating the end of the waiting period that is required before electing a (Backup) Designated Router) across all OSPF areas and interfaces.
Interface Backup Routers	The sum total number of Backup Designated Routers on the attached network for all OSPF areas and interfaces.
Interface Bidirectional Changes	The sum total number of changes in the set of bidirectional neighbors associated with any interface across all OSPF areas.

Table 107 Routing General OSPF field descriptions (continued)

Field	Description
Hello Timer Fired	The sum total number of times the Hello timer has been fired (which triggers the send of a Hello packet) across all OPSF areas and interfaces.
Retransmit Timer Fired	The sum total number of times the Retransmit timer has been fired across all OPSF areas and interfaces.
Link State Lock Timer Fired	The sum total number of times the LSA Lock timer has been fired across all OSPF areas and interfaces.
Link State Ack Timer Fired	The sum total number of times the LSA Ack timer has been fired across all ospf areas and interfaces.
Dbage Fired	The total number of times the Dbage has been fired.
Summary Timer Fired	The total number of times the Summary timer has been fired.
ASE Export Timer Fired	The total number of times the (Autonomous System External route) ASE Export timer has been fired.

Monitoring OSPF Routing—OSPF Area Statistics

Device Console > Monitor > Layer 3 > OSPF > OSPF Area Statistics

Table 108 Routing OSPF Area field descriptions

Field	Description
Index	The index of the OSPF Area for which these statistics apply.
Packets In	The total number of OSPF packets received for this OSPF interface.
Packets Out	The total number of OSPF packets transmitted for this OSPF interface.
Hello In	The total number of Hello packets received for this OSPF interface.
Hello Out	The total number of Hello packets transmitted for this OSPF interface.
Database Description In	The total number of Database Description packets received for this OSPF interface.
Database Description Out	The total number of Database Description packets transmitted for this OSPF interface.
Link State In	The total number of Link State Request packets received for this OSPF interface.
Link State Out	The total number of Link State Request packets transmitted for this OSPF interface.
Link State Ack In	The total number of Link State Acknowledgement packets received for this OSPF interface.
Link State Ack Out	The total number of Link State Acknowledgement packets transmitted for this OSPF interface.
Link State Update In	The total number of Link State Update packets received for this OSPF interface.
Link State Update Out	The total number of Link State Update packets transmitted for this OSPF interface.

Monitoring OSPF Routing—OSPF Area Neighbor Statistics

Device Console > Monitor > Layer 3 > OSPF > *OSPF Area Neighbor Statistics*

Table 109 Routing OSPF Area Neighbor Statistics

Field	Description
Index	The index of the OSPF Interface for which these statistics apply.
Hello In	The total number of Hello packets received from neighbors in this OSPF interface.
Start State	The total number of neighbors in this state (i.e. an indication that Hello packets should now be sent to the neighbor at intervals of HelloInterval seconds) in this OSPF interface.
Adjoint Okay	The total number of decisions to be made (again) as to whether an adjacency should be established or maintained with the neighbor for this OSPF interface.
Negotiated Done	The total number of neighbors in this state in which the Master/slave relationship has been negotiated, and sequence numbers have been exchanged, for this OSPF interface.
Exchange Done	The total number of neighbors in this state (i.e. in an adjacency's final state) having transmitted a full sequence of Database Description packets, for this OSPF interface.
Bad Link State Request	The total number of Link State Requests which have been received for a link state advertisement not contained in the database for this interface.
Bad Sequences	<p>The total number of Database Description packets which have been received that either:</p> <ul style="list-style-type: none"> • has an unexpected DD sequence number, or • has had the init bit set unexpectedly, or • has an options field differing from the last Options field received in a Database Description packet. <p>Any of these conditions indicate that some error has occurred while establishing adjacency for this interface.</p>
Loading Done	The total number of link state updates received for all out-of-date portions of the database for this OSPF interface.
Hello 1 way	The total number of Hello packets received from neighbors, in which this router is not mentioned for this OSPF interface.
Reset Adjacency	The sum total number of times the Neighbor adjacency has been reset on this interface.
Down	The total number of Neighboring routers down (i.e. in the initial state of a Neighbor conversation) for this interface.
Hello 2 Way	The total number of Hello packets received from neighbors, in which this router is mentioned in the OSPF area.

Monitoring OSPF Routing—OSPF Area Interface Statistics

Device Console > Monitor > Layer 3 > OSPF > *OSPF Area Interface Statistics*

Table 110 Routing OSPF Area Interfaces field descriptions

Field	Description
Index	The index of the OSPF Area for which these statistics apply.
Up	The total number of times the interface was up.
Down	The total number of times the interface was down.
Not Connected	The total number of times the interface was no longer connected to the attached network.
Connected	The total number of times the interface connected back to the attached network.
Wait Timer Fired	The total number of times the Wait Timer has been fired, (indicating the end of the waiting period that is required before electing a (Backup) Designated Router) for this OSPF interface.
Backup Routers	The total number of Backup Designated Routers on the attached network for this OSPF interface.
Bidirectional Changes	The total number of changes in the set of bidirectional neighbors associated with the interface for this OSPF interface.

Monitoring OSPF Routing—OSPF Area Receive Error Statistics

Device Console > Monitor > Layer 3 > OSPF > OSPF Area Receive Error Statistics

Table 111 Routing OSPF Area Receive Error Statistics field descriptions

Field	Description
Index	Index of the OSPF Area for which these statistics apply.
Wrong Password	Total number of packets received with a wrong password in this area.
Wrong NetMask	Total number of packets received with a wrong netmask in this area.
Wrong Hello Interval	Total number of packets received with a different hello interval in this area.
Dead Interval	Total number of packets received with a different dead interval in this area.
Options	Total number of packets received with a different options in this area.
Unknown Neighbor	Total number of packets received from an unknown neighbor in this area.
Wrong Area	Total number of packets received with a wrong area.

Monitoring OSPF Routing—OSPF Area Interface Receive Error Statistics

Device Console > Monitor > Layer 3 > OSPF > OSPF Area Interface Receive Error Statistics

Table 112 OSPF Area Interface Receive Error Statistics field descriptions

Field	Description
Index	Index of the OSPF Area for which these statistics apply.
Wrong Password	Total number of packets received with a wrong password in this area.
Wrong NetMask	Total number of packets received with a wrong netmask in this area.
Wrong Hello Interval	Total number of packets received with a different hello interval in this area.
Dead Interval	Total number of packets received with a different dead interval in this area.
Options	Total number of packets received with a different options in this area.
Unknown Neighbor	Total number of packets received from an unknown neighbor in this area.
Wrong Area	Total number of packets received with a wrong area.

Monitoring OSPF Routing—OSPF Interface Change Statistics

Device Console > Monitor > Layer 3 > OSPF > *OSPF Interface Change Statistics*

Table 113 OSPF Interface Change Statistics field descriptions

Field	Description
Index	The index number.
Interface Up	The sum total number of interfaces that are up in all OSPF areas.
Interface Down	The sum total number of interfaces down in all OSPF areas.
Interface Not Connected	The sum total of interfaces no longer connected to the attached network across all OSPF areas and interfaces.
Interface Connected	The sum total number of interfaces, connected to the attached network in all OSPF areas.
Interface Wait Timer Fired	The sum total number of times the Wait Timer has been fired, (indicating the end of the waiting period that is required before electing a (Backup) Designated Router) across all OSPF areas and interfaces.
Interface Backup Routers	The sum total number of Backup Designated Routers on the attached network for all OSPF areas and interfaces.
Interface Bidirectional Changes	The sum total number of changes in the set of bidirectional neighbors associated with any interface across all OSPF areas.

Monitoring OSPF Routing—OSPF Interface Transmission Statistics

Device Console > Monitor > Layer 3 > OSPF > OSPF Interface Transmission Statistics

Table 114 OSPF Interface Transmission Statistics field descriptions

Field	Description
Index	The index of the OSPF Area for which these statistics apply.
Packets In	The total number of OSPF packets received for this OSPF interface.
Packets Out	The total number of OSPF packets transmitted for this OSPF interface.
Hello In	The total number of Hello packets received for this OSPF interface.
Hello Out	The total number of Hello packets transmitted for this OSPF interface.
Database Description In	The total number of Database Description packets received for this OSPF interface.
Database Description Out	The total number of Database Description packets transmitted for this OSPF interface.
Link State Request In	The total number of Link State Request packets received for this OSPF interface.
Link State Request Out	The total number of Link State Request packets transmitted for this OSPF interface.
Link State Acks In	The total number of Link State Acknowledgement packets received for this OSPF interface.
Link State Acks Out	The total number of Link State Acknowledgement packets transmitted for this OSPF interface.
Link State Updates In	The total number of Link State Update packets received for this OSPF interface.
Link State Updates Out	The total number of Link State Update packets transmitted for this OSPF interface.

Monitoring OSPF Routing—OSPF Interface Neighbor Statistics

Device Console > Monitor > Layer 3 > OSPF > *OSPF Interface Neighbor Statistics*

Table 115 OSPF Interface Neighbor Statistics field descriptions

Field	Description
Index	The index of the OSPF Area for which these statistics apply.
Hello In	The total number of Hello packets received from neighbors in this OSPF interface.
Start State	The total number of neighbors in this state (i.e. an indication that Hello packets should now be sent to the neighbor at intervals of HelloInterval seconds.) in this OSPF interface.
Adjoint OK	The total number of decisions to be made (again) as to whether an adjacency should be established or maintained with the neighbor for this OSPF interface.
Negotiated Done	The total number of neighbors in this state wherein the Master/slave relationship has been negotiated, and sequence numbers have been exchanged, for this OSPF interface.
Exchange Done	The total number of neighbors in this state (i.e. in an adjacency's final state) having transmitted a full sequence of Database Description packets, for this OSPF interface.
Bad Link State Request	The total number of Link State Requests which have been received for a link state advertisement not contained in the database for this interface.
Bad Sequences	<p>The total number of Database Description packets that have been received that either:</p> <ul style="list-style-type: none"> • have an unexpected DD sequence number • unexpectedly have had the init bit set • have an options field that differs from the last Options field that was received in a Database Description packet. <p>Any of these conditions indicate that some error has occurred during adjacency establishment for this interface.</p>
Loading Done	The total number of link state updates received for all out-of-date portions of the database for this OSPF interface.
Hello 1 way	The total number of Hello packets received from neighbors, in which this router is not mentioned for this OSPF interface.
Reset Adjacency	The sum total number of times the Neighbor adjacency has been reset on this interface.

Table 115 OSPF Interface Neighbor Statistics field descriptions (continued)

Field	Description
Down	The total number of Neighboring routers down (i.e. in the initial state of a neighbor conversation.) for this interface.
Hello 2 Way	The total number of Hello packets received from neighbors, in which this router is mentioned in the OSPF area.

Monitoring OSPF Routing—OSPF Area Information

Device Console > Monitor > Layer 3 > OSPF > *OSPF Area Information*

Table 116 Routing OSPF Area Information field descriptions

Field	Description
Index	The OSPF area number for this OSPF information table.
Area IP address	The IP address associated with the OSPF area.
Interfaces	The total number of interfaces for this OSPF area.
Interfaces Up	The total number of interfaces that are UP in this area.
Link State Database Entries	The number of Link State Database entries for this OSPF area.

Monitoring OSPF Routing—OSPF Interface Information

Device Console > Monitor > Layer 3 > OSPF > *OSPF Interface Information*

Table 117 Routing OSPF Interface Information field descriptions

Field	Description
Index	The OSPF interface number for which the OSPF info table is related.
Interface IP address	The IP interface of the OSPF area.
Designated Router ID	The OSPF Designated Router ID (IP Address) for this OSPF interface.
Designated Router IP	The OSPF Designated Router IP address for this OSPF interface.
Wait Interval	The OSPF Wait interval for this OSPF interface.
Total Neighbors	The total number of neighbors for this OSPF interface.

Monitoring OSPF Routing—OSPF Neighbor Interface Information

Device Console > Monitor > Layer 3 > OSPF > *OSPF Neighbor Interface Information*

Table 118 Routing OSPF Neighbor Interface Information field descriptions

Field	Description
Interface	The OSPF interface number.
Neighbor	The OSPF neighbor identifier.
Priority	The priority of the OSPF neighbor.
State	The state of the OSPF neighbor: down, attempt, init, twoway, exStart, exchange, loading, full
Designated Router	IP address of the designated router for the OSPF neighbor.
Backup Designated Router	The IP Address of the backup designated router for this OSPF neighbor.
IP Address	The IP Address of the OSPF neighbor.

Monitoring OSPF Routing—OSPF Virtual Interface Information

Device Console > Monitor > Layer 3 > OSPF > *OSPF Virtual Interface Information*

Table 119 Routing OSPF Virtual Interface Information field descriptions

Field	Description
Index	The OSPF virtual interface number.
IP Address	The IP Address of this virtual interface.
Area	The OSPF area to which, this virtual interface belongs.
Router ID	The designated Router ID.
State	The state of this virtual interface (enabled/disabled).
Cost	The cost of this virtual interface.
Transit Delay	The transit delay for this virtual interface.
Hello Interval	The hello interval for this virtual interface.
Dead Interval	The dead interval for this virtual interface.
Wait Interval	The wait interval for this virtual interface.
Retransmit Interval	The retransmit interval for this virtual interface.
Authentication	The authentication type for this virtual interface.
Events	The total events associated with this virtual interface.
Neighbor	The IP Address of the OSPF neighbor for this virtual interface.
Neighbor State	The up/down state of OSPF neighbor for this virtual interface.

Monitoring OSPF Routing—OSPF Stats2 Information

Device Console > Monitor > Layer 3 > OSPF > OSPF Stats2 Information

Table 120 Routing OSPF Stats2 Information field descriptions

Field	Description
Start Time	The time when OSPF has been started.
Up Time	The time since OSPF has been started.
Supported Types	The Link State Types that are supported.
Interfaces for Router	The number of interfaces for this router.
Virtual Links for Router	The number of virtual links for this router.
Total Neighbors	The total number of OSPF neighbors.
Neighbors in Initial State	The number of neighbors in the initial state of exchange.
Neighbors in Exchange State	The number of neighbors in the exchange state.
Neighbors in Full State	The number of neighbors in the initial state of exchange.
Areas	The total number of areas.
Transit Areas	The total number of transit areas.
NSSA Areas	The total number of NSSA areas.

Monitoring OSPF Routing—OSPF Link-State DB Information

Device Console > Monitor > Layer 3 > OSPF > *OSPF Link-State DB Information*

Table 121 Routing OSPF Link-State DB Information field descriptions

Field	Description
Area of Link-state Advertisement	The 32 bit identifier of the Area from which the Link-state Advertisement was received.
Type	The type of the link state advertisement. Each link state type has a separate advertisement format.
Link-state ID	The Link State ID is an LS Type Specific field containing either a Router ID or an IP Address; it identifies the piece of the routing domain that is being described by the advertisement.
Originating Router	The 32 bit number that uniquely identifies the originating router in the Autonomous System.
Sequence	The sequence number field is a signed 32-bit integer. It is used to detect old and duplicate link state advertisements. The space of sequence numbers is linearly ordered. The larger the sequence number the more recent the advertisement.
Age	This field is the age of the link state advertisement in seconds.
Checksum	This field is the checksum of the complete contents of the advertisement, excepting the age field. The age field is excepted so that an advertisement's age can be incremented without updating the checksum. The checksum used is the same that is used for ISO connectionless datagrams; it is commonly referred to as the Fletcher checksum.
Advertisement	The entire Link State Advertisement, including its header.

Monitoring OSPF Routing—OSPF External Link-State DB Information

Device Console > Monitor > Layer 3 > OSPF > *OSPF External Link-State DB Information*

Table 122 Routing OSPF External Link-State DB Information field descriptions

Field	Description
Type	The type of the link state advertisement. Each link state type has a separate advertisement format.
ID	The Link State ID is an LS Type Specific field containing either a Router ID or an IP Address; it identifies the piece of the routing domain that is being described by the advertisement.
Router	The 32 bit number that uniquely identifies the originating router in the Autonomous System.
Sequence	The sequence number field is a signed 32-bit integer. It is used to detect old and duplicate link state advertisements. The space of sequence numbers is linearly ordered. The larger the sequence number, the more recent the advertisement.
Age	This field is the age of the link state advertisement in seconds.
Checksum	This field is the checksum of the complete contents of the advertisement, excepting the age field. The age field is excepted so that an advertisement's age can be incremented without updating the checksum. The checksum used is the same that is used for ISO connectionless datagrams; it is commonly referred to as the Fletcher checksum.
Advertisement	The entire Link State Advertisement, including its header.

Monitoring OSPF Routing—OSPF Summary Range Information

Device Console > Monitor > Layer 3 > OSPF > *OSPF Summary Range Information*

Table 123 Routing OSPF Summary Range Information field descriptions

Field	Description
Index	The OSPF range index.
Area	The area associated for this OSPF range.
Network	The network associated for this OSPF range.
Mask	The mask associated for this OSPF range.
Action	The action (propagate/hide) assigned to this OSPF range.
List Type	The summary address list (Non-NSSA/NSSA) assigned to this OSPF range.

Monitoring OSPF Routing—OSPF Routes Information

Device Console > Monitor > Layer 3 > OSPF > *OSPF Routes Information*

Table 124 Routing OSPF Routes Information field descriptions

Field	Description
Index	The OSPF route table index.
Destination	The destination associated with this OSPF route.
Mask	The mask associated with this OSPF route.
Via	The next hop for this OSPF route.
Type	The route type code: <ul style="list-style-type: none">• IA - OSPF inter area• N1 - OSPF NSSA external type 1• N2 - OSPF NSSA external type 2• E1 - OSPF external type 1• E2 - OSPF external type 2• * - best

How to Monitor IGMP Routing

Select Monitor's **Routing > IGMP** category to monitor IGMP Routing Statistics and Information. This section covers the following IGMP Routing statistics and information topics:

- [“Monitoring IGMP Routing—IGMP Information” on page 327](#)
- [“Monitoring IGMP Routing—Multicast Router Information” on page 328](#)
- [“Monitoring IGMP Routing—IGMP Snooping Statistics” on page 329](#)

Monitoring IGMP Routing—IGMP Information

Device Console > Monitor > Layer 3 > IGMP > *IGMP Information*

Table 125 Routing IGMP Information field descriptions

Field	Description
Index	Displays a numeric identifier for the IGMP instance.
Source	Displays the Source IP address of the iGMP group.
Group	Displays the IGMP Group number.
VLAN	Displays the VLAN on which the Multicast Router is connected.
Port	Displays the port on which the Multicast Router is connected.
Version	Displays the IGMP version.
Mode	Displays the IGMPv3 filter mode for this host (either INCLUDE, EXCLUDE, or N/A)
Expires	Displays the Multicast Router expiration time.
Fwd	Displays the IGMPv3 forwarding state for this source/group IP address.

Monitoring IGMP Routing—Multicast Router Information

Device Console > Monitor > Layer 3 > IGMP > *Multicast Router Information*

Table 126 Routing IGMP MRouter Information field descriptions

Field	Description
Index	Displays a numeric identifier for the IGMP instance.
VLAN	Displays the VLAN on which the Mrouter is connected.
Port	Displays the port on which the Mrouter is connected.
Version	Displays the IGMP version.
Expires	Displays the Mrouter expiration time.
Max Query Response Time	Displays the maximum query response time interval.
Querier Robustness	The Querier Robustness value of this IGMP Mrouter.
Querier Query Interval Code	The Querier query interval code of this IGMP Mrouter.
Source IP	The source IP address of this IGMP Mrouter.

Monitoring IGMP Routing—IGMP Snooping Statistics

Device Console > Monitor > Layer 3 > IGMP > IGMP Snooping Statistics

Table 127 Routing IGMP Snooping Statistics field descriptions

Field	Description
VLAN/Group	The index of the VLAN or Group for which these statistics apply.
Received Valid Packets	Total number of valid IGMP packets received on this VLAN.
Received Invalid Packets	Total number of invalid IGMP packets received on this VLAN.
Received General Queries	Total number of IGMP General Query packets received on this VLAN.
Received Specific Queries	Total number of IGMP Group Specific Query packets received on this VLAN.
Received Leave Packets	Total number of IGMP Leave packets received on this VLAN.
Received Report Packets	Total number of IGMP Report packets received on this VLAN.
Sent Specific Queries	Total number of IGMP Group Specific Query packets transmitted on this VLAN.
Sent Report Packets	Total number of IGMP Report packets transmitted on this VLAN.
Sent Leave Packets	Total number of IGMP Leave packets transmitted on this VLAN.
Received PIM Hello Packets	Total number of PIM Hello packets received on this VLAN
Received Group Source Specific Queries	Total number of Group Source Specific queries (GSSQ) received on this VLAN
Received Current State Records	Total number of IGMP Current State records (CSRs) received on this VLAN
Received Source List Changed Records	Total number of IGMP Source List Change records (SLCRs) received on this VLAN
Received Filter Changed Records	Total number of IGMP Filter Mode Change records (FMCs) received on this VLAN
Sent General Query Packets	Total number of IGMP General Query packets sent on this VLAN
Received Discarded Packets	Total number of IGMP packets discarded on this VLAN

How to Monitor Virtual Routing

Select Monitor's **Virtual Routing** category to monitor Virtual Routing Statistics and Information. This section covers the following Virtual Routing statistics and information topics:

- [“Monitoring Virtual Routing Statistics” on page 331](#)
- [“Monitoring Virtual Routing State” on page 332](#)

Monitoring Virtual Routing Statistics

Device Console > Monitor > Layer 3 > Virtual Routing > *Virtual Routing Statistics*

Table 128 Virtual Routing field descriptions

Field	Description
VRRP Advertisements In	The total number of VRRP advertisements that were received.
VRRP Advertisements Out	The total number of VRRP advertisements that were transmitted.
Bad VRRP Advertisements	The total number of bad VRRP advertisements that were received. Bad VRRP advertisements are the advertisements that are ignored.
VRRP Bad Version	The total number of VRRP advertisements that had a bad version number.
VRRP Bad Address	The total number of VRRP advertisements that had a bad address.
VRRP Bad Password	The total number of VRRP advertisements that had a bad password.
VRRP Bad VRID	The total number of VRRP advertisements that had a bad virtual router ID.
VRRP Bad Data	The total number of VRRP advertisements that had bad data.
VRRP Bad Interval	The total number of VRRP advertisements that had a bad interval.

Monitoring Virtual Routing State

Device Console > Monitor > Layer 3 > Virtual Routing > *Virtual Routing State*

Table 129 Virtual Routing State field descriptions

Field	Description
Virtual Router Index	The index number of the VRRP virtual router.
State	<p>The state of the VRRP virtual router, as follows:</p> <ul style="list-style-type: none">• init identifies the initialization state which essentially announces each VRRP participating routers parameters such as capability, priority.• master identifies the elected master virtual router.• backup identifies that the virtual router is in backup mode.• holdoff identifies the state when a router changes the state from backup to master.
VRRP Ownership	<p>The ownership status of the VRRP virtual router, as follows:</p> <ul style="list-style-type: none">• owner identifies the preferred master virtual router. A virtual router is the owner when the IP address of the virtual router and its IP interface are the same.• renter identifies virtual routers which are not owned by this device.

How to Monitor Access Control Lists

Select Monitor's **Access Control List** category to monitor Access Control Lists (ACL) statistics. This section covers the following ACL statistics topics:

- ["Monitoring ACL Statistics" on page 334](#)
- ["Monitoring ACL Port Statistics" on page 335](#)
- ["Monitoring MAC ACL Statistics" on page 336](#)
- ["Monitoring IP ACL Statistics" on page 337](#)

Monitoring ACL Statistics

Device Console > Monitor > Access Control List > *ACL Statistics*

Table 130 ACL Statistics field descriptions

Field	Description
ACL	ACL Index Number.
Total Hits	Total number of hits (matches) for the ACL.

Monitoring ACL Port Statistics

Device Console > Monitor > Access Control List > *MAC ACL Statistics*

Table 131 ACL Statistics field descriptions

Field	Description
ACL	ACL index number.
Port	Port index number.
Total Hits	Total number of hits (matches) for the ACL.

Monitoring MAC ACL Statistics

Device Console > Monitor > Access Control List > *MAC ACL Statistics*

Table 132 ACL Statistics field descriptions

Field	Description
MAC ACL No	MAC ACL index number.
MAC Match Count	Total number of matches for the ACL.
MAC ACL Stats	Total number of hits for the ACL.

Monitoring IP ACL Statistics

Device Console > Monitor > Access Control List > *IP ACL Statistics*

Table 133 ACL Statistics field descriptions

Field	Description
IP ACL No	IP ACL index number.
IP Match Count	Total number of matches for the ACL.
IP ACL Stats	Total number of hits for the ACL.

How to Monitor Fiber Channel over Ethernet (FCoE)

Select Monitor's FCoE category to view information about FCoE Initialization Protocol (FIP) Snooping information and statistics. This section covers the following topics:

- [“Viewing FIP Snooping Port Information” on page 339](#)
- [“Viewing FIP Snooping Statistics” on page 340](#)
- [“Viewing FIP Snooping Information” on page 341](#)
- [“Viewing FIP Snooping FCF Detected Information” on page 342](#)
- [“Viewing FIP Snooping FCoE Connections Detected Information” on page 343](#)

Viewing FIP Snooping Port Information

Device Console > Monitor > FCoE > FIP Snooping Port Information

Note: This tab is available only for FCoE capable switches. Please disregard this information if it does not apply to your switch.

Table 134 FIP Snooping Port Information field descriptions

Field	Description
Port	Port index for FIP Snooping.
ACL Sequencer	FIP sequence number for an ACL in the corresponding port.
ACL	FIP Snooping ACL entry.

Viewing FIP Snooping Statistics

Device Console > Monitor > FCoE > FIP Snooping Statistics

Note: This tab is available only for FCoE capable switches. Please disregard this information if it does not apply to your switch.

Table 135 FIP Snooping Statistics field descriptions

Field	Description
Index	The index of FIP snooping statistics.
FCF Added	Number of FCF (Fiber Channel Forwarder) added to the FCoE database.
FCF Removed	Number of FCF (Fiber Channel Forwarder) removed from the FCoE database.
FCoE Connection Added	Number of FCoE connections added to the FCoE database.
FCoE Connection Removed	Number of FCoE connections removed from the FCoE database.

Viewing FIP Snooping Information

Device Console > Monitor > FCoE > FIP Snooping Information

Note: This tab is available only for FCoE capable switches. Please disregard this information if it does not apply to your switch.

Table 136 FIP Snooping Information field descriptions

Field	Description
Total number of FCFs detected	The total number of FCFs detected.
Total number of FCoE connections	The total number of FCoE connections.

Viewing FIP Snooping FCF Detected Information

Device Console > Monitor > FCoE > *FIP Snooping FCF Detected*

Note: This tab is available only for FCoE capable switches. Please disregard this information if it does not apply to your switch.

Table 137 FIP Snooping FCF Detected field descriptions

Field	Description
Index	FCF index
FCF MAC	FCF MAC address
Port	FCF port
VLAN	FCF VLAN

Viewing FIP Snooping FCoE Connections Detected Information

Device Console > Monitor > FCoE > *FIP Snooping FCoE Connections Detected*

Note: This tab is available only for FCoE capable switches. Please disregard this information if it does not apply to your switch.

Table 138 FIP Snooping FCoE Connections Detected field descriptions

Field	Description
Index	FCoE connection index.
VN Port MAC	FCoE connection VN Port MAC.
FCF MAC	FCoE connection FCF MAC.
Port	FCoE connection Port.
VLAN	FCoE connection VLAN.

Viewing FIP Snooping VLAN Information

Device Console > Monitor > FCoE > FIP Snooping VLAN Information

Note: This tab is available only for FCoE capable switches. Please disregard this information if it does not apply to your switch.

Table 139 FIP Snooping VLAN field descriptions

Field	Description
FCOE VLAN Index	The FCoE VLAN index.
Feature Index	The FCoE VLAN feature index. The feature index will accept values from 1 to the maximum SPAR ID (8) for the VLANs created by SPAR and 0 for other types of VLANs.
FCOE VLAN Creator	The FCoE VLAN Creator.
VLAN Ports	The port list information in the VLAN.

How to Monitor QoS Information

Select Monitor's **QoS** category to view information about QoS. This section covers the following topics:

- [“Monitoring QoS Counters” on page 346](#)

Monitoring QoS Counters

Device Console > Monitor > QoS > QoS Counters

Note: This tab or some of its fields might not be available for the selected switch type. Please disregard this information if it does not apply to your switch.

Table 140 QoS Counters field descriptions

Field	Description
Port Index	The index of the port
Queue Index	The index of the queue per port
Total Tx Packets	The total transmitted packets
Dropped Packets	The dropped packets
Total Tx Bytes	The total transmitted bytes
Dropped Bytes	The dropped bytes
Tx Packets Rate	The transmitted packets rate
Dropped Packets Rate	The dropped packets rate
Tx Bytes Rate	The transmitted bytes rate
Dropped Bytes Rate	The dropped bytes rate

How to Monitor Virtualization

Select Monitor's **Virtualization** category to view information about the association of various ports with Virtual Switch Groups, trunk groups and LACP keys, as well as VM information listing the details of all Virtual Machines discovered by the VMready switch. This section covers the following topics:

- [“Viewing VMready Port Information” on page 348](#)
- [“Viewing VMready VM Information” on page 349](#)

Viewing VMready Port Information

Device Console > Monitor > Virtualization > VMready Port Info

Note: This tab is available only for the VMready capable switches. Please disregard this information if it does not apply to your switch.

Uplink Port

This section lists all uplink (non-server) ports showing the status, Group number, Trunk number, and LACP key number.

Table 141 Uplink Port field descriptions

Field	Description
Status	Status of uplink port. Green icon indicates Up status and Red icon indicates Down status.
Port	Alias of uplink port.
Group	Group number to which the uplink port is associated.
Trunk #	Trunk number to which the uplink port is associated.
LACP Key #	LACP key number to which the uplink port is associated.

Server Port

This section lists all server (or internal) ports showing the status, Group number, Trunk number, and LACP key number.

Table 142 Server Port field descriptions

Field	Description
Status	Status of uplink port. Green icon indicates Up status and Red icon indicates Down status.
Port	Alias of server port.
Group	Group number to which the server port is associated.
Trunk #	Trunk number to which the uplink port is associated.
LACP Key #	LACP key number to which the uplink port is associated.

Viewing VMready VM Information

Device Console > Monitor > Virtualization > VMready VM Info

This section lists all Virtual Machines (VMs) discovered by the switch. You can filter the Virtual Machines list based on the Virtual Switch Groups (Groups) to which they belong.

Note: This table will be blank if no VM have been discovered by the switch. This table will not be shown in the tab if Virtual Machine Groups have not been enabled on the switch.

Table 143 VMs Discovery field descriptions

Field	Description
Virtual MAC	MAC address of the Virtual Machine.
Group	Group number to which the Virtual Machine is associated.
IP Address	IP Address of the Virtual Machine.
VM Name	Name of the virtual machine discovered on the selected port. If the VM Management Server Connector is not configured, this field is blank.
Hypervisor	Name of the Hypervisor on which the VM is running. If the VM Management Server Connector is not configured, this field is blank.
VLAN	VLAN to which the Virtual Machine is associated.
Port	Server port on which Virtual Machine was discovered.

How to Monitor Edge Virtual Bridging (EVB)

Select Monitor's Virtualization > EVB category to view information about Edge Virtual Bridging (EVB) information. This section covers the following topics:

- [“Viewing VDP TLV \(VSI Discovery Protocol Type-Length-Value\) Information” on page 351](#)
- [“Viewing VSI \(Virtual Station Interface\) Information” on page 352](#)
- [“Viewing VM Information” on page 353](#)
- [“Viewing VSI DB Information” on page 354](#)
- [“Viewing VSI DB ACL Information” on page 355](#)

Viewing VDP TLV (VSI Discovery Protocol Type-Length-Value) Information

Device Console > Monitor > Virtualization > EVB > VDP TLV Info

Note: This tab is available only for EVB capable switches. Please disregard this information if it does not apply to your switch.

Table 144 VDP TLV Information field descriptions

Field	Description
Index	VDP Type-Length-Value (TLV) Index.
Type	TLV Type.
Length	TLV length.
TLV OUI	Organizationally Unique Identifier (OUI) associated with TLV.
Sub Type	TLV sub type.
Request	Request information.
Response	Response information.
Manager ID	Manager ID.

Viewing VSI (Virtual Station Interface) Information

Device Console > Monitor > Virtualization > EVB > VSI Info

Note: This tab is available only for EVB capable switches. Please disregard this information if it does not apply to your switch.

Table 145 VSI Information field descriptions

Field	Description
Index	VSI index number.
VSI Type ID	VSI Type ID.
Version	VSI version.
MAC Address	MAC address associated with the VSI type.
VLAN	VLAN associated with the VSI type.
Port	Port associated with the VSI type.
Tx ACL	Transmit ACL number.
Rx Entry	Receive Entry.

Viewing VM Information

Device Console > Monitor > Virtualization > EVB > VM Info

Note: This tab might not be available for the selected switch. Please disregard this information if it does not apply to your switch.

Table 146 Virtual Machine Information field descriptions

Field	Description
Index	VM index number.
VSI Type ID	VSI Type ID associated with this VM.
Version	VSI Type version information.
MAC Address	VSI MAC associated with this VM.
VLAN	VLAN associated with this VM.
Port	The VSI Port.
Transmit ACL	The transmit ACL information of this VM.
Receiver Info	The receiver information of this VM.
ACL Info	ACL information of this VM.

Viewing VSI DB Information

Device Console > Monitor > Virtualization > EVB > VSI DB Info

Note: This tab might not be available for the selected switch. Please disregard this information if it does not apply to your switch.

Table 147 VSI Database Information field descriptions

Field	Description
Index	VM index number.
DB Name	VSI database (DB) name.
VSI Type ID	VSI Type ID associated with this VM.
Version	VSI Type version information.
Manager ID	VSI DB Manager ID.
VLANs	VLANs associated with this VSI DB.
Tx Rate	The transmit rate.
Tx Burst	The transmit burst count.
Rx Rate	The receive rate.
Rx Burst	The receive burst count.

Viewing VSI DB ACL Information

Device Console > Monitor > Virtualization > EVB > VSI DB ACL Info

Note: This tab might not be available for the selected switch. Please disregard this information if it does not apply to your switch.

Table 148 VSI Database ACL Information field descriptions

Field	Description
Index	VM index number.
ACL	The ACL index number.
VSI Type ID	VSI Type ID.
Manager ID	VSI Manager ID.
Source MAC	The source MAC address.
Source MAC Mask	The source MAC address mask.
Destination MAC	The destination MAC address.
Destination MAC Mask	The destination MAC address mask.
VLAN	The virtual LAN.
Ethernet Type	The ethernet type.
Source	The source IP address.
Source Mask	The source IP address mask.
Destination	The destination IP address.
Destination Mask	The destination IP address mask.
ToS	Type of Service.
IP Proto	The IP protocol.
TCP Flags	TCP flags.
TCP Flags Mask	TCP flags mask.
Source Port	The source port.
Source Port Mask	The source port mask.
Destination Port	The destination port.
Destination Port Mask	The destination port mask.
ACL Action	The ACL action.
New Priority	The new priority value.

How to Monitor Unified Fabric Port Information

Select Monitor's **UFP** category to view information about Unified Fabric Port (UFP). This section covers the following topics:

- [“Monitoring CDCP Information” on page 357](#)
- [“Monitoring Port Information” on page 358](#)
- [“Monitoring QoS Information” on page 359](#)
- [“Monitoring TLV Information” on page 360](#)
- [“Monitoring VLAN Information” on page 361](#)
- [“Monitoring Virtual Port Information” on page 362](#)

Monitoring CDCP Information

Device Console > Monitor > Virtualization > UFP > CDCP Information

Note: This tab or some of its fields might not be available for the selected switch type. Please disregard this tab or field descriptions that do not apply to your switch.

Table 149 CDCP Information field descriptions

Field	Description
Index	The CDCP port index
Status	The CDCP port status

Monitoring Port Information

Device Console > Monitor > Virtualization > UFP > Port Information

Note: This tab or some of its fields might not be available for the selected switch type. Please disregard this tab or field descriptions that do not apply to your switch.

Table 150 Port Information field descriptions

Field	Description
Index	The port index.
State	The port state information.
Virtual Ports	The virtual ports information.
Channel 1 State	The Channel 1 State.
Channel 2 State	The Channel 2 State.
Channel 3 State	The Channel 3 State.
Channel 4 State	The Channel 4 State.

Monitoring QoS Information

Device Console > Monitor > Virtualization > UFP > QoS Information

Note: This tab or some of its fields might not be available for the selected switch type. Please disregard this tab or field descriptions that do not apply to your switch.

Table 151 QoS Information field descriptions

Field	Description
Port Index	The port index.
Virtual Port Index	The Virtual Port index.
Min Bandwidth per vPort	The minimum bandwidth per vPort.
Max Bandwidth per vPort	The maximum bandwidth per vPort.

Monitoring TLV Information

Device Console > Monitor > Virtualization > UFP > TLV Information

Note: This tab or some of its fields might not be available for the selected switch type. Please disregard this tab or field descriptions that do not apply to your switch.

Table 152 TLV Information field descriptions

Field	Description
Index	The TLV port index.
Status	The TLV port status.

Monitoring VLAN Information

Device Console > Monitor > Virtualization > UFP > VLAN Information

Note: This tab or some of its fields might not be available for the selected switch type. Please disregard this tab or field descriptions that do not apply to your switch.

Table 153 VLAN Information field descriptions

Field	Description
Index	The VLAN index.
Virtual Port List	The virtual ports list.
External Port List	The external ports list.
Internal Port List	The internal ports list.
UFP Port List	The UFP ports list.

Monitoring Virtual Port Information

Device Console > Monitor > Virtualization > UFP > *Virtual Port Information*

Note: This tab or some of its fields might not be available for the selected switch type. Please disregard this tab or field descriptions that do not apply to your switch

Table 154 Virtual Port Information field descriptions

Field	Description
Port Index	The port index.
Virtual Port Index	The virtual port index.
State	The virtual port state.
Mode	The virtual port mode.
SV ID	The virtual port Svid.
Default VLAN	The virtual port default VLAN.
Default Tag	The virtual port default tag.
Virtual Ports VLAN	The virtual port VLANs.

How to Monitor iSwitch Information

Select Monitor's **iSwitch** category to view information about iSwitch information. This section covers the following topics:

- [“Viewing Port Information” on page 364](#)
- [“Viewing Host Uplink Information” on page 365](#)

Viewing Port Information

Device Console > Monitor > iSwitch > Port Information

Table 155 Port Information field descriptions

Field	Description
Port ID	The OS port ID mapping to the distributed virtual port ID on vDS.
vDS Port ID	The distributed virtual port ID on virtual distributed switch (vDS).
Profile	The PortGroup to which the distributed virtual port ID belongs.
Connected	The name of the entity (example: VM name) connected to the port.
MAC Address	The MAC address of the entity (example: VM MAC address) connected to the port.
Host	The VMware host on which the entity (example: VM) connects to the port.
State	The status (Link Up/down/blocked) of the port.

Viewing Host Uplink Information

Device Console > Monitor > iSwitch > *Host Uplink Information*

Table 156 Host Uplink Information field descriptions

Field	Description
Host Name	The name of the VMware host.
Port ID	The OS uplink port ID.
Device Name	The name of the entity (ex: physical nic) connected to the uplink port.
State	The status (Link Up/down/blocked) of the uplink port.
MAC Address	The MAC address of the entity connected to the uplink port.
Port Group	The PortGroup to which the port ID belongs to.

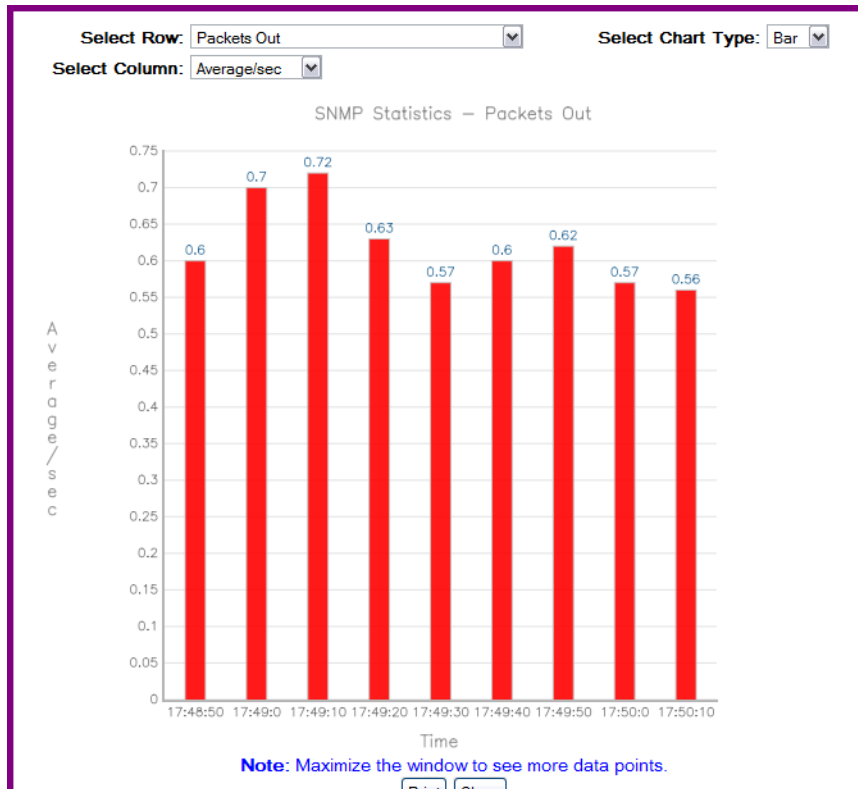
How to Launch a Chart

Real-time charting facility is supported for all statistics data. The chart feature plots the trend (the difference between the previous value and the current value) of either the Absolute Value—for statistics that show Absolute, Cumulative, Average/sec, Minimum/sec, Maximum/sec and LastVal/sec (such as **Monitor > Switch > SNMP Statistics**)—or the selected columnar value (such as “Bytes In” from the **Monitor > Port > Summary** page).

You can launch a chart using the following steps:

- 1 Select a switch and click any Monitor page showing statistics data.
- 2 In the statistics page, select a row that you want to plot.
- 3 For statistics pages showing Absolute, Cumulative values (such as **Monitor > Switch > SNMP Statistics**), click the **Chart** button to start plotting the graph.
- 4 For statistics pages that show only Absolute values for various parameters (such as the **Monitor > Port > Summary** page that show values for Bytes In, Bytes Out and so on), do the following:
 - a Select the column for which you want to plot the graph. You can do so by making use of the drop-down list next to Chart button.
 - b Click the **Chart** button to start plotting the graph.

[Figure 57 on page 367](#) shows an example graph plotting the trend for the Bytes In parameter of a port.

Figure 57 Bar Chart

When plotting charts from tables of statistics that include Absolute, Cumulative, Average values (such as the **Monitor > Switch > SNMP Statistics** page), you can perform the following actions:

- Change the chart type to Bar or Line by using **Select Chart Type** drop-down list.
- You can change to a different row by using **Select Row** drop-down list.
- You can Print a snap-shot of the graph by clicking the **Print** button.

When plotting charts from tables having multiple parameters (such as the **Monitor > Port > Summary** page), you can perform the following actions:

- Change the chart type to Bar or Line by using **Select Chart Type** drop-down list.
- You can change to a different row by using **Select Row** drop-down list.
- You can change to a different column by using **Select Column** drop-down list.
- You can Print a snap-shot of the graph by clicking the **Print** button.

How to Export a Statistical Summary

System Networking Switch Center gives you the option to export statistical data to a comma separated value (.csv) file that you can open in any spreadsheet program, such as Microsoft Excel or OpenOffice.

- 1 Select a switch.
- 2 Click **Monitor**.
- 3 Select a category, such as **Switch**.
- 4 Click a statistic category, such as packet statistics.
- 5 Click **Export** (see [Figure 58 on page 368](#)).
 - a Click **OK** to accept the default settings.
 - b Click **Save to Disk** to save the file on your computer.
 - c Click **Do this automatically for files like this from now on** to preserve your settings.


Process the file as you would any other spreadsheet. [Figure 58 on page 368](#) shows an example of an exported spreadsheet that contains packet statistics.

Tip: If you open the spreadsheet in Microsoft Office Excel 2007, you can save the spreadsheet as an Excel 97-2003 Workbook so that Microsoft Office Excel 2003 users can open it.

Figure 58 Packet Statistics Spreadsheet example

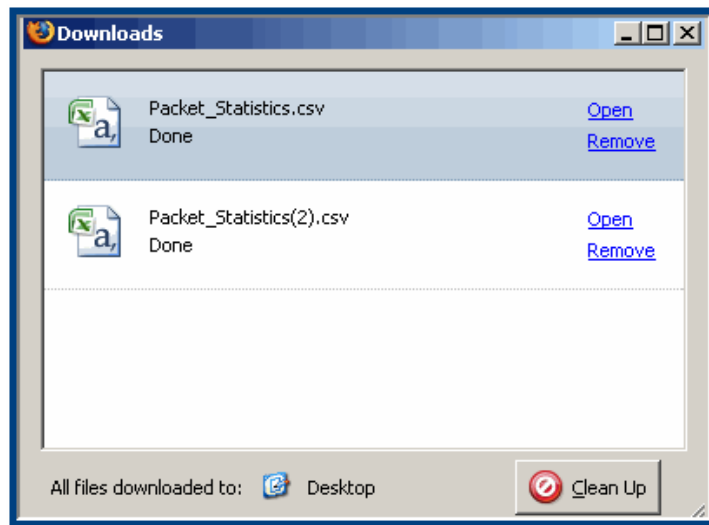
	A	B	C	D	E	F	G
1	Packet_Statistics						
2		Absolute\	Cumulative	Average/s	Minimum	Maximum	LastVal/sec
3	Packets Al	49501392	57473	10	0	0	0
4	Packets Fr	49501390	57473	10	0	0	0
5	Failed Pac	0	0	0	0	0	0
6	Medium P	2	110	0	0	0	0
7	Jumbo Pa	0	0	0	0	0	0
8	Small Pack	0	0	0	0	0	0
9	Medium P	51	0	0	0	0	0
10	Jumbo Pa	0	0	0	0	0	0
11	Small Pack	20	0	0	0	0	0

Administering Exported Files

After you export a file, System Networking Switch Center opens a window that displays the name of the exported file and the download status of the file. Click the  icon in your task bar to open the Downloads window (see [Figure 59 on page 369](#)). You can perform the following tasks:

- Click **Open** to view the exported spreadsheet.
- Click **Remove** to delete the exported spreadsheet from your desktop.
- Click **Clean Up** to clear all information about exported files from the Downloads window.

Figure 59 Downloads window



How to Print a Statistical Summary

The statistical summary is printed in portrait format and might contain multiple pages, depending on the volume of data.

- 1 Select a switch.
- 2 Click **Monitor**.
- 3 Select a category, such as **Switch**.
- 4 Click a statistic category, such as packet statistics.
- 5 Click **Print**.

Configuring the Switch

Using the configuration facility in System Networking Switch Center (SNSC), you can configure various parameters of a selected switch. The configuration facility is provided as part of the Device Console page (see [Figure 11 on page 88](#)).

Note: The configuration feature is available for certain firmware versions. You can see the list of supported switch types along with the firmware version from About dialog (see [“How to View Information About IBM System Networking Switch Center” on page 132](#)).

Note: You must be logged in using the administrator account to change switch configuration settings.

The topics in this chapter cover the following main switch configuration features:

- [“Configuration Steps” on page 373](#)
- [“General Switch Configuration” on page 379](#)
- [“Configuring Access Users” on page 406](#)
- [“Configuring Layer 2 Protocols” on page 408](#)
- [“Configuring Trunks” on page 410](#)
- [“Configuring LACP” on page 414](#)
- [“Configuring 802.1x” on page 417](#)
- [“Configuring MSTP and RSTP” on page 422](#)
- [“Configuring CIST” on page 424](#)
- [“Configuring Spanning Tree Protocol” on page 427](#)
- [“Configuring Forwarding Database” on page 433](#)
- [“Configuring Virtual Link Aggregation Groups” on page 437](#)
- [“Configuring Hot Links” on page 443](#)
- [“Configuring Virtual LANs” on page 446](#)
- [“Configuring Link Layer Discovery Protocol \(LLDP\)” on page 453](#)
- [“Configuring Failover” on page 458](#)
- [“Configuring Active Multipath Protocol \(AMP\)” on page 461](#)
- [“Configuring Edge Control Protocol \(ECP\)” on page 464](#)
- [“Configuring IP Interfaces” on page 466](#)

- [“Configuring Gateways” on page 473](#)
- [“Configuring Routes” on page 475](#)
- [“Configuring RMAPs” on page 481](#)
- [“Configuring RIP” on page 485](#)
- [“Configuring OSPF” on page 494](#)
- [“Configuring BGP” on page 509](#)
- [“Configuring IGMP” on page 516](#)
- [“Configuring DNS” on page 527](#)
- [“Configuring Bootp-Relay” on page 529](#)
- [“Configuring Flooding” on page 535](#)
- [“Configuring VRRP” on page 537](#)
- [“Configuring DHCP Snooping” on page 543](#)
- [“Configuring ARP” on page 546](#)
- [“Configuring Ports” on page 549](#)
- [“Configuring QoS – WRED/ECN” on page 563](#)
- [“Configuring ACLs” on page 566](#)
- [“Configuring CEE \(Converged Enhanced Ethernet\)” on page 580](#)
- [“Configuring FCoE \(Fiber Channel over Ethernet\)” on page 591](#)
- [“Configuring Switch Partition” on page 594](#)
- [“Configuring Virtualization” on page 597](#)
- [“Configuring iSwitch Virtual Data Station” on page 614](#)
- [“Configuring Unified Fabric Port \(UFP\)” on page 617](#)

Configuration Steps

This topic covers the steps involved in configuring switch parameters:

- [“Editing in Form Pane” on page 374](#)
- [“Editing in Tabular Pane” on page 375](#)
- [“Selection Windows” on page 376](#)
- [“Submitting and Applying Changes” on page 377](#)

Editing in Form Pane

The Form pane (see [Figure 60 on page 374](#)) is mainly displayed for those configurable features associated with scalar variables. You can configure the parameters either by entering new values in the text fields or by selecting the value from the drop-down list or using radio-buttons. The non-configurable parameters' values are shown in italics.

Figure 60 Configuration: Form Pane

Parameters

Non-editable fields

Launching Selection Window

Range

Actions Help

General Firmware Deployment Syslog Hosts Trap Settings RADIUS Server

TACACS Server TACACS - User Map NTP Service Management Network Port Mirroring

Switch General

System Description: *BNT 1/10Gb Uplink Ethernet Switch Module for IBM BladeCenter*

MAC address: *00:22:00:92:6b:00*

System Up Since: *1 days, 11 hours, 39 minutes and 3 seconds*

System Name:

Location:

Contact:

Current Date: 02/27/2000

Current Time: 10:02:09

Switch HTTP Server Port: 80

Switch Telnet Server Port: 24

Login Banner: BHM Rizzo switch1

Port Mirroring State: ☒ enabled ☐ disabled

CLI Session Idle Timeout: 45 1..60 (minutes)

Submit Apply Refresh Help

Editing in Tabular Pane

The Tabular pane (see [Figure 61 on page 375](#)) is mainly displayed for those configurable features associated with tables. Unlike form pane, tabular pane allows you to configure the parameters either through inline cell editing or in a separate window that can be launched by clicking **Modify**. While inline editing, you can configure the parameters either by entering new values in the editable cell or by selecting the value from the drop-down list associated with the cell. The non-configurable parameters are shown in non-editable cells with a slightly dark background.

Note: When you modify data in a cell, the cell appears blue until the change is saved.

Figure 61 Configuration: Tabular Pane

Table Heading

Selected Row

VLAN	Name	Ports	State	Spanning Tree Group
1	Default VLAN	INT1-INT14;EXT1;EXT	enabled	2
2	VM group 6	INT2;EXT2	enabled	1
20	VM group 5	INT2;EXT2	enabled	1
30	VM group 11	INT2;EXT2	enabled	1
35	VM group 10	INT2;EXT2	enabled	1
4095	Mgmt VLAN	INT1-MGT2	enabled	128

Non-editable cells

Editable cells (light background)

Submit Apply Refresh Insert Modify Delete Export Print Help Note: Double-click light background cells to modify the value

Selection Windows

Selection windows appear throughout System Networking Switch Center's configuration panels to let you select from a list of values.

To use a Selection window:

- 1 Click **Browse...** beside a field that displays it. The resultant window shows the already configured value with checked check box along with a slightly dark background for the row color.
- 2 From the Selection window, select the desired item.
- 3 Some Selection windows allow for multiple selections and some only allow for one selection.
- 4 Click **OK**.

Submitting and Applying Changes

You can submit your changes using the following steps:

- 1 Click **Submit** in the bottom of form or tabular pane. By default, the **Submit** button is disabled. However, when you make an edit, it is enabled. The Submit action results in sending your changes to the switch. Note that Submit action is specific to the panel.
- 2 Click **Apply**. This action results in applying the changes that you had submitted in the previous step.
- 3 Click **Save** for saving the changes to the flash memory.
- 4 You can activate **Apply** and **Save** actions from any configuration panel. In other words, they are not specific to any panel.
- 5 Use the Save indicator located at the right top corner of the Device Console window (see [Figure 11 on page 88](#)) to decide whether **Save** should be activated or not.

About Various Configure Tabs

Some **Device Console > Configure** tabs might not be available for the selected switch. For some switch types, though the tabs are present, but some fields might not be available. Please disregard the corresponding information if it does not apply to your switch.

General Switch Configuration

The following sections describe general switch configuration tasks you can perform with System Networking Switch Center (SNSC):

- [“General Configuration” on page 380](#)
- [“Software Image Configuration” on page 382](#)
- [“Configuration, Image, and Dump Control” on page 403](#)
- [“Syslog Hosts Configuration” on page 384](#)
- [“SNMP Trap Settings” on page 387](#)
- [“Syslog Settings” on page 388](#)
- [“General RADIUS Configuration” on page 390](#)
- [“RADIUS Server Configuration” on page 391](#)
- [“General TACACS+ Configuration” on page 393](#)
- [“TACACS+ Server Configuration” on page 394](#)
- [“TACACS+ User Map Configuration” on page 396](#)
- [“TACACS+ Command Authorization Configuration” on page 397](#)
- [“LDAP Server Configuration” on page 398](#)
- [“Network Time Protocol Configuration” on page 399](#)
- [“NTP MD5 Key Configuration” on page 400](#)
- [“Management Network Configuration” on page 401](#)
- [“Port Mirroring Configuration” on page 402](#)

General Configuration

Device Console > Configure > Switch > General

The following table describes the fields of the **General** configuration tab.

Table 157 Switch General Configuration field descriptions

Field	Description
System Description	Displays the product name of the switch.
Management/Switch MAC Address	MAC address of the switch.
System Up Since	Displays the date and time when the switch was last booted.
System Name	The administrative-assigned name for the managed node. You may enter the name of the device in this field to show up in the tool tip.
Location	The physical location of the node, such as telephone closet, 3rd floor.
Contact	Information about the contact person for this managed node.
Current Date	Displays the date on the real time clock.
Current Time	Displays the time on the real time clock.
Switch HTTP Server Port	Sets the TCP port number that the switch uses for any HTTP traffic. The default is port 80. Click Browse... to list all available TCP ports.
Switch Telnet Server Port	Sets the TCP port number that the switch uses for Telnet traffic. The default is HTTP port 23. Click Browse... to list all available TCP ports.
Login Banner	Displays the user-defined login banner. The message is displayed whenever you log into the switch using the Command Line Interface.
Port Mirroring State	Enables or disables the port mirroring state of the switch. The mirroring and monitoring ports are configured under the Mirror tab.
CLI Session Idle Timeout	Sets the idle timeout for CLI sessions, in minutes.
Service Required LED	Enables or disables the Service Required LED.
Logging Option	The logging option specifying whether the logging is to be done at console or not.
Login Authentication	Sets the login mechanism to local, remoteRadius or remoteTacacs.
Time Zone	Shows the configuration save status.
Telnet Access	Sets the Telnet access on the switch.
Switch Tftp Server Port	Sets the TFTP server listening port.

Table 157 Switch General Configuration field descriptions

Field	Description
System Banner	Sets the banner text.
DayLight Savings Time	Enables or disables Daylight Saving Time (DST).
Display Host in CLI Prompt	Enables or disables displaying the host name in CLI prompt.
Default IP Address on Data Interface	Enables or disables the use of default IP address on Data interface.
Default IP Address on Mgmt Interface	Enables or disables the use of default IP address on Management interface.
Default IP Address on MgmtA Interface	Enables or disables the use of default IP address on ManagementA interface.
Default IP Address on MgmtB Interface	Enable or disable the use of default IP address on ManagementB interface.
DCBX Feature	Enables or disables DCBX features.

Software Image Configuration

Device Console > Configure > Switch > Firmware

Use the Firmware tab to manage the switch software images. The following table describes the fields of the **Firmware** configuration tab.

Note: Some fields might not be available for the selected switch type. Please disregard field descriptions that do not apply to your switch.

Table 158 Switch Firmware Configuration field descriptions

Field	Description
Running Software Version	The version of the software image that is currently running on the system.
Boot Code Version	The software version of the switch boot code.
Image 1 Software Version	The software version of the image stored in the first image storage area.
Image 2 Software Version	The software version of the image stored in the second image storage area.
Image For Next Reset	Selects the software image to use during after the next reboot.
Configuration For Next Reset	Selects the configuration information to load during the next reboot.
CLI Mode for Next Reset	Selects the CLI mode used after the next reboot.
Use BOOTP	Enables or disables the usage of BOOTP for obtaining an IP address for the switch.
Use DHCP	Enables or disables Dynamic Host Control Protocol for setting the management IP address. When enabled, the IP address obtained from the DHCP server overrides the static IP address.
Use DHCP for MGTA	Enables or disables DHCP for setting the management IP address on management port A. When enabled, the IP address obtained from the DHCP server overrides the static IP address.
Use DHCP for MGTB	Enables or disables DHCP for setting the management IP address on management port B. When enabled, the IP address obtained from the DHCP server overrides the static IP address.
Use DHCP for EXTM	Enables or disables DHCP for setting the management IP address on external management port. When enabled, the IP address obtained from the DHCP server overrides the static IP address.
Apply Pending	Indicates whether any pending changes must be applied to the switch configuration.

Table 158 Switch Firmware Configuration field descriptions

Field	Description
Save Pending	Indicates whether any applied changes to the switch configuration must also be saved.
SNMP Free Resources Timeout	<p>The SNMP Free Resources Timeout indicates the number of minutes before the resources are freed and the state is set back to idle. Once SNMP operations that use the machine state are finished, the resources used by these operations must be freed by setting the state back to idle so that other commands can be issued via SNMP. One such operation would be an SNMP apply.</p> <p>This setting normally would not require modification unless you are using a MIB browser or performing debugging operations that might require a shorter or longer timeout period for SNMP operations.</p>
Boot Profile For Next Reset	The profile to use after the next reboot.
Configuration Save Option	Indicates whether the configuration of the switch has to be saved or not.
Configuration Save File Name	The file in which the switch configuration to be saved.
Configuration Save Status	Shows the configuration save status.
Configuration Restore Option	Indicates whether the configuration of the switch has to be restored or not.
Configuration Restore File Version	The file in which the switch configuration to be restored.
Configuration Restore Status	Shows the configuration restore status.
MTM	Sets the value for Machine Type Model (MTM).

Syslog Hosts Configuration

Device Console > Configure > Switch > Syslog Hosts

Use the **Syslog Hosts** tab to configure where syslog messages are sent and the severity of messages to be sent.

Table 159 Syslog Hosts Configuration field descriptions

Field	Description
1st Syslog Host IP Address	The IP address of the first Syslog host. The Syslog host is where syslog messages are to be sent.
Transfer Port for 1st Syslog Host	Selects the transfer port to use for sending syslog message to first Syslog host: <ul style="list-style-type: none"> DATA: Data port EXTM: External management port MGT, MGTA, MGTB: Internal management port
2nd Syslog Host IP Address	The IP address of the second Syslog host. The Syslog host is where syslog messages are to be sent.
Transfer Port for 2nd Syslog Host	Selects the transfer port to use for sending syslog message to second Syslog host: <ul style="list-style-type: none"> DATA: Data port EXTM: External management port MGT, MGTA, MGTB: Internal management port
1st Syslog Host Facility	Syslog Facility: Messages are dumped from the 1st Syslog Host to the selected bucket: local0 to local7.
2nd Syslog Host Facility	Syslog Second Facility: Messages are dumped from the 2nd Syslog Host to the selected bucket: local0 to local7.
1st Syslog Host Severity	This option sets the severity level of the first syslog host displayed. The default is 7, which logs all severity levels. For a detailed description of the severity levels, see "Levels of Severity" , next. The severity levels of the 1st Syslog Host are separate from those of the 2nd Syslog Host.
2nd Syslog Host Severity	This option sets the severity level of the second syslog host displayed. The default is 7, which logs all severity levels. For a detailed description of the seven levels of severity, see "Levels of Severity" . The severity levels of the 2nd Syslog Host are separate from those of the 1st Syslog Host.
Source Loopback Interface	Sets the loopback interface used for the source IP of the Syslog message.

Table 159 Syslog Hosts Configuration field descriptions

Field	Description
Syslog Console Severity	This option sets the severity level of the syslog console. The default is 7, which logs all severity levels. For a detailed description of the seven levels of severity, see "Levels of Severity" .
Syslog Flash Severity	This option sets the severity level of the syslog flash. The default is 7, which logs all severity levels. For a detailed description of the seven levels of severity, see "Levels of Severity" .

Levels of Severity

All Syslog messages have a level of severity attached to them. The following table describes the severity levels.

Table 160 Syslog Severity Level descriptions

Number	Name	Description
0	Emergency	The system is unusable.
1	Alert	Take action immediately.
2	Critical	The condition of the system is critical.
3	Error	The system has errors.
4	Warning	The system is giving a warning.
5	Notice	The condition of the system is normal but with significant conditions that need attention.
6	Informational	The system is working but information about certain conditions is available.
7	Debug	The system is giving out debug-level messages.

SNMP Trap Settings

Device Console > Configure > Switch > *SNMP Trap Settings*

Use the **SNMP Trap Settings** tab to enable or disable SNMP traps on a per-feature basis. The following tables describe various fields.

Note: Some fields might not be available for the selected switch type. Please disregard field descriptions that do not apply to your switch.

Table 161 SNMP Trap Settings field descriptions

Field	Description
Send Authentication Traps	Enables or disables the switch to generate authentication failure traps.
UFD Trap	Enables or disables generation of Uplink Failure Detection traps.
Logging	Enables or disables syslog and email alert features.
Time Stamp	Enables or disables timestamp option.
Console	Enables or disables console logging.
System Buffers	Sets the number of log buffers to be allocated.
SNMP Trap Source Interface	SNMP Trap Source Interface

Syslog Settings

Device Console > Configure > Switch > Syslog Settings

Use the **Syslog Settings** tab to enable or disable Syslog messages on a per-feature basis. The following tables describe various fields.

Note: Some fields might not be available for the selected switch type. Please disregard field descriptions that do not apply to your switch.

Table 162 Syslog Settings field descriptions

Field	Description
Console	Enables or disables logging of messages to the console.
System	Enables or disables system level alerts.
Management (flash, config, login)	Enables or disables management (flash, config, login) alerts.
CLI	Enables or disables CLI generated error messages.
Spanning Tree	Enables or disables spanning tree-related alerts.
VLAN	Enables or disables VLAN-related alerts.
SSH	Enables or disables SSH-related alerts.
VRRP	Enables or disables VRRP-related alerts.
NTP	Enables or disables NTP-related alerts.
IP	Enables or disables IP-related alerts.
WEBUI	Enables or disables Browser Based Interface-related alerts.
OSPF	Enables or disables OSPF-related alerts.
RMON	Enables or disables RMON-related alerts.
UFP	Enables or disables UFP-related alerts.
802.1x	Enables or disables 802.1-related alerts.
Config	Enable or disable switch configuration-related syslog and SNMP traps.
Config Change	Enable or disable switch configuration change related alerts.
BGP	Enables or disables BGP-related alerts.
Hot Links	Enables or disables Hot Links-related alerts.
Server	Enables or disables Server-related alerts.
Difftrak	Enables or disables Difftrak-related alerts.
LLDP	Enables or disables LLDP-related alerts.
VM	Enables or disables VM-related alerts.

Table 162 Syslog Settings field descriptions

Field	Description
Failover	Enables or disables Failover-related alerts.
DCBX	Enables or disables DCBX-related alerts.
FCoE	Enables or disables FCoE-related alerts.
VLAG	Enables or disables VLAG-related alerts.
LACP	Enables or disables LACP-related alerts.
Link	Enables or disables Link-related alerts.
VNIC	Enables or disables VNIC-related alerts.
TFTP	Enables or disables TFTP-related alerts.
Stacking	Enables or disables Stacking-related alerts.

General RADIUS Configuration

Device Console > Configure > Switch > *RADIUS General*

Use the **RADIUS General** tab to configure general parameters associated with RADIUS Server.

Note: Some fields might not be available for the selected switch type. Please disregard field descriptions that do not apply to your switch.

Table 163 RADIUS General field descriptions

Field	Description
Ext Debug Mask	Mask for enabling or disabling the Debug/Trace prints in the RADIUS module.
Maximum Number of Users	Maximum number of User entries stored. The value of this object will be stored for the MemPool Initialization.
Secure Backdoor Status	Status of RADIUS Server Secure Backdoor. If it is enabled allow noradius user to login with admin password otherwise it won't allow noradius user to login.
Port	Specify the RADIUS port number.
Server Enabled	Flag to denote whether the server is enabled or not.
Acct Port	Specify the RADIUS Accounting port number.
Accounting Enabled	Flag to denote whether the RADIUS Accounting is enabled or not.

RADIUS Server Configuration

Device Console > Configure > Switch > RADIUS Server

Use the **RADIUS Server** tab to configure parameters to access RADIUS Server for authentication.

Note: Some fields might not be available for the selected switch type. Please disregard field descriptions that do not apply to your switch.

Table 164 RADIUS Server Settings field descriptions

Field	Description
Primary RADIUS Server IP Address	Sets the IP address for the primary RADIUS server.
Secondary RADIUS Server IP Address	Sets the IP address for the secondary RADIUS server.
Primary RADIUS Server Port	Selects the type of port to which the primary RADIUS server is connected: <ul style="list-style-type: none"> data: Data port ext7/extm: External management port mgt: Internal management port
Secondary RADIUS Server Port	Selects the type of port to which the secondary RADIUS server is connected: <ul style="list-style-type: none"> data: Data port ext7/extm: External management port mgt: Internal management port
Port	Sets the user-configurable RADIUS application port. The default is RADIUS port number 1645.
Timeout	Sets the time-out in seconds.
Retries	Sets the number of retries to the RADIUS server before timing out.
RADIUS Authentication	Enables or disables RADIUS authentication.
Primary Secret	Sets the shared secret password between the switch and the primary RADIUS server.
Secondary Secret	Sets the shared secret password between the switch and the secondary RADIUS server.
Source Loopback Interface	Sets the loopback interface used for the source IP of the RADIUS message.

Table 164 RADIUS Server Settings field descriptions

Field	Description
RADIUS Telnet Backdoor	Enables or disables access through the RADIUS backdoor. Enabling this feature allows console access and disabling it allows Telnet access.
Secure Backdoor	Enables or disables the RADIUS backdoor using secure password for telnet/SSH/ HTTP/HTTPS.

Note: In case of IBM System Networking Distributed Switch 5000V, the RADIUS Server Configuration is listed in a table form with the parameters listed in the following table.

Table 165 RADIUS Server Table field descriptions

Field	Description
Server Index	RADIUS server index.
Server IP Address	Sets the IP address for the given RADIUS server.
Server Type	Sets the RADIUS server type (auth, acct, both).
Server Secret	Sets the shared secret password between the switch and this RADIUS server.
Timeout	Sets the time-out interval, in seconds.
Retries	Set the number of retries to the RADIUS server before timing out.

General TACACS+ Configuration

Device Console > Configure > Switch > TACACS General

Use the **TACACS General** tab to configure general parameters associated with TACACS+ Server.

Note: Some fields might not be available for the selected switch type. Please disregard field descriptions that do not apply to your switch.

Table 166 TACACS General field descriptions

Field	Description
Server	The active server address. Setting this object to zero disables the active server concept.
Trace Level	The debug trace level for TACACS+ client implementation. This is bit mapped data. Each bit of this object represent a trace level as given below: 0x00000001 - Information 0x00000002 - Errors 0x00000004 - Tx. packet dump 0x00000008 - Rx. packet dump 0xffffffff - All of the above 0x00000000 - No trace
Retransmit	Number of times the TACACS+ client searches the list of TACACS+ servers.
Privilege Level	Enable/disable Cisco type privilege level mapping. By default, privilege level mapping is disabled and the privilege levels are mapped as follows: 0 = CLI_AUTH_USER 3 = CLI_AUTH_OPER 6 = CLI_AUTH_ADMIN Once the privilege level is enabled, the following privilege levels are mapped: 0 - 1 = CLI_AUTH_USER 6 - 8 = CLI_AUTH_OPER 14 - 15 = CLI_AUTH_ADMIN
Secure Backdoor Status	Status of TACACS Server Secure Backdoor.
Server Enabled	Flag to denote whether the server is enabled or not.

TACACS+ Server Configuration

Device Console > Configure > Switch > TACACS Server

Use the **TACACS Server** tab to configure parameters to access TACACS+ Server for authentication.

Note: Some fields might not be available for the selected switch type. Please disregard field descriptions that do not apply to your switch.

Table 167 TACACS+ Server Settings field descriptions

Field	Description
Primary Server	Sets the IP address for the primary TACACS+ server.
Secondary Server	Sets the IP address for the secondary TACACS+ server.
Primary Server Port	Selects the port type to which the primary TACACS+ server is connected: <ul style="list-style-type: none"> data: Data port ext7/extm: External management port mgt: Internal management port
Secondary Server Port	Selects the type of port to which the secondary TACACS+ server is connected: <ul style="list-style-type: none"> data: Data port ext7/extm: External management port mgt: Internal management port
Port	Sets the user-configurable TACACS+ application port. The default is TACACS+ port number 49.
Timeout	Sets the time-out in seconds.
Retries	Sets the number of retries to the TACACS+ server before timing out.
TACACS+ Authentication	Enables or disables TACACS+ authentication.
Password Change	Enables or disables password change.
Primary Secret	Sets the shared secret password between the switch and the primary TACACS+ server.
Secondary Secret	Sets the shared secret password between the switch and the secondary TACACS+ server.
TACACS+ Backdoor	Enables or disables access through the TACACS+ backdoor. Enabling this feature allows console access and disabling it allows Telnet access.
Secure Backdoor	Enables or disables the TACACS+ backdoor using secure password for telnet/SSH/ HTTP/HTTPS.

Table 167 TACACS+ Server Settings field descriptions

Field	Description
Privilege Level Mapping	Enables or disables TACACS+ privilege-level mapping.
Command Authorization	Enables or disables command authentication.
Command Logging	Enables or disables command logging.
Directed Request	Enables or disables TACACS+ directed request.
Login Attempts	Sets the number of login attempts to the TACACS+ server.
Accounting	Enables or disables TACACS+ accounting.
Source Loopback Interface	Sets the loopback interface used for the source IP of the TACACS+ message.

Note: In case of IBM System Networking Distributed Switch 5000V, the TACACS+ Server Configuration is listed in a table form with the parameters listed in the following table.

Table 168 TACACS+ Server Table field descriptions

Field	Description
Server IP Address	Sets the IP address for the given TACACS+ server.
Server Single Connect	Enables (yes) or disables (no) server single connect.
Port	Sets the user-configurable TACACS+ application port. The default port is 49.
Timeout	Sets the time-out interval, in seconds.
Server Secret	Sets the shared secret password between the switch and this TACACS+ server.

TACACS+ User Map Configuration

Device Console > Configure > Switch > TACACS User Map

Use the **TACACS User Map** tab to configure TACACS User Mappings.

Note: This feature might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 169 TACACS+ User Mapping field descriptions

Field	Description
User ID	The remote privilege identifier
Mapping	The user mapping. It can be one of the following: none, user, oper and admin

TACACS+ Command Authorization Configuration

Device Console > Configure > Switch > TACACS Command Auth

Use the **TACACS Command Auth** tab to configure TACACS command authorization parameters.

Note: Some fields might not be available for the selected switch type. Please disregard field descriptions that do not apply to your switch.

Table 170 TACACS+ Command Auth field descriptions

Field	Description
Privilege Level	Privilege level associated with the CLI command.
Authorization Status	If command authorization status is true, then all commands with specified privilege level will be sent to TACACS+ server for authorization.
Accounting Status	If command accounting status is true, then all commands with specified privilege level will be sent to TACACS+ server for accounting.

LDAP Server Configuration

Device Console > Configure > Switch > LDAP Server

Use the **LDAP Server** tab to configure parameters to access LDAP Server for authentication.

Note: This tab or some fields might not be available for the selected switch type. Please disregard this tab or field descriptions that do not apply to your switch.

Table 171 LDAP Server Settings field descriptions

Field	Description
Primary Server	Sets the IP address for the primary LDAP server.
Transfer Port for Primary Server	Selects the type of port to which the primaryLDAP server is connected: <ul style="list-style-type: none"> • data: Data port • mgt: Management port • extm: External management port
Secondary Server	Sets the IP address for the secondary LDAP server.
Transfer Port for Secondary Server	Selects the type of port to which the secondary LDAP server is connected: <ul style="list-style-type: none"> • data: Data port • mgt: Management port • extm: External management port
Port	Sets the user-configurable LDAP application port. The default is LDAP port number 389.
Timeout	Sets the time-out in seconds.
Retries	Sets the number of retries to the LDAP server before timing out.
LDAP Authentication	Enables or disables LDAP authentication.
LADP Backdoor	Enables or disables the LDAP backdoor.
Domain Name	Sets the LDAP domain name.

Network Time Protocol Configuration

Device Console > Configure > Switch > NTP Service

Use the **NTP Service** tab to configure Network Time Protocol settings.

Note: Some fields might not be available for the selected switch type. Please disregard field descriptions that do not apply to your switch.

Table 172 NTP Server Settings field descriptions

Field	Description
NTP Service	Enables or disables the Network Time Protocol (NTP) switch.
Primary NTP Service IP Address	Sets the IP address of the primary NTP server.
Secondary NTP Service IP Address	Sets the IP address of the secondary NTP server.
Primary NTP Server Port	Selects the type of port to which the primary NTP server is connected: <ul style="list-style-type: none"> data: Data port ext7/extm: External management port mgt: Internal management port
Secondary NTP Server Port	Selects the type of port to which the secondary NTP server is connected: <ul style="list-style-type: none"> data: Data port ext7/extm: External management port mgt: Internal management port
Server Resync Interval	Specifies how often to resynchronize the switch clock with the NTP server:
Source Loopback Interface	Sets the loopback interface used for the source IP of the NTP message.
Admin Status	Sets the Admin Status (<i>up</i> , <i>down</i> , <i>testing</i>).
Ops Poll Server	Enables (yes) or disables (no) the trigger for the NTP client to transmit a request to the designated servers.

NTP MD5 Key Configuration

Device Console > Configure > Switch > NTP MD5 Key

Use the **NTP MD5 Key** tab to configure NTP MD5 key parameters.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 173 NTP MD5 Key Settings field descriptions

Field	Description
Index	The index for the NTP MD5 key.
MD5 Key	The NTP MD5 key code.

Management Network Configuration

Device Console > Configure > Switch > *Management Network*

Use the **Management Network** tab to define IP address ranges allowed to manage the switch using both the data and management ports.

Table 174 Switch Management Network field descriptions

Field	Description
Index	The index for the Management Network.
IP Address	The IP address for the Management Network.
IP Mask	The IP Mask for the Management Network.

Port Mirroring Configuration

Device Console > Configure > Switch > Port Mirroring

Use the **Port Mirroring** tab to configure, enable, and disable the monitored port. When port mirroring is enabled, network packets being sent and/or received on a target port are duplicated and sent to a monitoring port. You can attach a network analyzer to the monitoring port to collect detailed information about your network performance and usage.

Table 175 Port Mirroring field descriptions

Field	Description
Monitoring Port	The selected port for monitoring: Receives the duplicated packets delivered by the Mirrored Port.
Mirrored Port	Sets the selected port for mirroring: Packets received by or delivered from this port are delivered to the Monitoring Port.
Direction Mirrored	<p>This field lets you specify the direction in which packets are received by the mirrored port:</p> <ul style="list-style-type: none"> • in: Packets received by the mirrored port. • out: Packets transmitted from the mirrored port. • both: Packets received by or transmitted from the mirrored port. <p>It is necessary to specify the direction because:</p> <ul style="list-style-type: none"> • If the source port of the frame matches the mirrored port and the mirrored direction is set to in, then no frame is sent to the monitor port; if the direction is set to both, then only packets sent out by the mirrored port are sent to monitor port. • If the destination port of the frame matches the mirrored port and the mirrored direction is set to out, then no frame is sent to the monitor port.

Configuration, Image, and Dump Control

Device Console > Configure > Config/Image/Dump Control > Config/Image/Dump Control

Use the Config/Image/Dump Control to configure an FTP, TFTP, or SFTP server required for software image or configuration upgrade/download operations, and for downloading Panic and Tech Support Dump from the switch. The following table describes the fields of the **Config/Image/Dump Control** configuration tab.

Table 176 Config/Image/Dump Control field descriptions

Field	Description
User Name	User name for FTP operation. If specified, the transfer mode is set to FTP. If this field is blank, the transfer mode is set to TFTP.
Password	Password required for FTP operation. Blank for TFTP mode.
Server	Domain name or IP address of the FTP/SFTP/TFTP server.
Configuration File Name	Name of the file to be used in get/put configuration action selected in the Action drop-down list.
Dump File Name	Name of the file to be used in put dump action selected in the Action drop-down list.
TS Dump File Name	Name of the file to be used in put tsdump action selected in the Action drop-down list.
Image File Name	Name of the file to be used in combination with the action selected in the Action drop-down list.
Port for Transfer	Selects the transfer port to use for config/image/dump control operation: <ul style="list-style-type: none"> • data: Data port • extm: External management port • mgt: Internal management port
Image	Selects the image file slot to use in file transfer operations that pertain to the switch image files. The choices are <code>image1</code> , <code>image2</code> , and <code>boot</code> .

Table 176 Config/Image/Dump Control field descriptions (continued)

Field	Description
Action	<p>Select the FTP/SFTP/TFTP server action:</p> <ul style="list-style-type: none"> • Image Upgrade: Downloads the file specified in the Image File Name field from the FTP/SFTP/TFTP server to one of the switch image slots. The image slot is specified in the Image menu. • Config Upgrade: Downloads the configuration information contained in the file specified in the Configuration File Name field from the FTP/SFTP/TFTP server to the switch and makes it the active switch configuration. • Config Backup: Backs up the active configuration by uploading it from the switch to the FTP/SFTP/TFTP server. The backup file name is specified in the Configuration File Name field. • Panic Dump: Backs up the core dump from the switch to the FTP/SFTP/TFTP server. The backup file name is specified in the Dump File Name field. • Image Backup: Backs up the firmware by uploading it from the switch to the FTP/SFTP/TFTP server. The backup image file name is specified in the Image File Name field. • Tech Support Dump: Uploads the TS dump from the switch to the FTP/SFTP/TFTP server. The TS dump file name is specified in the TS Dump File Name field. • bkupconfig-upgrade: Downloads the backup configuration information contained in the file specified in the Configuration File Name field from the FTP/SFTP/TFTP server to the switch. • bkupconfig-backup: Backs up the backup configuration by uploading it from the switch to the FTP/SFTP/TFTP server. The backup file name is specified in the Configuration File Name field. • activeconfig-upgrade: Downloads the active configuration information contained in the file specified in the Configuration File Name field from the FTP/SFTP/TFTP server to the switch. • activeconfig-backup: Backs up the active configuration by uploading it from the switch to the FTP/SFTP/TFTP server. The active backup file name is specified in the Configuration File Name field.
Transfer Status	The transfer status of the selected Action.

USB Copy

Device Console > Configure > Config/Image/Dump Control > *USB Copy*

Use the **USB Copy** tab to copy switch image, configuration, syslog and crash dump from switch flash to USB.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 177 USB Copy field descriptions

Field	Description
Operation	Select the operation: <ul style="list-style-type: none">• FromUSB – copy from USB to Flash• ToUSB – copy from Flash to USB
File Name	Name of the USB file to be used for copy operation.
Flash File	Select the flash file slot to use for copy operation, as follows: boot, image1, active, syslog, and crashdump.
Transfer Status	The transfer status of the copy operation.

Configuring Access Users

The following sections describe configuration tasks you can perform for access users:

- [“Configuring Access User” on page 407](#)

Configuring Access User

Device Console > Configure > Access User > Access User

Use the **Access User** tab to configure access user parameters.

Note: Some fields might not be available for the selected switch type. Please disregard field descriptions that do not apply to your switch.

Table 178 Access User field descriptions

Field	Description
User Identifier	The user identification number.
Class of Service	The Class of Service level for the user.
User Name	The user name.
Password	The user password. Note that <encrypted> is displayed in this field.
State	The state indicating whether the user is enabled or not.

Configuring Layer 2 Protocols

The following sections describe configuration tasks you can perform for Layer 2 protocols:

- [“General Layer 2 Protocol Configuration” on page 409](#)

General Layer 2 Protocol Configuration

Device Console > Configure > Layer 2 > General > General

Use the **General** tab to configure Layer 2 protocol settings.

Note: Some fields might not be available for the selected switch type. Please disregard field descriptions that do not apply to your switch.

Table 179 General Layer 2 field descriptions

Field	Description
Spanning Tree State	Enables or disables Spanning Tree State.
PVST+ Compatibility	Enables or disables PVST+ compatibility mode.
VLAN Auto STG	Enables or disables VLAN automatic STG assignment.
STP Loop Guard	Enables or disables STP Loop Guard.
MAC Notification	Enables or disables MAC address Notification.

Configuring Trunks

The following sections describe trunk configuration tasks you can perform:

- [“IP Trunk Hash Configuration” on page 411](#)
- [“Trunk Groups Configuration” on page 412](#)

IP Trunk Hash Configuration

Device Console > Configure > Layer 2 > Trunk > *Trunk Hash*

Trunk hash parameters are set globally for the switch. Select one or two parameters, to configure any of the following valid combinations:

- SMAC (source MAC only)
- DMAC (destination MAC only)
- SIP (source IP only)
- DIP (destination IP only)
- SIP + DIP (source IP and destination IP)
- SMAC + DMAC (source MAC and destination MAC)

The following table describes the fields of the **Trunk Hash** configuration tab.

Table 180 Trunk Hash field descriptions

Field	Description
Layer 2 Source MAC Hash	Enable or disable trunk hashing on the source MAC.
Layer 2 Destination MAC	Enable or disable trunk hashing on the destination MAC.
Layer 2/3 Source IP Hash	Enable or disable trunk hashing on the source IP.
Layer 2/3 Destination IP Hash	Enable or disable trunk hashing on the destination IP.
Layer 2 Ingress Port/Ingress Port	Enable or disable trunk hashing on the ingress port.
Layer 2 L4 Port/L4 Port Hash	Enable or disable trunk hashing on L4 port.
Use L2 for IP Hash	Enable or disable using L2 for trunk hashing.

Trunk Groups Configuration

Device Console > Configure > Layer 2 > Trunk > *Trunk Groups*

Trunk groups provide super-bandwidth, multi-link connections between switches or other trunk-capable devices. A trunk group is a group of ports that act together, combining their bandwidth to create a single, larger virtual link. For details, see your switch's Application Guide.

The following restrictions apply:

- Any physical switch port can belong to only one trunk group.
- Best performance is achieved when all ports in any given trunk group are configured for the same speed.
- Trunking from non-IBM BLADE devices must comply with Cisco® EtherChannel® technology.

The following table describes the fields of the **Trunk Groups** configuration tab.

Table 181 Trunk Groups field descriptions

Field	Description
Trunk Group	The number of the trunk group.
Ports	The physical ports in the trunk group.
State	Enables or disables the trunk group.

LACP Trunk Group Configuration

Device Console > Configure > Layer 2 > Trunk > LACP Trunk Groups

LACP trunk groups provide aggregation of trunk lines to have super-bandwidth, multi-link connections between switches or other trunk-capable devices. An LACP trunk group is a group of trunks that act together, combining their bandwidth to create a single, larger virtual link. For details, see your switch's Application Guide.

The following table describes the fields of the **Trunk Groups** configuration tab.

Table 182 LACP Trunk Groups field descriptions

Field	Description
LACP Trunk Group	The LACP trunk group.
Admin Key	Admin Key.

Configuring LACP

The following sections describe LACP configuration tasks you can perform:

- [“LACP General Configuration” on page 415](#)
- [“LACP Ports Configuration” on page 416](#)

LACP General Configuration

Device Console > Configure > Layer 2 > LACP > LACP General

The switch supports the IEEE 802.3ad standard. At the core of the 802.3ad standard is Link Aggregation Control Protocol (LACP). This protocol lets you to group several physical ports into one logical port (LACP trunk group) with any switch that supports IEEE 802.3ad standard (LACP). You can configure the trunk groups manually, called the static trunks, as well as you can configure trunk group using the IEEE 802.3ad standard called the LACP trunks. If more than the maximum number of ports are configured in the LACP trunk, they are put in the standby state to replace any ports that fail.

LACP automatically determines which member links can be aggregated and then aggregates them. It provides for the controlled addition and removal of physical links for the link aggregation.

The following lists LACP modes:

- *off* (default): You can configure this port in to a regular static trunk group. When the system initializes, all ports are in off mode by default.
- *active*: The port is capable of forming an LACP trunk. This port initiates negotiation with the partner system port by sending LACP packets.
- *passive*: The port is capable of forming an LACP trunk. This port only responds to the negotiation requests sent from an LACP active port.

Each LACP *active* or *passive* port must have an admin key, an operational key, and an aggregator for LACP to start negotiation on these ports. You must assign the same admin key to a group of ports to make them aggregatable. Link Aggregation ID (LAG ID) is generated internally based on the operational key. All the aggregatable ports must have the same LAG ID. You can form an active LACP trunk group with all the ports that have the same LAG ID.

The following table describes the fields of the **LACP General** configuration tab.

Table 183 LACP General field descriptions

Field	Description
Actor System Priority	Defines the priority value. Lower numbers provide higher priority.
LACPDU Timeout	Defines the timeout period before invalidating LACP data from a remote partner. You can choose between short (3 seconds) or long (90 seconds) timeout periods.

LACP Ports Configuration

Device Console > Configure > Layer 2 > LACP > LACP Ports

Use the **LACP Ports** tab to configure individual ports for LACP operation.

The following table describes the fields of the **LACP Ports** configuration tab.

Table 184 LACP Ports field descriptions

Field	Description
Port	The port number
Mode	<p>The ports can be in the following modes:</p> <ul style="list-style-type: none">• off: Using this option, you can turn LACP off for this port. You can use this port to manually configure a static trunk. All ports are in off mode by default.• active: Using this option, you can turn LACP on and set this port to active. Only active ports initiate negotiation with the partner system port by sending the LACP packets.• passive: Using this option, you can turn LACP on and set this port to passive mode. Passive ports do not initiate negotiation, but only respond to the negotiation requests from active ports.
Port Priority	Sets the priority value for the selected port. Lower numbers provide higher priority.
Administrative Key	Sets the admin key for this port. Only ports with the same <code>admin</code> key and <code>oper</code> key (operational state) can form an LACP trunk group.
Minimum links	Sets the minimum links for this port.

Configuring 802.1x

The following sections describe 802.1x configuration tasks you can perform using:

- [“General 802.1x Configuration” on page 418](#)
- [“Global 802.1x Configuration” on page 419](#)
- [“Guest VLAN Configuration” on page 420](#)
- [“Port Configuration” on page 421](#)

General 802.1x Configuration

Device Console > Configure > Layer 2 > 802.1x > General

Use the **General** tab to configure 802.1x status.

Table 185 General 802.1x field descriptions

Field	Description
Status	Enables or disables 802.1x

Global 802.1x Configuration

Device Console > Configure > Layer 2 > 802.1x > Global

Use the **Global** tab to configure 802.1x properties.

Note: Some fields might not be available for the selected switch type. Please disregard field descriptions that do not apply to your switch.

Table 186 Global 802.1x field descriptions

Field	Description
Authentication Mode	Sets the type of access control as follows: forceUnauth, auto, forceAuth
EAP-Request/ Identity Quiet Period	Sets the wait-time interval before transmitting an EAP-Request/ Identity frame to the client after an authentication failure in the previous round of authentication.
Retransmission Period	Sets the wait time interval for an EAP-Response/Identity frame from the client before retransmitting an EAP-Request/Identity frame.
Supplicant Timeout	Sets the wait-time interval for an EAP-Response packet from the client before retransmitting the EAP-Request packet to the authentication server.
Server Authentication Request Timeout	Sets the wait-time interval for a response from the RADIUS server before declaring an authentication timeout.
Maximum Requests	Sets the maximum number of times the authenticator retransmits an EAP-Request packet to the client.
Re-authentication Period	Sets the wait-time interval before re-authenticating a client.
Re-authentication Status	Sets the re-authentication status (on or off).
Dynamic VLAN Assignment	Sets Dynamic VLAN assignment (on or off).

Guest VLAN Configuration

Device Console > Configure > Layer 2 > 802.1x > Guest VLAN

Use the **Guest VLAN** tab to configure 802.1x guest VLANs.

Table 187 Guest VLAN field descriptions

Field	Description
VLAN	VLAN number of the Guest VLAN.
Status	Enables or disables the Guest VLAN.

Port Configuration

Device Console > Configure > Layer 2 > 802.1x > Port

Use the **Port** tab to configure 802.1x port parameters.

Note: Some fields might not be available for the selected switch type. Please disregard field descriptions that do not apply to your switch.

Table 188 Port 802.1x field descriptions

Field	Description
Port	Port Index
Authentication Mode	Sets the access control type as follows: forceUnauth, auto, forceAuth
EAP-Request/ Identity Quiet Period	Sets the wait period before transmitting an EAP-Request/Identity frame to the client after an authentication failure in the previous round of authentication.
Retransmission Period	Sets the wait period for an EAP-Response/Identity frame from the client before retransmitting an EAP-Request/Identity frame.
Supplicant Timeout	Sets the wait period for an EAP-Response packet from the client before retransmitting the EAP-Request packet to the authentication server.
Server Authentication Request Timeout	Sets the wait period for a response from the RADIUS server before declaring an authentication timeout.
Maximum Requests	Sets the maximum number of times the authenticator retransmits an EAP-Request packet to the client.
Re-authentication Period	Sets the wait period before re-authenticating a client when periodic re-authentication is enabled.
Re-authentication Status	Sets the re-authentication status (on or off).
Dynamic VLAN Assignment	Sets Dynamic VLAN assignment (on or off).

Configuring MSTP and RSTP

The following sections describe the configuration tasks you can perform to MSTP and RSTP:

- [“MSTP/RSTP Configuration” on page 423](#)

MSTP/RSTP Configuration

Device Console > Configure > Layer 2 > MSTP/RSTP > *MSTP*

Use MSTP tab to configure and manage parameters for Multiple Spanning Tree Protocol (MSTP) and Rapid Spanning Tree Protocol (RSTP).

Note: Some fields might not be available for the selected switch type. Please disregard field descriptions that do not apply to your switch.

The following table describes the fields of the **MSTP** configuration tab.

Table 189 MSTP and RSTP field descriptions

Field	Description
MSTP/RSTP	Enables or disables the bridge MSTP or RSTP.
Region's Name	Sets the region name for MST.
MST Region Revision/MST Region Version	Sets the region revision being used for MST.
Maximum Hop Count	Sets the maximum hop count value for the MST.
Spanning Tree Mode	Specifies whether MSTP, RSTP, or PVRST is being used.

Configuring CIST

The following sections describe the configuration tasks you can perform to Common and Internal Spanning Tree (CIST):

- [“CIST Bridge Configuration” on page 425](#)
- [“CIST Port Configuration” on page 426](#)

CIST Bridge Configuration

Device Console > Configure > Layer 2 > CIST > CIST Bridge

Use the CIST Bridge tab to configure CIST bridge parameters.

The following table describes the fields of the **CIST Bridge** configuration tab.

Table 190 CIST Bridge field descriptions

Field	Description
Bridge Priority	Sets the CIST bridge priority value.
Bridge Root Maximum Age	Sets the time (in seconds) for the maximum age of a CIST bridge root.
Bridge Root Forward Delay	Sets the time (in seconds) for a CIST bridge root forward delay.
Virtual LANs	Defines a list of VLANs associated with the CIST.

CIST Port Configuration

Device Console > Configure > Layer 2 > CIST > CIST Port

Use the CIST Port tab to configure CIST bridge port parameters.

The following table describes the fields of the **CIST Port** configuration tab.

Table 191 CIST Port field descriptions

Field	Description
Port	Specifies the CIST bridge port being configured.
Priority	Configures the port priority. The port priority helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment.
Path Cost	Configures the port path cost. The port path cost is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. A value of 0 indicates that the default cost is computed for an auto negotiated link speed.
Link Type	Sets the port link type.
Edge Port	Enables or disables this port as an edge port.
Spanning Tree State	Enable or disables STP for this port.
Hello Time	Sets the Hello interval in seconds.
PVST Protection	Enables or disables PVST Protection for this port.

Configuring Spanning Tree Protocol

The following sections describe the configuration tasks you can perform to Spanning Tree Protocol (STP):

- [“Spanning Tree Configuration” on page 428](#)
- [“STP Groups Configuration” on page 431](#)
- [“STG Port Configuration” on page 432](#)

Spanning Tree Configuration

Device Console > Configure > Layer 2 > Spanning Tree Protocol > *Spanning Tree*

Use the Spanning Tree tab to configure STP properties.

Note: Some fields might not be available for the selected switch type. Please disregard field descriptions that do not apply to your switch.

The following table describes the fields of the **Spanning Tree** configuration tab.

Table 192 Spanning Tree Protocol field descriptions

Field	Description
Protocol Type	Displays the version of Spanning Tree Protocol, as follows: <ul style="list-style-type: none"> • decLb100(2) indicates the DEC LANbridge 100 Spanning Tree Protocol • ieee8021d(3) indicates IEEE 802.1d
Priority	Configures the bridge priority. The bridge priority parameter controls which bridge on the network is the STP root bridge. To make this switch the root bridge, configure the bridge priority lower than all other switches and bridges on your network. The lower the value, the higher the bridge priority.
Last Topology Change	The time since a topology change was last detected by the bridge. Time is displayed in days:hours:minutes:seconds.
Total Topology Changes	Displays total number of topology changes that were detected by the bridge.
Root Identifier	The bridge identifier of the root of the spanning tree. This value is used as the Root Identifier parameter in all the configuration bridge protocol data units (PDU) that were originated by this node.
Root Cost	The cost of the path to the root as seen from this bridge.
Root Port	The number of the port that offers the lowest cost path from this bridge to the root bridge.
Maximum Age	Configures the bridge maximum age. The maximum age parameter specifies the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it re-configures the STP network.

Table 192 Spanning Tree Protocol field descriptions

Field	Description
Hello Interval	Configures the bridge hello time. The hello time specifies how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value. The value is entered in units of 1/100 of a second. Therefore, the default value of 2 seconds is displayed in this field as 200. The time is measured when the bridge is the root of the spanning tree (or trying to become so).
Forwarding Delay	The time for a port to change its spanning state when moving to a Forwarding state. Forwarding Delay determines how long the port stays in the Listening and Learning states that precede the Forwarding state. This value is also used for aging all dynamic entries in the Forwarding Database, after a topology change. Forwarding Delay is displayed in units of 1/100 of a second. The bridge uses this value, unless the bridge becomes the root. In that case, Forwarding Delay becomes the value that all bridges, including this one, use when this bridge becomes the root.
Root Maximum Age	Sets the Maximum bridge age. When this bridge is acting as the root, all bridges use Root Maximum Age for Maximum Age: 6 to 40 seconds. The value is entered into this field in units of 1/100 of a second. Therefore, the default value of 20 seconds is displayed in this field as 2000. Maximum Age is an integer: an error may be returned if the input value is not a whole number.
Root Hello Interval	Sets the value that all bridges use for Hello Interval when this bridge is acting as the root: 1 to 10 seconds. The value is entered into this field in units of 1/100 of a second. Therefore, the default value of 2 seconds is displayed in this field as 200. Hello Root Interval is an integer: an error may be returned if the input value is not a whole number.
Root Forwarding Delay	Sets the state change delay. When this bridge is acting as the root, all bridges use Root Forwarding Delay for Forwarding Delay: 4 to 30 seconds. The value is entered in units of 1/100 of a second. Therefore, the default value of 15 seconds is displayed in this field as 1500. Root Forwarding Delay is an integer: an error may be returned if the input value is not a whole number.
Aging Time	Sets the time-out period, in seconds, for the dynamically-learned forwarding information.
Hold Time	The time value that determines the interval length during which no more than two Configuration bridge PDUs shall be transmitted by this node, in units of 1/100 of a second.

Table 192 Spanning Tree Protocol field descriptions

Field	Description
Uplink Fast	Enables or disables Fast Uplink Convergence, which provides rapid Spanning Tree convergence to an upstream switch during failover. Note: When enabled, this feature increases bridge priorities to 65500 for all STGs and path cost by 3000 for all external STP ports.
Station Update Rate	Configures the station update rate, in packets per second.
BPDU Guard	Enables or disables BPDU guard, to avoid spanning-tree loops on ports with Port Fast Forwarding enabled.

STP Groups Configuration

Device Console > Configure > Layer 2 > Spanning Tree Protocol > STP Groups

Use the STP Groups tab to configure and maintain Spanning Tree Groups.

Note: Some fields might not be available for the selected switch type. Please disregard field descriptions that do not apply to your switch.

The following table describes the fields of the **STP Groups** configuration tab.

Table 193 STP Groups field descriptions

Field	Description
Index	The Spanning Tree Group (STG) index number.
State	The current state (on or off) of Spanning Tree Protocol for the Spanning Tree Group.
Priority	Configures the bridge priority. The bridge priority parameter controls which bridge on the network is the STP root bridge. To make this switch the root bridge, configure the bridge priority lower than all other switches and bridges on your network. The lower the value, the higher the bridge priority. The range is 0 to 65535, and the default is 32768.
Hello Time	Configures the bridge hello time. The hello time specifies how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value. The range is 1 to 10 seconds, and the default is 2 seconds.
Forward Delay	Configures the bridge forward delay parameter. The forward delay parameter specifies the amount of time that a bridge port has to wait before it changes from the listening state to the learning state and from the learning state to the forwarding state. The range is 4 to 30 seconds, and the default is 15 seconds.
Maximum Age	Configures the bridge maximum age. The maximum age parameter specifies the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it re configures the STP network. The range is 6 to 40 seconds, and the default is 20 seconds.
Aging Time	Configures the forwarding database aging time. The aging time specifies the amount of time the bridge waits without receiving a packet from a station before removing the station from the forwarding database. The range is 1 to 65535 seconds, and the default is 300 seconds. To disable aging, set this parameter to 0.
VLANs	Displays the VLANs in the Spanning Tree Group.

STG Port Configuration

Device Console > Configure > Layer 2 > Spanning Tree Protocol > STG Port

Use the STG Port tab to configure and manage STG ports.

Note: Some fields might not be available for the selected switch type. Please disregard field descriptions that do not apply to your switch.

The following table describes the fields of the **STG Port** configuration tab.

Table 194 STG Port field descriptions

Field	Description
Group Index	The Spanning Tree Group (STG) number.
Port	The port number that is associated with the Spanning Tree Group.
Port State	Shows the STP port state information as either on or off.
Priority	Configures the port priority. The port priority helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment.
Path Cost	Configures the port path cost. The port path cost is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. A value of 0 indicates that the default cost is computed for an auto negotiated link speed.
Port Link Type	Sets the port link type.
Port Edge State	Enables or disables this port as an edge port.
Fast Forwarding	Enables or disables Port Fast Forward on the port.

Configuring Forwarding Database

The following sections describe the configuration tasks you can perform to Forwarding Database (FDB):

- [“FDB General Configuration” on page 434](#)
- [“FDB Static Configuration” on page 435](#)
- [“FDB Static Multicast Configuration” on page 436](#)

FDB General Configuration

Device Console > Configure > Layer 2 > Forwarding Database > FDB General

Use the FDB General tab to configure general FDB properties.

Note: Some fields might not be available for the selected switch type. Please disregard field descriptions that do not apply to your switch.

The following table describes the fields of the **FDB General** configuration tab.

Table 195 Forwarding Database General field descriptions

Field	Description
FDB Aging Value	Configures the aging value for FDB entries.
FDB Learning	Enables or disables the process of learning FDB entries.
Flooding	Enables or disables FDB flooding.

FDB Static Configuration

Device Console > Configure > Layer 2 > Forwarding Database > FDB Static

Use the **FDB Static** tab to configure static entries in the FDB.

Note: Some fields might not be available for the selected switch type. Please disregard field descriptions that do not apply to your switch.

The following table describes the fields of the **FDB Static** configuration tab.

Table 196 Forwarding Database Static field descriptions

Field	Description
Index	Configures the FDB entry number.
MAC Address	Configures the MAC address of the static FDB entry.
VLAN	Configures the VLAN number of the static FDB entry.
Port	Configures the port number of the static FDB entry.
Type	Sets the type (<code>port</code> , <code>trunk</code> , <code>adminkey</code>).
Trunk	Configures the trunk number. This field applies only if Type is set to <code>trunk</code> .
Adminkey	Configures the LACP adminkey . This field applies only if the Type is set to <code>adminkey</code> .

FDB Static Multicast Configuration

Device Console > Configure > Layer 2 > Forwarding Database > Static Multicast

Use the **Static Multicast** tab to configure FDB static multicast entries.

Note: Some fields might not be available for the selected switch type. Please disregard field descriptions that do not apply to your switch.

Table 197 FDB Static Multicast field descriptions

Field	Description
Index	Configures the FDB entry number.
MAC Address	Configures the MAC address of the static multicast FDB entry.
VLAN	Configures the VLAN number of the static multicast FDB entry.
Ports	Configures the port numbers of the static multicast FDB entry.

Configuring Virtual Link Aggregation Groups

The following sections describe the configuration tasks associated with Virtual Link Aggregation Groups (VLAGs):

- [“General Configuration” on page 438](#)
- [“Health Check Configuration” on page 439](#)
- [“Trunk Configuration” on page 440](#)
- [“LACP Configuration” on page 441](#)
- [“Inter-Switch Link \(ISL\) Configuration” on page 442](#)

General Configuration

Device Console > Configure > Layer 2 > VLAG > General

Use the **General** tab to configure general VLAG properties.

Table 198 VLAG General field descriptions

Field	Description
Peer IP Address	Sets the IP address of the VLAG peer.
System Priority	Sets the VLAG priority for the switch used for election of Primary and Secondary VLAG switches.
Health Check Peer IP Address	Sets the IP address of the peer switch used for health checks.
Tier ID	Sets the VLAG Tier ID.
StartUp Delay Interval	Sets the VLAG startup Delay Timer interval.
Global State	Enables or disables VLAG globally on the switch.

Health Check Configuration

Device Console > Configure > Layer 2 > VLAG > Health Check

Use the Health Check tab to set VLAG health check parameters.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch. .

Table 199 VLAG Health Check field descriptions

Field	Description
Peer IP Address	Sets the IP address of the peer switch used for health checks.
Connect Retry Interval	Sets the interval at which the retry attempt will be made to connect to the peer.
Attempts	Sets the number of keep-alive attempts.
Interval	Sets the interval between keep-alive messages sent during health checks.

Trunk Configuration

Device Console > Configure > Layer 2 > VLAG > *Trunk*

Use the **Trunk** tab to configure VLAG trunk groups.

Table 200 VLAG Trunk field descriptions

Field	Description
Trunk Groups	Sets the trunk group as VLAG.
State	Enables or disables VLAG for this trunk group.

LACP Configuration

Device Console > Configure > Layer 2 > VLAG > LACP

Use the **LACP** tab to configure LACP trunks for VLAG.

Table 201 VLAG LACP field descriptions

Field	Description
LACP Admin Key	Sets the LACP <i>admin key</i> .
State	Enables or disables LACP <i>admin key</i> .

Inter-Switch Link (ISL) Configuration

Device Console > Configure > Layer 2 > VLAG > ISL

Use the **ISL** tab to configure Inter-Switch Links for VLAG.

Table 202 VLAG ISL field descriptions

Field	Description
Trunk	Sets the trunk group for the VLAG Inter-Switch Link (ISL).
Admin Key	Sets the LACP <i>admin key</i> for the VLAG Inter-Switch Link.
VLAN	Sets the VLAN to carry VLAG protocol data.

Configuring Hot Links

The following sections describe the configuration tasks associated with Hot Links:

- [“Hot Links General Configuration” on page 444](#)
- [“Hot Links Triggers Configuration” on page 445](#)

Hot Links General Configuration

Device Console > Configure > Layer 2 > Hot Links > General Configuration

Use the General Configuration tab to configure general Hot Links properties.

Note: This tab is available only for certain switch types. In addition, some fields might not be available for the selected switch type. Please disregard the information if it does not apply to your switch.

The following table describes the fields of the **Hot Links** General Configuration tab.

Table 203 Hot Links General field descriptions

Field	Description
Hot Links	Enables or disables Hot Links.
FDB Update	Enables or disables Hot Links FDB Update.
FDB Update Rate	Sets FDB update rate in packets per second.
BPDU Flood	Enables or disables Hot Links BPDU Flooding.

Hot Links Triggers Configuration

Device Console > Configure > Layer 2 > Hot Links > Triggers

Use the Triggers tab to configure Hot Links triggers.

Note: This tab is available only for certain switch types. In addition, some fields might not be available for the selected switch type. Please disregard the information if it does not apply to your switch.

The following table describes the fields of the **Triggers** tab.

Table 204 Hot Links Triggers field descriptions

Field	Description
Trigger ID	The trigger identifier.
Name	The trigger name.
State	Enables or disables Trigger state.
Preemption State	Enables or disables Preemption state.
Forward Delay	Forward Delay setting, in seconds.
Master Port	The master interface port number.
Master Trunk	The master interface trunk number.
Master Adminkey	The master interface <i>admin key</i> number.
Backup Port	The backup interface port number.
Backup Trunk	The backup interface trunk number.
Backup Adminkey	The backup interface <i>admin key</i> number.

Configuring Virtual LANs

The following sections describe the configuration tasks associated with Virtual LANs (VLANs):

- [“VLAN Memberships Configuration” on page 447](#)
- [“Private VLAN Configuration” on page 448](#)
- [“Private VLAN Configuration” on page 448](#)
- [“VMAP Configuration for Non-Server Ports” on page 450](#)
- [“VMAP Configuration for Server Ports” on page 451](#)
- [“VMAP Configuration for All Ports” on page 452](#)

VLAN Memberships Configuration

Device Console > Configure > Layer 2 > Virtual LANs > VLAN Memberships

Use Virtual Local Area Networks (VLANs) to split up groups of network users into manageable broadcast domains, to create logical segmentation of workgroups, and to enforce security policies among logical segments.

Note: All ports must belong to at least one VLAN. Any port which is removed from a VLAN and which is not a member of any other VLAN is automatically added to default VLAN 1. A port cannot be removed from VLAN 1 if the port has no membership in any other VLAN. Also, a port cannot be part of more than one VLAN unless it is configured for VLAN tagging.

Use the VLAN Memberships General tab to configure general FDB properties.

The following table describes the fields of the **VLAN Memberships** configuration tab.

Table 205 VLAN Memberships field descriptions

Field	Description
VLAN	The VLAN identification number. The number can be set when a VLAN is inserted or modified.
Name	The VLAN name. The default is none, except for the first VLAN name, which has a default name of Default VLAN.
Ports	The ports in the VLAN. The default is none except for VLAN 1. By default, all ports belong to VLAN 1. To select the ports belonging to the VLAN group by Click Ports... or double-click on the ports column in the table to select the ports belonging to the VLAN group.
State	Enables or disables a VLAN.
Spanning Tree Group	The Spanning Tree Group (STG) assigned to the VLAN. To choose an STG, double-click on the field. Then right-click to select Browse...
Management State	Enables or disables Management VLAN.
Virtual Ports	Displays a list of configured virtual ports in the VLAN.

Private VLAN Configuration

Device Console > Configure > Layer 2 > Virtual LANs > Private VLAN

Use this feature to configure Private VLANs.

Table 206 Private VLAN field descriptions

Field	Description
VLAN	The VLAN ID configured as Private VLAN.
VLAN Type	The VLAN type, as follows: none, primary, isolated, community
Primary VLAN	Sets Private VLAN mapping between a primary and a secondary VLAN.
State	Enables or disables Private VLAN.

Protocol VLAN Configuration

Device Console > Configure > Layer 2 > Virtual LANs > Protocol VLAN

Use this feature to configure Protocol VLANs (PVLANS).

Table 207 Protocol VLAN field descriptions

Field	Description
VLAN	The VLAN ID configured as Protocol VLAN.
Protocol VLAN Identifier	Sets the priority value for this PVLAN.
Frame Type	Sets the frame type for the selected protocol.
Ether Type	Sets the ether type for the selected protocol.
Predefined Protocol	Sets the predefined protocol.
Priority	Sets the protocol priority.
State	Enables or disables the selected protocol on the VLAN.
Ports	List of ports belongs to the selected protocol on this VLAN.
Tagged Ports	List of ports that will be tagged by the selected protocol on this VLAN.

VMAP Configuration for Non-Server Ports

Device Console > Configure > Layer 2 > Virtual LANs > *VMAP for Non Server Ports*

Use this feature to add or remove a VLAN Map to non-server ports.

Note: This tab is available only for VMready capable switches. Please disregard this information if it does not apply to your switch.

Table 208 VMAP for Non-Server Ports field descriptions

Field	Description
VLAN ID	The VLAN Id.
VMAP	List of VLAN Maps

VMAP Configuration for Server Ports

Device Console > Configure > Layer 2 > Virtual LANs > VMAP for Server Ports

Use this feature to add or remove a VLAN Map to server ports.

Note: This tab is available only for VMready capable switches. Please disregard this information if it does not apply to your switch.

The following table describes the fields of the **VMAP for Server Ports** configuration tab.

Table 209 VMAP for Server Ports field descriptions

Field	Description
VLAN ID	The VLAN Id.
VMAP	List of VLAN Maps

VMAP Configuration for All Ports

Device Console > Configure > Layer 2 > Virtual LANs > VMAP for All Ports

Use this feature to add or remove a VLAN Map to External and Internal ports.

Note: This tab is available only for VMready capable switches. Please disregard this information if it does not apply to your switch.

The following table describes the fields of the **VMAP for All Ports** configuration tab.

Table 210 VMAP for All Ports field descriptions

Field	Description
VLAN ID	VLAN identifier.
VMAP	List of VLAN Maps

Configuring Link Layer Discovery Protocol (LLDP)

The following sections describe the configuration tasks associated with LLDP:

- [“LLDP General Configuration” on page 454](#)
- [“LLDP Port Configuration” on page 455](#)
- [“Port Global TLV State” on page 457](#)

LLDP General Configuration

Device Console > Configure > Layer 2 > LLDP > General

Use the LLDP General tab for enabling or disabling LLDP state and configuring general parameters.

Note: This tab or some fields might not be available for the selected switch type. Please disregard this tab or field descriptions that do not apply to your switch.

Table 211 LLDP General field descriptions

Field	Description
LLDP State	Enable or disable LLDP state.
Transmission Interval	Sets the message transmission interval in seconds.
Holdtime Multiplier	Sets the message hold time multiplier.
Notification Interval	Sets the trap notification interval, in seconds.
Transmission Delay	Sets the message transmission delay, in seconds.
Reinitialization Delay	Sets the re-initialization delay, in seconds.

LLDP Port Configuration

Device Console > Configure > LLDP > LLDP Port

Use the LLDP Port tab to enable or disable EDCP TLV State of the ports.

Note: This tab is available only for LLDP capable switches. Please disregard this information if it does not apply to your switch.

Table 212 LLDP Port field descriptions

Field	Description
Port	Port number.
Admin Status	Enables or disables the admin status of the LLDP port.
SNMP Trap Notification	Enables or disables the SNMP trap notification state of the LLDP port.
Port Description TLV State	Enables or disables Port Description TLV state of the LLDP port.
System Name TLV State	Enables or disables System Name TLV state of the LLDP port.
System Description TLV State	Enables or disables System Description TLV state of the LLDP port.
System Capabilities TLV State	Enables or disables System Capabilities TLV state of the LLDP port.
Management Address TLV State	Enables or disables Management Address TLV state of the LLDP port.
Port VLAN ID TLV State	Enables or disables Port VLAN ID TLV state of the LLDP port.
Port-Protocol VLAN ID TLV State	Enables or disables Port and Protocol VLAN ID TLV state of the LLDP port.
VLAN Name TLV State	Enables or disables VLAN Name TLV state of the LLDP port.
Protocol Identity TLV State	Enables or disables Protocol Identity TLV state of the LLDP port.
MAC/PHY Config/Status TLV State	Enables or disables MAC/PHY Configuration/Status TLV state of the LLDP port.
Power Via MDI TLV State	Enables or disables Power Via MDI TLV state of the LLDP port.
Link Aggregation TLV State	Enables or disables Link Aggregation TLV state of the LLDP port.
Maximum Frame Size TLV State	Enables or disables Maximum Frame Size TLV state of the LLDP port.

Table 212 LLDP Port field descriptions

Field	Description
EDCP TLV State	Enables or disables EDCP TLV state.
ALL LLDP Ports State	Set the corresponding state for all the LLDP port's TLVs.
DCBX TLV State	Enables or disables DCBX TLV state of the LLDP port.

Port Global TLV State

Device Console > Configure > Layer 2 > LLDP > *Port Global TLV State*

Use the **Port Global TLV State** tab to set LLDP port's TLV state.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 213 Port Global TLV State field descriptions

Field	Description
Port	The port index.
Global TLV State	Select the global TLV state for the port.

Configuring Failover

The following sections describe the tasks associated with Failover configuration:

- [“General Configuration” on page 459](#)
- [“Triggers Configuration” on page 460](#)

General Configuration

Device Console > Configure > Layer 2 > Failover > General

Use the **General** tab to enable or disable Layer 2 Failover.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 214 Failover General Configuration field descriptions

Field	Description
Failover State	Enables or disables Failover.
VLAN State	Enables or disables Failover VLAN Monitor.

Triggers Configuration

Device Console > Configure > Layer 2 > Failover > *Trigger*

Use the **Trigger** tab to set Failover Triggers.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 215 Failover Triggers field descriptions

Field	Description
Trigger Identifier	The Failover trigger identifier.
State	Enables or disables the trigger state.
Limit	Sets the minimum number of operational links allowed within each trigger before the trigger initiates a failover event.
	Auto Monitor (AM)
AM Trunk	Adds a trunk group to the Auto Monitor port configuration.
AM Key	Adds a LACP admin key to the Auto Monitor.
	Manual Monitor (MM)
MM Port	Adds the selected port to the Manual Monitor port configuration.
MM Trunk	Adds a trunk group to the Manual Monitor port configuration.
MM Key	Adds an LACP admin key to the Manual Monitor.
	Manual Control (MC)
MC Port	Adds the selected port to the Manual Control port configuration.
MC Trunk	Adds a trunk group to the Manual Control port configuration.
MC Key	Adds an LACP admin key to the Manual Control.

Configuring Active Multipath Protocol (AMP)

The following sections describe the configuration tasks associated with Active Multipath Protocol (AMP):

- [“General Configuration” on page 462](#)
- [“Group Configuration” on page 463](#)

General Configuration

Device Console > Configure > Layer 2 > AMP > General

Use the **General** tab to configure AMP properties.

Table 216 AMP General field descriptions

Field	Description
AMP State	Globally enables or disables Active Multipath Protocol (AMP).
Switch Type	Sets the active multipath switch type to access or aggregator.
Switch Priority	Sets the AMP priority for the switch. A lower priority value denotes a higher precedence. It is recommended that aggregator switches be configured with lower priority values than access switches.
Keep Alive Interval	Sets the time interval between AMP keep alive messages.
Keep Alive Timeout Count	Sets the timeout count, which is the number of unreceived keep-alive packets the switch waits before declaring a timeout due to loss of connectivity with the peer.
Aggregator Link Type	Sets the Aggregator Link Type as follows: port, trunk, lacp
Aggregator Link Id	Sets the consistent value for Aggregator Link Type.

Group Configuration

Device Console > Configure > Layer 2 > AMP > Group

Use the **Group** tab to configure AMP groups.

Table 217 AMP Group field descriptions

Field	Description
Index	AMP Group Index.
State	Enables or disables AMP Group.
First Link Type	Sets First AMP Link Type as follows: none, port, trunk, lacp
First Link Id	Sets the consistent value for First Link type.
Second Link Type	Sets Second AMP Link Type as follows: none, port, trunk, lacp
Second Link Id	Sets the consistent value for Second Link type.

Configuring Edge Control Protocol (ECP)

The following sections describe the configuration tasks associated with ECP:

- [“ECP General Configuration” on page 465](#)

ECP General Configuration

Device Console > Configure > Layer 2 > ECP > General

Use the **General** tab to configure ECP properties.

Note: This tab is available only for ECP-capable switches. Please disregard this information if it does not apply to your switch.

Table 218 ECP General field descriptions

Field	Description
Retransmission Interval	Sets ECP retransmission interval in milliseconds.

Configuring IP Interfaces

The following sections describe the configuration tasks associated with IP interfaces:

- [“IP General Configuration” on page 467](#)
- [“IP Interfaces Configuration” on page 468](#)
- [“IP Forwarding Configuration” on page 469](#)
- [“Network Filters Configuration” on page 470](#)
- [“Loopback Interfaces Configuration” on page 471](#)
- [“Static ARP Configuration” on page 472](#)

IP General Configuration

Device Console > Configure > Layer 3 > IP > General

Use the **General** tab to set the Router ID.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

IP Interfaces Configuration

Device Console > Configure > Layer 3 > IP > Interfaces

Use the IP Interfaces tab to configure IP Interfaces.

Note: This tab is available only for certain switch types. In addition, some fields might not be available for the selected switch type. Please disregard the information if it does not apply to your switch.

The following table describes the fields of the **IP Interfaces** tab.

Table 219 IP Interfaces field descriptions

Field	Description
Index	Index number of the interface.
MTU	Sets the maximum transmission unit (MTU) for the interface.
Admin Status	Sets the administrative status (up, down, testing).
Port Name	Sets the port name (alias).
IP Interface	The IP interface number. This number can be set when an IP interface is inserted.
Address	The IP address of the interface in IPv4 interfaces.
Mask	The subnet mask of the interface in IPv4 interfaces.
VLAN	The VLAN associated with the interface. Each interface can belong to one VLAN, although any VLAN can have multiple IP interfaces associated with it.
State	Enables or disables the state of the interface.
Boot Relay	Enables or disables the BOOTP relay.

IP Forwarding Configuration

Device Console > Configure > Layer 3 > IP > Forwarding

Use the Forwarding tab to configure IP Forwarding.

Table 220 IP Forwarding field descriptions

Field	Description
Forwarding State	Sets the forwarding state (on or off).
Directed Broadcasts	Enables or disables directed broadcasts.
ICMP Redirects	Enables or disables ICMP Redirects.
ICMPv6 Redirects	Enables or disables ICMPv6 Redirects.

Network Filters Configuration

Device Console > Configure > Layer 3 > IP > *Network Filters*

Use this tab to configure network filters.

Table 221 Network Filters field descriptions

Field	Description
Index	The index number of the network filter.
Address	Sets the IP address.
Mask	Sets the IP subnet mask.
State	Enables or disables the network filter.

Loopback Interfaces Configuration

Device Console > Configure > Layer 3 > IP > *Loopback Interfaces*

Use this tab to configure loopback interfaces.

Table 222 Loopback Interfaces field descriptions

Field	Description
Index	The index number of the loopback interface.
Address	Sets the IP address.
Mask	Sets the IP subnet mask.
State	Enables or disables the loopback interface.

Static ARP Configuration

Device Console > Configure > Layer 3 > IP > *Static ARP*

Use this tab to configure static ARP entries.

Table 223 Static ARP field descriptions

Field	Description
Index	The index number of the static ARP entry.
Interface	Sets the IP interface for the entry.
Address	Sets the IP address of the entry.
MAC Address	Sets the MAC address for the entry.

Configuring Gateways

The following sections describe the configuration tasks associated with gateways:

- [“Gateways Configuration” on page 474](#)

Gateways Configuration

Device Console > Configure > Layer 3 > Gateways > Gateways

Use the Gateways tab to configure gateways.

Note: This tab is available only for certain switch types. In addition, some fields might not be available for the selected switch type. Please disregard the information if it does not apply to your switch.

The following table describes the fields of the **Gateways** tab.

Table 224 Gateways field descriptions

Field	Description
Index	The gateway index number.
IP Address	Sets the IPv4 address of the default gateway.
Interval	Sets the interval between ping attempts.
Retries	Sets the number of failed attempts to declare the default gateway down.
State	Enables or disables the default gateway.
ARP	Enables or disables the Address Resolution Protocol health checks.

Configuring Routes

The following sections describe the tasks associated with Routes configuration:

- [“General Configuration” on page 476](#)
- [“IP Static Routes Configuration” on page 477](#)
- [“IPMC Ports Configuration” on page 478](#)
- [“IPMC Trunks Configuration” on page 479](#)
- [“IPMC Adminkeys Configuration” on page 480](#)

General Configuration

Device Console > Configure > Layer 3 > Routes > General

Use the **General** tab to configure Routes health check and hash parameters.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 225 Routes General Configuration field descriptions

Field	Description
Ping Interval for ECMP Health Check	Sets the ECMP health-check ping interval, in seconds.
Retries for ECMP Health Check	Sets the number of ECMP health-check retries.
ECMP Hash	Sets ECMP hashing parameters: dipsip, sip
Gateway Health Check	Enables or disables Gateway health-check functionality.

IP Static Routes Configuration

Device Console > Configure > Layer 3 > Routes > *IP Static Routes*

Use the **IP Static Routes** tab to configure Static Routes.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 226 IP Static Routes Configuration field descriptions

Field	Description
Index	The index of the static routing table.
Destination IP	Sets the destination IP address for this route.
Subnet Mask	Sets the subnet mask for this route.
Gateway	Sets the IP address of the gateway for this route.
Route IP Interface	Sets the IP interface for this route.

IPMC Ports Configuration

Device Console > Configure > Layer 3 > Routes > IPMC Ports

Use the **IPMC Ports** tab to configure IPMC ports.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 227 IPMC Ports Configuration field descriptions

Field	Description
Index	The index of the IPMC static routing table.
Destination IP	Sets the destination IPMC address for this route.
VLAN	Sets the VLAN ID for this IPMC route.
Host Ports	Sets the ports as host ports for this IPMC route.
Primary Ports	Sets the ports as primary ports for this IPMC route.
Backup Ports	Sets the ports as backup ports for this IPMC route.
Virtual Router	Sets the virtual router ID for this IPMC route.
Delete	Clears Host Ports or Primary Ports or Backup Ports from this IPMC route.

IPMC Trunks Configuration

Device Console > Configure > Layer 3 > Routes > IPMC Trunks

Use the **IPMC Trunks** tab to configure IPMC trunks.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 228 IPMC Trunks Configuration field descriptions

Field	Description
Index	The index of the IPMC static routing table.
Destination IP	Sets the destination IPMC address for this route.
VLAN	Sets the VLAN ID for this IPMC route.
Host Trunk	Sets the trunk as host trunk for this IPMC route.
Primary Trunk	Sets the trunk as primary trunk for this IPMC route.
Backup Trunk	Sets the trunk as backup trunk for this IPMC route.
Virtual Router	Sets the virtual router ID for this IPMC route.
Host Ports	Shows the ports of host trunks configured for this IPMC route.
Primary Ports	Shows the ports of primary trunks configured for this IPMC route.
Backup Ports	Shows the ports of backup trunks configured for this IPMC route.
Delete	Clears Host Trunk(s) or Primary Trunk(s) or Backup Trunk(s) from this IPMC route.

IPMC Adminkeys Configuration

Device Console > Configure > Layer 3 > Routes > IPMC Adminkeys

Use the **IPMC Adminkeys** tab to configure IPMC *admin keys*.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 229 IPMC Adminkeys Configuration field descriptions

Field	Description
Index	The index of the IPMC static routing table.
Destination IP	Sets the destination IPMC address for this route.
VLAN	Sets the VLAN ID for this IPMC route.
Host Adminkey	Sets the adminkey as host adminkey for this IPMC route.
Primary Adminkey	Sets the adminkey as primary adminkey for this IPMC route.
Backup Adminkey	Sets the adminkey as backup adminkey for this IPMC route.
Virtual Router	Sets the virtual router ID for this IPMC route.
Host Ports	Shows the ports of host adminkeys configured for this IPMC route.
Primary Ports	Shows the ports of primary adminkeys configured for this IPMC route.
Backup Ports	Shows the ports of backup adminkeys configured for this IPMC route.
Delete	Clears Host Adminkey(s) or Primary Adminkey(s) or Backup Adminkey(s) from this IPMC route.

Configuring RMAPs

The following sections describe the tasks associated with RMAP configuration:

- [“General Configuration” on page 482](#)
- [“Access List Configuration” on page 483](#)
- [“AS-Path Access List Configuration” on page 484](#)

General Configuration

Device Console > Configure > Layer 3 > RMAP > General

Use the **General** tab to configure RMAP parameters.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 230 RMAP General Configuration field descriptions

Field	Description
RMAP	The route map index.
Local Preference	Sets the local preference of the matched route.
AS-Path	Sets AS-Path Prepend of the matched route.
Precedence	Sets the precedence of the route map.
Metric Type	Sets metric-type of the matched route: none, type 1, or type 2
Metric	Sets the metric of the route map.
Weight	Sets the weight of the route map.
State	Enables or disables the route map.

Access List Configuration

Device Console > Configure > Layer 3 > RMAP > Access List

Use the **Access List** tab to configure RMAP Access List.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 231 RMAP Access List Configuration field descriptions

Field	Description
RMAP	The route map index.
Access List	Sets the IP access list.
Network Filter	Sets the network filter for the route map access list.
Metric	Sets the metric for the route map access list.
Action	Sets the action for the route map access list: permit or deny
State	Enables or disables the route map access list.

AS-Path Access List Configuration

Device Console > Configure > Layer 3 > RMAP > AS-Path Access List

Use the **AS-Path Access List** tab to configure RMAP Autonomous System path Access List.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 232 RMAP AS-Path Access List Configuration field descriptions

Field	Description
RMAP	The route map index.
AS-path Index	Sets the Autonomous System (AS) path index.
AS Number	Sets AS filter's path number.
Action	Sets the AS filter action: permit or deny
State	Enables or disables the AS filter.

Configuring RIP

The following sections describe the tasks associated with RIP configuration:

- [“General Configuration” on page 486](#)
- [“RIP Interface Configuration” on page 487](#)
- [“Static Route Redistribute Configuration” on page 488](#)
- [“BGP External Route Redistribute Configuration” on page 489](#)
- [“BGP Internal Route Redistribute Configuration” on page 490](#)
- [“Fixed Route Redistribute Configuration” on page 491](#)
- [“OSPF Route Redistribute Configuration” on page 492](#)
- [“OSPF External Route Redistribute Configuration” on page 493](#)

General Configuration

Device Console > Configure > Layer 3 > RIP > General

Use the **General** tab to configure RIP state and update period

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 233 RIP General Configuration field descriptions

Field	Description
Global RIP State	Enables or disables RIP.
Update Period	Sets the time interval for sending for RIP table updates, in seconds.

RIP Interface Configuration

Device Console > Configure > Layer 3 > RIP > *RIP Interface*

Use the **RIP Interface** tab to configure RIP interfaces.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 234 RIP Interface Configuration field descriptions

Field	Description
Index	RIP Interface Index.
Version	Sets the RIP version used by this interface: v1, v2, both
Supplying Route Updates	Enables or disables supplying route updates to other routers.
Listening to Route Updates	Enables or disables listening to route updates from other routers.
Triggered Updates	Enables or disables Triggered Updates, which are used to speed convergence.
Multicast Updates	Enables or disables multicast updates of the routing table.
Poisoned Reverse	Enables or disables the poisoned reverse. When disabled, the switch uses only split horizon.
RIP Protocol	Enables or disables RIP protocol.
Route Metric	Sets the RIP route metric for this interface.
Authentication Type	Sets the authentication type used on this interface: none, password
Authentication Key	Sets the authentication key password.
Default Route action	Sets the default route action: both, supply, listen, none
Split Horizon	Enables or disables split horizon.

Static Route Redistribute Configuration

Device Console > Configure > Layer 3 > RIP > *Static Route Redistribute*

Use the **Static Route Distribute** tab to configure RIP static route redistribution parameters.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 235 RIP Static Route Redistribute Configuration field descriptions

Field	Description
Metric	Specify the metric to be assigned to RIP Static Route. A value of 0 indicates none.
Route Maps	Click Browse... to open a Browser window. You can select pre-defined route maps in this window.

BGP External Route Redistribute Configuration

Device Console > Configure > Layer 3 > RIP > BGP External Route Redistribute

Use the **BGP External Route Distribute** tab to configure RIP External BGP redistribution.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 236 RIP – BGP External Route Redistribute Configuration field descriptions

Field	Description
Metric	Specify the metric to be assigned to the RIP External BGP Route. A value of 0 indicates none.
Route Maps	Click Browse... to open a Browser window. You can select pre-defined route maps in this window.

BGP Internal Route Redistribute Configuration

Device Console > Configure > Layer 3 > RIP > *BGP Internal Route Redistribute*

Use the **BGP Internal Route Distribute** tab to configure RIP Internal BGP redistribution.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 237 RIP – BGP Internal Route Redistribute Configuration field descriptions

Field	Description
Metric	Specify the metric to be assigned to the RIP Internal BGP Route. A value of 0 indicates none.
Route Maps	Click Browse... to open a Browser window. You can select pre-defined route maps in this window.

Fixed Route Redistribute Configuration

Device Console > Configure > Layer 3 > RIP > *Fixed Route Redistribute*

Use the **Fixed Route Distribute** tab to configure RIP Fixed Route redistribution.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 238 RIP – Fixed Route Redistribute Configuration field descriptions

Field	Description
Metric	Specify the metric to be assigned to the RIP Fixed Route. A value of 0 indicates none.
Route Maps	Click Browse... to open a Browser window. You can select pre-defined route maps in this window.

OSPF Route Redistribute Configuration

Device Console > Configure > Layer 3 > RIP > OSPF Route Redistribute

Use the **Fixed Route Distribute** tab to configure RIP OSPF routes redistribution.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 239 RIP – OSPF Route Redistribute Configuration field descriptions

Field	Description
Metric	Specify the metric to be assigned to the RIP OSPF Route. A value of 0 indicates none.
Route Maps	Click Browse... to open a Browser window. You can select pre-defined route maps in this window.

OSPF External Route Redistribute Configuration

Device Console > Configure > Layer 3 > RIP > OSPF External Route Redistribute

Use the **Fixed Route Distribute** tab to configure RIP OSPF external routes redistribution.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 240 RIP – OSPF External Route Redistribute Configuration field descriptions

Field	Description
Metric	Specify the metric to be assigned to the RIP OSPF External Route. A value of 0 indicates none.
Route Maps	Click Browse... to open a Browser window. You can select pre-defined route maps in this window.

Configuring OSPF

The following sections describe the configuration tasks associated with Open Shortest Path First (OSPF) Routing protocol:

- [“OSPF General Configuration” on page 495](#)
- [“OSPF Area Configuration” on page 496](#)
- [“OSPF Interface Configuration” on page 497](#)
- [“OSPF Summary Range Configuration” on page 499](#)
- [“OSPF Virtual Interface Configuration” on page 500](#)
- [“OSPF Host Table Configuration” on page 501](#)
- [“OSPF Static Routes Configuration” on page 502](#)
- [“OSPF Fixed Routes Configuration” on page 503](#)
- [“OSPF RIP Configuration” on page 504](#)
- [“OSPF MD5 Key Configuration” on page 505](#)
- [“OSPF Loopback Interface Configuration” on page 506](#)
- [“OSPF BGP External Route Redistribute Configuration” on page 507](#)
- [“OSPF BGP Internal Route Redistribute Configuration” on page 508](#)

OSPF General Configuration

Device Console > Configure > Layer 3 > OSPF > General

Use the General tab to configure OSPF administrative settings.

Note: This tab is available only for certain switch types. Please disregard the information if it does not apply to your switch.

The following table describes the fields of the **General** tab.

Table 241 OSPF General field descriptions

Field	Description
Route Metric	The AS External metric to be assigned.
Route Metric Type	Sets the AS External metric type: none, type 1, or type 2.
State	Enables or disables OSPF. The value enabled denotes that the OSPF Process is active on at least one interface; disabled disables it on all interfaces.
LSBD	Sets the LSDB limit for external LSA.

OSPF Area Configuration

Device Console > Configure > Layer 3 > OSPF > Areas

Use the Area tab to configure OSPF Area settings.

Note: This tab is available only for certain switch types. Please disregard the information if it does not apply to your switch.

The following table describes the fields of the **Areas** tab.

Table 242 OSPF Area field descriptions

Field	Description
Index	The OSPF area number for which the OSPF area table is related.
ID	The OSPF area ID. This is a 32-bit integer that uniquely identifies an area. Area ID 0.0.0.0 is used for the OSPF backbone. If you are attempting to delete the OSPF backbone area, make sure there are no configured Virtual Interfaces.
Type	<p>Defines the type of area. For example, when a virtual link has to be established with the backbone, the area type must be defined as transit.</p> <ul style="list-style-type: none"> • Transit area: This area type allows area summary information to be exchanged between routing devices. Any area that is not a stub area or NSSA is considered to be transit area. • Stub area: An OSPF area where external routing information is not distributed. Typically, a stub area is connected to only one other area. • NSSA: Not-So-Stubby Area (NSSA) is similar to stub area, with additional capabilities. For example, routes originating from within the NSSA can be propagated to adjacent transit and backbone areas. External routes from outside the Autonomous System (AS) can be advertised within the NSSA, but are not distributed into other areas.
Metric	The metric value applied at the indicated type of service. This metric is the metric that is applied to the default route when it is advertised in a Stub/NSSA area.
Authentication Type	<p>Type of authentication being used, as follows:</p> <ul style="list-style-type: none"> • None: No authentication required. • Password: Authenticates simple passwords so that only trusted routing devices can participate. • MD5: MD5 cryptographic authentication is required.
SPF Interval	The OSPF interval, which is the time interval between two successive SPF calculations of the shortest path tree using the Dijkstra's algorithm.
Status	This variable displays the status of the entry. Currently it is always in active state.

OSPF Interface Configuration

Device Console > Configure > Layer 3 > OSPF > Interfaces

Use the Interfaces tab to configure OSPF Interfaces settings.

Note: This tab is available only for certain switch types. Please disregard the information if it does not apply to your switch.

The following table describes the fields of the **Interfaces** tab.

Table 243 OSPF Interfaces field descriptions

Field	Description
Index	The OSPF area index
Area	Configures the area number this OSPF interface.
Priority	The priority of this interface. Used in multi-access networks, this field is used in the designated router election algorithm. The value of 0 (zero) signifies that the router is not eligible to become the designated router on this particular network. In the event of a tie in this value, routers use their Router ID as a tie breaker.
Cost	Configures cost set for the selected path--preferred or backup. Usually the cost is inversely proportional to the bandwidth of the interface. Low cost indicates high bandwidth.
Hello Interval	Configures the interval in seconds or milliseconds (depending on Hello Interval Unit) between the Hello packets for the interfaces.
Hello Interval Unit	Sets the unit of measurement (seconds or milliseconds) for Hello Interval.
Router Dead Interval	The number of seconds or milliseconds (depending on Dead Interval Unit) that a router's hello packets have not been seen before its neighbors declare the router down. This should be some multiple of the hello interval. This value must be the same for all routers attached to a common network.
Router Dead Interval Unit	Sets the unit of measurement (seconds or milliseconds) for Router Dead Interval.
Transit Delay/ Transmission Delay	The estimated number of seconds it takes to transmit a link state update packet over this interface.
Retransmit Interval/ Retransmission Interval	The number of seconds between link-state advertisement retransmissions, for adjacencies belonging to this interface. This value is also used when retransmitting database description and link-state request packets.

Table 243 OSPF Interfaces field descriptions

Field	Description
Authentication Key	The Authentication Key. If the Area's Authorization Type is a simple password, and the key length is shorter than 8 octets, the agent left adjusts and zero fills to 8 octets. Note that unauthenticated interfaces need no authentication key, and simple password authentication cannot use a key of more than 8 octets. Larger keys are useful only with authentication mechanisms not specified in this document. When read, the Authentication key always returns an Octet String of length zero.
MD5 Key	MD5 authentication key string.
Passive	Enables or disables Passive mode.
Point-to-Point Interface	Enables or disables point-to-point interface.
Status	Enables or disables the status of the entry.

OSPF Summary Range Configuration

Device Console > Configure > Layer 3 > OSPF > Summary Ranges

Use the Summary Ranges tab to configure OSPF Summary Range settings.

Note: This tab is available only for certain switch types. Please disregard the information if it does not apply to your switch.

The following table describes the fields of the **Summary Ranges** tab.

Table 244 OSPF Summary Ranges field descriptions

Field	Description
Index	The current OSPF summary range.
Address	The base IP address for the range.
Mask	The IP address mask for the range.
Area Index	The area index used by the switch.
Hide State	Allows the OSPF summary range to be hidden or visible.
State	Enables or disables the OSPF summary range.

OSPF Virtual Interface Configuration

Device Console > Configure > Layer 3 > OSPF > Virtual Interfaces

Use the Virtual Interfaces tab to configure OSPF Virtual Interfaces settings.

Note: This tab is available only for certain switch types. Please disregard the information if it does not apply to your switch.

The following table describes the fields of the **Virtual Interfaces** tab.

Table 245 OSPF Virtual Interfaces field descriptions

Field	Description
Index	The Virtual Interface index.
Area Index	The OSPF area index
Hello Interval	Configures the interval in seconds or milliseconds (depending on Hello Interval Unit) between the hello packets for the interfaces.
Hello Interval Unit	Sets the unit of measurement (seconds or milliseconds) for Hello Interval.
Router Dead Interval	The number of seconds or milliseconds (depending on Dead Interval Unit) that a router's hello packets have not been seen before its neighbors declare the router down. This should be some multiple of the hello interval. This value must be the same for all routers attached to a common network.
Router Dead Interval Unit	Sets the unit of measurement (seconds or milliseconds) for Router Dead Interval.
Transit Delay/ Transmission Delay	The estimated number of seconds it takes to transmit a link-state update packet over this interface.
Retransmit Interval/ Retransmission Interval	The number of seconds between link-state advertisement retransmissions, for adjacencies that belong to this interface. This value is also used when retransmitting database description and link-state request packets. This value should be well over the expected round-trip time.
Neighbor	The Router ID of the Virtual Neighbor.
Authentication Key	The authentication key. If the Authorization Type is a simple password, the device left-adjusts and zero-fills to 8 octets. Simple password authentication cannot use a key of more than 8 octets. Note: Unauthenticated interfaces do not require an authentication key.
MD5 Key	MD5 key authentication string.
Status	Enables or disables the status of the entry.

OSPF Host Table Configuration

Device Console > Configure > Layer 3 > OSPF > Host Table

Use the Host Table tab to configure OSPF Host Table settings.

Note: You must enable the OSPF Administrative Status (State) for performing this configuration.

Note: This tab is available only for certain switch types. Please disregard the information if it does not apply to your switch.

The following table describes the fields of the **Host Table** tab.

Table 246 OSPF Host Table field descriptions

Field	Description
Index	Enter a host entry number. Host routes are used for advertising network device IP addresses to external networks within OSPF.
Host Address	The IP Address of the OSPF host.
Area Number	The OSPF area index number.
Cost	The metric to be advertised.
State	Enables or disables the status of the entry.

OSPF Static Routes Configuration

Device Console > Configure > Layer 3 > OSPF > Static Routes

Use the Static Routes tab to configure OSPF Static Routes settings.

Note: You must enable the OSPF Administrative Status (State) for performing this configuration.

Note: This tab is available only for certain switch types. Please disregard the information if it does not apply to your switch.

The following table describes the fields of the **Static Routes** tab.

Table 247 OSPF Static Routes field descriptions

Field	Description
Metric	Specify the metric to be assigned to static routes. A value of 0 indicates none.
Metric Type	The AS External metric type for Static routes.
Route Maps	Click the Browse... button to open a Browser window. You can select pre-defined route maps in this window.

OSPF Fixed Routes Configuration

Device Console > Configure > Layer 3 > OSPF > *Fixed Routes*

Use the Fixed Routes tab to configure OSPF Fixed Routes settings.

Note: You must enable the OSPF Administrative Status (State) for performing this configuration.

Note: This tab is available only for certain switch types. Please disregard the information if it does not apply to your switch.

The following table describes the fields of the **Fixed Routes** tab.

Table 248 OSPF Fixed Routes field descriptions

Field	Description
Metric	The export metric for fixed routes. A value of 0 indicates none.
Metric Type	The AS External metric type for fixed routes.
Route Maps	Click the Browse... button to open a Browser window. You can select pre-defined route maps in this window.

OSPF RIP Configuration

Device Console > Configure > Layer 3 > OSPF > RIP

Use the RIP tab to configure OSPF Routing Information Protocol (RIP) settings.

Note: You must enable the OSPF Administrative Status (State) for performing this configuration.

Note: This tab is available only for certain switch types. Please disregard the information if it does not apply to your switch.

The following table describes the fields of the **RIP** tab.

Table 249 OSPF RIP field descriptions

Field	Description
Metric	The RIP metric to use. Zero (0) indicates none.
Metric Type	The RIP metric type can be: none, type1, or type2.
Route Maps	Click the Browse... button to open a Browser window. You can select pre-defined route maps in this window.

OSPF MD5 Key Configuration

Device Console > Configure > Layer 3 > OSPF > MD5 Key

Use this tab to configure OSPF MD5 keys.

Table 250 OSPF MD5 Key field descriptions

Field	Description
Index	Key index number
Key	Sets the MD5 key for OSPF packets.

OSPF Loopback Interface Configuration

Device Console > Configure > Layer 3 > OSPF > *Loopback Interface*

Use this tab to configure an OSPF loopback interface.

Table 251 OSPF Loopback Interface field descriptions

Field	Description
Index	Sets the index number of the loopback interface.
Area	Sets the area number for the interface.
Status	Enables or disables the OSPF loopback interface.

OSPF BGP External Route Redistribute Configuration

Device Console > Configure > Layer 3 > OSPF > *BGP External Route Redistribute*

Use this tab to configure an OSPF BGP External Route Redistribute.

Table 252 OSPF BGP External Route Redistribute field descriptions

Field	Description
Metric	Sets the metric to be assigned to BGP External Route Redistribute. A value of 0 indicates none.
Metric Type	Sets the BGP External Route Redistribute metric type to: none, type1, or type2.
Route Maps	Click Browse... to open a browser window. You can select pre-defined route maps in this window.

OSPF BGP Internal Route Redistribute Configuration

Device Console > Configure > Layer 3 > OSPF > *BGP Internal Route Redistribute*

Use this tab to configure an OSPF BGP Internal Route Redistribute.

Table 253 OSPF BGP Internal Route Redistribute field descriptions

Field	Description
Metric	Sets the metric to be assigned to BGP Internal Route Redistribute. A value of 0 indicates none.
Metric Type	Sets the BGP Internal Route Redistribute metric type to: none, type1, or type2.
Route Maps	Click Browse... to open a browser window. You can select pre-defined route maps in this window.

Configuring BGP

The following sections describe the tasks associated with BGP configuration:

- [“General Configuration” on page 510](#)
- [“Peer Configuration” on page 511](#)
- [“Peer Redistribution Configuration” on page 512](#)
- [“Aggregation Configuration” on page 513](#)
- [“Group Configuration” on page 514](#)
- [“Group Redistribution Configuration” on page 515](#)

General Configuration

Device Console > Configure > Layer 3 > BGP > General

Use the **General** tab to configure BGP parameters.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 254 BGP General Configuration field descriptions

Field	Description
State	Enables or disables BGP state.
Local Preference	Sets the local preference value. The path with the higher value is preferred.
Autonomous System Number	Sets the autonomous system (AS) number.
Max External BGP Paths	Sets the maximum external BGP paths.
Max Internal BGP Paths	Sets the maximum internal BGP paths.
ASN4 to ASN2 Compatibility	Enables or disables ASN4 to ASN2 compatibility.
DSCP Marking	Sets the BGP DSCP marking value.

Peer Configuration

Device Console > Configure > Layer 3 > BGP > Peer General

Use the **Peer General** tab to configure BGP peer parameters.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 255 BGP Peer Configuration field descriptions

Field	Description
Index	BGP Peer index.
Remote Address	Sets the remote IP address for the specified peer.
Remote Autonomous System	Sets the remote autonomous system number for the specified peer.
Local Interface	Sets the Local IP interface.
Local Loopback Interface	Sets the Local IP loopback interface.
Hold Time	Sets the Hold Time.
Keep Alive Time	Sets the keep-alive time for the specified peer in seconds.
Advertisements Time	Sets the minimum time between Advertisements.
Time to Live	Sets the time-to-live value for the specified peer.
Next Hop Self	Enables or disables using this router as next-hop in BGP updates.
Connect Retry Interval	Sets the connection retry interval, in seconds.
Route Originations Time	Sets the minimum time between route originations.
Peer State	Enables or disables the peer.
Password	Sets the peer BGP password.
Passive State	Enables or disables BGP passive peer.
TTL Security Hops	Sets BGP TTL Security Hops.
In-Route Map	Click Browse... to open a Browser window. You can select pre-defined route maps in this window to add them to the in-route map list.
Out-Route Map	Click Browse... to open a Browser window. You can select pre-defined route maps in this window to add them to the out-route map list.

Peer Redistribution Configuration

Device Console > Configure > Layer 3 > BGP > Peer Redistribution

Use the **Peer Redistribution** tab to configure BGP redistribution parameters.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 256 BGP Peer Redistribution Configuration field descriptions

Field	Description
Index	BGP Peer index.
Route Metric	Sets the default metric of advertised routes.
Default Route Action	Sets the default route action: none, import, originate or redistribute.
RIP State	Enables or disables advertising RIP routes.
OSPF State	Enables or disables advertising OSPF routes.
Fixed State	Enables or disables advertising fixed routes.
Static State	Enables or disables advertising static routes.

Aggregation Configuration

Device Console > Configure > Layer 3 > BGP > Aggregation

Use the **Aggregation** tab to configure BGP aggregation.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 257 BGP Aggregation Configuration field descriptions

Field	Description
Index	Aggregation index
Address	Sets the starting subnet IP address for the aggregation.
Mask	Sets the subnet mask for the aggregation.
State	Enables or disables the aggregation.

Group Configuration

Device Console > Configure > Layer 3 > BGP > Group

Use the **Group** tab to configure BGP Groups.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 258 BGP Group Configuration field descriptions

Field	Description
Index	BGP Group index.
Name	Sets the group name.
Remote Address	Sets the remote IP address for the specified group.
Remote Mask	Sets the remote network mask for the specified group.
Local Interface	Sets the Local IP interface.
Local Loopback Interface	Sets the Local IP loopback interface.
Limit	Sets the maximum number of BGP dynamic peers.
Hold Time	Sets the Hold Time.
Keep Alive Time	Sets the keep-alive time for the specified peer in seconds.
Advertisements Time	Sets the minimum time between Advertisements.
Time to Live	Sets the time-to-live value for the specified peer.
Next Hop Self	Enables or disables using this router as next-hop in BGP updates.
Route Originations Time	Sets the minimum time between route originations.
Peer State	Enables or disables the peer.
TTL Security Hops	Sets BGP TTL Security Hops.
Password	Sets the peer BGP password.
In-Route Map	Click Browse... to open a Browser window. You can select pre-defined route maps in this window to add them to the in-route map list.
Out-Route Map	Click Browse... to open a Browser window. You can select pre-defined route maps in this window to add them to the out-route map list.

Group Redistribution Configuration

Device Console > Configure > Layer 3 > BGP > *Group Redistribution*

Use the **Group Redistribution** tab to configure BGP Group Redistribution.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 259 BGP Group Redistribution Configuration field descriptions

Field	Description
Index	BGP Group index.
Route Metric	Sets the default metric of advertised routes.
Default Route Action	Sets the default route action: none, import, originate or redistribute.
RIP State	Enables or disables advertising RIP routes.
OSPF State	Enables or disables advertising OSPF routes.
Fixed State	Enables or disables advertising fixed routes.
Static State	Enables or disables advertising static routes.

Configuring IGMP

The following sections describe the tasks associated with IGMP configuration:

- [“General Configuration” on page 517](#)
- [“Snooping Configuration” on page 518](#)
- [“IGMPv3 Snooping Configuration” on page 519](#)
- [“Static Multicast Router Configuration” on page 520](#)
- [“Relay Configuration” on page 521](#)
- [“Relay Multicast Router Configuration” on page 522](#)
- [“Filter Configuration” on page 523](#)
- [“Filter Ports Configuration” on page 524](#)
- [“Advanced Configuration” on page 525](#)
- [“Querier Configuration” on page 526](#)

General Configuration

Device Console > Configure > Layer 3 > IGMP > General

Use the **General** tab to configure IGMP parameters.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 260 IGMP General Configuration field descriptions

Field	Description
State	Enables or disables IGMP state.
Filter State	Enables or disables Filter state.
Querier State	Enables or disables Querier state.

Snooping Configuration

Device Console > Configure > Layer 3 > IGMP > Snooping

Use the **Snooping** tab to configure IGMP Snooping.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 261 IGMP Snooping Configuration field descriptions

Field	Description
State	Enables or disables IGMP Snooping state.
Multicast Router Timeout	Sets the timeout value, in seconds, for IGMP Membership queries.
Query Response Interval	Sets the query response interval.
Interval	Sets the query interval.
Robustness	Sets the IGMP robustness.
Unregistered IPMC	Enables or disables unregistered IPMC flooding.
Router Alert	Enables or disables sending IGMP router alert messages.
Report Aggregation	Enables or disables IGMP Membership Report aggregation.
Source IP	Sets the source IP address used as a proxy for IGMP Group Specific Queries.
Snooping VLANs	Click Browse... to open a Browser window. You can select the VLANs in this window to add them to IGMP Snooping.
Fast Leave VLANs	List of configured FastLeave VLANs.

IGMPv3 Snooping Configuration

Device Console > Configure > Layer 3 > IGMP > V3 Snooping

Use the **V3 Snooping** tab to configure IGMPv3 Snooping.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 262 IGMPv3 Snooping Configuration field descriptions

Field	Description
State	Enables or disables IGMPv3 Snooping.
Sources	Sets the maximum number of IGMP multicast sources to snoop from within the group record.
Exclude Filter-mode Reports	Enables or disables snooping on IGMPv3 Exclude Reports. When disabled, the switch ignores Exclude Reports.
V1/V2 Report Snooping	Enables or disables snooping on IGMP version 1 and version 2 reports. When disabled, the switch drops IGMPv1 and IGMPv2 reports.

Static Multicast Router Configuration

Device Console > Configure > Layer 3 > IGMP > *Static Multicast Router*

Use the **Static Multicast Router** tab for IGMP static multicast router configuration.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 263 IGMP Static Multicast Router Configuration field descriptions

Field	Description
Port	Sets the port number of the Static Multicast Router entry.
VLAN	Sets the VLAN number of the Static Multicast Router.
Version	Sets the IGMP version of the Static Multicast Router: version1, version2, version3.

Relay Configuration

Device Console > Configure > Layer 3 > IGMP > Relay

Use the **Relay** tab for IGMP relay configuration.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 264 IGMP Relay Configuration field descriptions

Field	Description
State	Enables or disables IGMP Relay.
VLANs	Click Browse... to open a Browser window. You can select the VLANs in this window to add them to IGMP Relay.
Report Interval	Sets the unsolicited reports interval in seconds.

Relay Multicast Router Configuration

Device Console > Configure > Layer 3 > IGMP > *Relay Multicast Router*

Use the **Relay Multicast Router** tab for IGMP relay multicast router configuration.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 265 IGMP Relay Multicast Router Configuration field descriptions

Field	Description
Index	IGMP Relay Multicast Router index.
Address	Sets the IP address of the IGMP multicast router used for IGMP Relay.
State	Enables or disables the multicast router.
Interval	Sets the time interval, in seconds, between ping attempts to the upstream multicast routers.
Failed Attempts	Sets the number of failed ping attempts required before the switch declares this multicast router as DOWN.
Successful Attempts	Sets the number of successful ping attempts required before the switch declares this multicast router as UP.
Version	Sets the IGMP Version: igmpv1 or igmpv2

Filter Configuration

Device Console > Configure > Layer 3 > IGMP > Filter

Use the **Filter** tab for IGMP filter configuration.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 266 IGMP Filter Configuration field descriptions

Field	Description
Index	IGMP Filter index.
Multicast Address1	Sets the IP Multicast Address 1 for the filter.
Multicast Address2	Sets the IP Multicast Address 2 for the filter.
Action	Allows or denies multicast traffic for the specified IP multicast addresses.
State	Enables or disables IGMP filter.

Filter Ports Configuration

Device Console > Configure > Layer 3 > IGMP > *Filter Ports*

Use the **Filter Ports** tab for IGMP filter ports configuration.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 267 IGMP Filter Ports Configuration field descriptions

Field	Description
Port	The port index.
State	Enables or disables IGMP filtering on a port.
Filter	Adds an IGMP filter to this port.

Advanced Configuration

Device Console > Configure > Layer 3 > IGMP > Advanced

Use the **Advanced** tab for IGMP advanced configuration.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 268 IGMP Advanced Configuration field descriptions

Field	Description
Query Interval	Sets the interval for IGMP Query Reports, in seconds.
Expected Packet Loss on Subnet	Sets the value of expected packet loss on the subnet.
Timeout	Sets the timeout value for IGMP Membership Reports, in seconds.
Fast leave VLANs	Click Browse... to open a Browser window. You can select the VLANs in this window to add them to Fast Leave VLANs list.
Router Alert	Enables or disables the Router Alert option in IGMP messages.
Flood State	Enables or disables the status of the flood unregistered.
Unregistered IPMC to CPU	Enables or disables unregistered IPMC to CPU.

Querier Configuration

Device Console > Configure > Layer 3 > IGMP > Querier

Use the **Querier** tab for IGMP Querier configuration.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 269 IGMP Querier Configuration field descriptions

Field	Description
VLAN	The VLAN index.
Source IP	Sets the IGMP snooping source IP address for the selected VLAN.
Election Type	Sets the IGMP Querier election criteria as IPv4 address or MAC address.
Interval	Sets the interval between IGMP Query broadcasts, in seconds.
Max Response Time	Sets the maximum query response interval, in seconds.
Robustness	Sets the IGMP Robustness variable, which is number of times that the switch sends each IGMP message.
Startup Interval	Sets the Startup Query Interval, in seconds, which is the interval between general queries sent out during startup.
Startup Count	Sets the Startup Query Count, which is the number of IGMP queries sent out during startup. Each query is separated by the Startup Query Interval.
Querier Type	Sets the Querier Type: querier, nonQuerier, checkingMembership
Version	Sets the IGMP Version of the VLAN: igmpv1, igmpv2, igmpv3
State	Enables or disables Querier on the selected VLAN.

Configuring DNS

The following sections describe the tasks associated with DNS configuration:

- [“DNS Server Configuration” on page 528](#)

DNS Server Configuration

Device Console > Configure > Layer 3 > DNS > *DNS Server*

Use the **DNS Server** tab to configure DNS Server.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 270 DNS Server Configuration field descriptions

Field	Description
Primary Server IP Address	Sets the IP address of primary DNS server.
Primary Port	Sets the port of primary DNS server: data, mgt, or extm
Secondary Server IP Address	Sets the IP address of secondary DNS server.
Secondary Port	Sets the port of secondary DNS server: data, mgt, or extm
Domain Name	Sets the default domain name used by the switch.
IP Version	Sets the IP version: currently fixed at IPv4.

Configuring Bootp-Relay

The following sections describe the tasks associated with Bootp-Relay configuration:

- [“General Configuration” on page 530](#)
- [“Server Configuration” on page 531](#)
- [“Broadcast Domain Configuration” on page 532](#)
- [“Broadcast Domain Server Configuration” on page 533](#)
- [“Option82 Configuration” on page 534](#)

General Configuration

Device Console > Configure > Layer 3 > Bootp-Relay > *General*

Use the **General** tab to configure Bootp-Relay state.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 271 Bootp-Relay General Configuration field descriptions

Field	Description
State	Enables or disables Bootp-Relay

Server Configuration

Device Console > Configure > Layer 3 > Bootp-Relay > Server

Use the **Server** tab to configure Bootp-Relay Server.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 272 Bootp-Relay Server Configuration field descriptions

Field	Description
Index	The server index.
Address	Sets the Bootp-Relay server address.

Broadcast Domain Configuration

Device Console > Configure > Layer 3 > Bootp-Relay > *Broadcast Domain*

Use the **Broadcast Domain** tab to configure Bootp-Relay broadcast domain.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 273 Bootp-Relay Broadcast Domain Configuration field descriptions

Field	Description
Index	Broadcast domain index.
VLAN	Sets the VLAN of the broadcast domain. Each broadcast domain must have a unique VLAN.
State	Enables or disables the broadcast domain.

Broadcast Domain Server Configuration

Device Console > Configure > Layer 3 > Bootp-Relay > Broadcast Domain Server

Use the **Broadcast Domain Server** tab to configure Bootp-Relay broadcast domain server.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 274 Bootp-Relay Broadcast Domain Server Configuration field descriptions

Field	Description
Index	Broadcast domain index.
Server	Broadcast domain server index.
Address	Sets the broadcast domain server address.

Option82 Configuration

Device Console > Configure > Layer 3 > Bootp-Relay > Option82

Use the **Option82** tab for Bootp-Relay option82 configuration.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 275 Bootp-Relay Option82 Configuration field descriptions

Field	Description
State	Enables or disables the Bootp-Relay option 82.
Policy	Sets the policy of Bootp-Relay option 82: replace, drop, or keep

Configuring Flooding

The following sections describe the flooding configuration tasks you can perform:

- [“VLAN Flooding Configuration” on page 536](#)

VLAN Flooding Configuration

Device Console > Configure > Layer 3 > Flooding > *VLAN Flooding*

Use this tab to configure VLAN flooding.

Table 276 VLAN Flooding field descriptions

Field	Description
VLAN	Sets the VLAN ID.
Flood unregistered IPMC	Enables or disables flooding unregistered IPMCs.
Send unregistered IPMC to CPU	Enables or disables flooding unregistered IPMCs to CPU.
Optimized Flooding	Enables or disables Optimized flooding.

Configuring VRRP

The following sections describe the configuration tasks associated with Virtual Router Redundancy Protocol (VRRP) protocol:

- [“VRRP General Configuration” on page 538](#)
- [“VRRP Virtual Router Configuration” on page 539](#)
- [“VRRP Virtual Interface Configuration” on page 541](#)
- [“VRRP Virtual Router Group Configuration” on page 542](#)

VRRP General Configuration

Device Console > Configure > Layer 3 > VRRP > General

Use the General tab to configure general VRRP settings.

Note: This tab is available only for certain switch types. Please disregard the information if it does not apply to your switch.

The following table describes the fields of the **General** tab.

Table 277 VRRP General field descriptions

Field	Description
VRRP Operation State	Globally enables or disables VRRP operation.
Virtual Router Tracking	Sets the increment of VRRP virtual router priority. This priority is adjusted by tracking the state of other virtual routers. The value 254 provides maximum priority.
IP Interface Tracking	Sets the increment of VRRP virtual router priority. This priority is adjusted by tracking the number of active (up) IP interfaces on the switch.
VLAN Switch Port Tracking	Sets the increment of VRRP virtual router priority. The priority is adjusted by tracking the port state of those ports that belong to the same virtual LAN as the virtual router.
Hot Standby	Enables or disables hot-standby processing, in which two or more switches provide redundancy for each other.
Hold Off	Sets the Hold Off value.

VRRP Virtual Router Configuration

Device Console > Configure > Layer 3 > VRRP > Virtual Router

Use the Virtual Router tab to configure VRRP Virtual Router settings.

Note: This tab is available only for certain switch types. Please disregard the information if it does not apply to your switch.

The following table describes the fields of the **Virtual Router** tab.

Table 278 VRRP Virtual Router field descriptions

Field	Description
Index	The index number of the VRRP virtual router.
ID	Defines the virtual router ID. This is used in conjunction with addr (below) to define a virtual router on this switch. To create a pool of VRRP-enabled routing devices which can provide redundancy to each other, each participating VRRP device must be configured with the same virtual router: one that shares the same VRID and addr combination. The VRID for standard virtual routers (where the virtual router IP address is not the same as any virtual server) can be any integer as defined on your particular switch model.
IP Address	Defines the IP address for this virtual router using dotted decimal notation. This is used in conjunction with the VRID (above) to configure the same virtual router on each participating VRRP device.
IP Interface	Sets the IP interface that the VRRP virtual router represents. If the IP interface has the same IP address as the IP Address option above, this switch is considered the "owner" of the defined virtual router. An owner has a special priority of the highest available virtual router number, and always assumes the role of master router, even if it must pre-empt another virtual router which has assumed master routing authority. This pre-emption occurs even if the Pre-emption option below is disabled.
Virtual Router State	Enables or disables the virtual router.
Priority	Defines the election priority bias for this virtual server. During the master router election process, the routing device with the highest virtual router priority number wins. If there is a tie, the device with the highest IP interface address wins. If this virtual router's IP address (addr) is the same as the one used by the IP interface, the priority for this virtual router is automatically set to the highest available priority value.
Advertisement Interval	Sets the time interval between VRRP advertisements.

Table 278 VRRP Virtual Router field descriptions

Field	Description
Pre-emption	Enables or disables a higher priority Backup VRRP virtual router to pre-empt a low-priority Master. When enabled, if this virtual router is in backup mode but has a higher priority than the current master, this virtual router pre-empts the lower priority master and assumes control. Note that even when Pre-emption is disabled, this virtual router always pre-empts any other master if this switch is the owner. A switch is the owner when the IP interface address and virtual router address are the same.
Pre-emption Delay	Sets the delay for pre-emption.
Virtual Routes Tracking	Enables or disables tracking other virtual routers for priority adjustment.
IP Interfaces Tracking	Enables or disables tracking other router interfaces for priority adjustment.
VLAN Switch Ports Tracking	Enables or disables tracking the states of VLAN ports for priority adjustment.
Fast Advertisement	Enables or disables fast advertisement.

VRRP Virtual Interface Configuration

Device Console > Configure > Layer 3 > VRRP > *Virtual Interface*

Use the Virtual Interface tab to configure VRRP Virtual Interface settings.

Note: This tab is available only for certain switch types. Please disregard the information if it does not apply to your switch.

The following table describes the fields of the **Virtual Interface** tab.

Table 279 VRRP Virtual Interface field descriptions

Field	Description
Index	The VRRP interface number.
Authentication	Sets the type of authentication in use. <ul style="list-style-type: none">• none: No authentication.• password: use the specified password for authentication.
Password	Sets the password for authentication.

VRRP Virtual Router Group Configuration

Device Console > Configure > Layer 3 > VRRP > Virtual Router Group

Use the Virtual Router Group tab to configure VRRP Virtual Router Group settings.

Note: This tab is available only for certain switch types. Please disregard the information if it does not apply to your switch.

The following table describes the fields of the **Virtual Router Group** tab.

Table 280 VRRP Virtual Router Group field descriptions

Field	Description
Index	The number of the VRRP virtual router. Note: The index value is always 1 and you can add only one entry in this table.
ID	The VRRP virtual group identifier.
IP Interface	Sets the IP Interface that the VRRP virtual group represents.
Virtual Router State	Enables or disables the VRRP virtual router.
Virtual Router Group State	Enables or disables the VRRP virtual router group.
Priority	Sets the priority value to be used by the specified VRRP virtual routers.
Advertisement Interval	Sets the time interval (in seconds) between VRRP advertisements.
Pre-emption	Enables or disables a higher priority Backup VRRP virtual router to pre-empt a low priority Master.
Pre-emptive Delay Interval	Sets the pre-emptive delay interval, in seconds.
IP Interfaces Tracking	Enables or disables tracking other router interfaces for priority adjustment.
VLAN Switch Ports Tracking	Enables or disables tracking port state of VLAN ports for priority adjustment.
Fast Advertisements	Enables or disables fast advertisement.

Configuring DHCP Snooping

The following sections describe DHCP Snooping configuration tasks you can perform:

- [“DHCP Snooping Configuration” on page 544](#)
- [“DHCP Snooping VLAN Configuration” on page 545](#)

DHCP Snooping Configuration

Device Console > Configure > Layer 3 > DHCP > *Snooping*

Use this tab to configure DHCP Snooping.

Table 281 DHCP Snooping field descriptions

Field	Description
DHCP Snooping	Enables or disables DHCP Snooping.
DHCP Snooping Option82	Enables or disables use of Option82 information in DHCP Snooping.

DHCP Snooping VLAN Configuration

Device Console > Configure > Layer 3 > DHCP > *Snooping VLAN*

Use this tab to configure the DHCP Snooping VLAN.

Table 282 DHCP Snooping VLAN field descriptions

Field	Description
VLAN ID	Sets the VLAN ID number.
State	Enables or disables DHCP for the VLAN.

Configuring ARP

The following sections describe ARP configuration tasks you can perform:

- [“ARP Configuration” on page 547](#)
- [“Static ARP Configuration” on page 548](#)

ARP Configuration

Device Console > Configure > Layer 3 > ARP > ARP

Use this tab to configure Address Resolution Protocol (ARP) parameters.

Table 283 ARP field descriptions

Field	Description
Cache Timeout	Sets the time after which the entry in cache is deleted.
Cache Pending Time	Sets the time for which an unresolved entry is held until a response is received.
Max Retries	Sets the maximum number of retry attempts.
Re-ARP Period	Sets the Re-ARP period in seconds.

Static ARP Configuration

Device Console > Configure > Layer 3 > ARP > *Static ARP*

Use the **Static ARP** tab to configure ARP parameters.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 284 Static ARP Configuration field descriptions

Field	Description
Index	The static ARP index.
IP Address	Sets the IP address for the ARP entry.
MAC Address	Sets the MAC address for the ARP entry.
VLAN	Sets the VLAN for the ARP entry.
Port	Sets the Port for the ARP entry.

Configuring Ports

System Networking Switch Center lets you configure physical properties on a per-port basis.

This section covers the following topics:

- [“Port Properties Configuration” on page 550](#)
- [“Ports General Configuration” on page 552](#)
- [“Threshold Rate Configuration” on page 553](#)
- [“Gigabit Link Configuration” on page 554](#)
- [“Unidirectional Link Detection \(UDLD\) Configuration” on page 555](#)
- [“Operations, Administration and Management \(OAM\) Configuration” on page 556](#)
- [“ACL Configuration” on page 557](#)
- [“STP Configuration” on page 558](#)
- [“Port Priority Configuration” on page 559](#)
- [“DHCP Snooping Configuration” on page 560](#)
- [“WRED/ECN General Configuration” on page 561](#)
- [“WRED/ECN Profile Configuration” on page 562](#)

Port Properties Configuration

Device Console > Configure > Ports > Ports

Use this feature to configure port properties.

Note: Some fields might not be available for the selected switch type. Please disregard field descriptions that do not apply to your switch.

The following table describes the fields of the **Ports** configuration tab.

Table 285 Ports field descriptions

Field	Description
Port	Port Index
Name	Port Name
State	Enables or disables the port.
VLAN Tag State	Sets the VLAN tagging of the port: tagged or untagged. You cannot add a port to more than one VLAN unless the port is tagged.
Default VLAN	Sets the default VLAN ID for the port. Note: To select another VLAN ID for this port, double-click the cell to display configured VLANs and select any of the VLANs that appear in the list. Then click Modify . The Default VLAN field displays the new selection.
PVID Tag State	Sets the PVID tag state: tagged or untagged.
PVID ingress Tag State	Sets the ingress PVID tag state of the port: tagged or untagged.
DSCP Remarking	Enables or disables DSCP re-marking on a port.
Gig Auto Negotiate	Sets the autonegotiation for Gigabit Ethernet connection: on or off.
Gigabit Ethernet Speed	The port speed for Fast Ethernet connection: 10Mbps, 100Mbps, 1000Mbps, or any.
Gigabit Mode	The port mode for Fast Ethernet connection: full-duplex, half-duplex, or full-or half-duplex.
Gig Flow Control	Sets the port flow control for Gigabit Ethernet connection: other, transmit, receive, both, or none.
FDB Learning	Enables or disables Layer 2 FDB learning on the port.
Flood Blocking	Enables or disables port Flood Blocking. When enabled, unicast and multicast packets with unknown destination MAC addresses are blocked from the port.

Table 285 Ports field descriptions

Field	Description
Fast Forwarding Mode	Disables or enables Port Fast Forwarding, which permits a port that participates in Spanning Tree to bypass the Listening and Learning states and enter directly into the Forwarding state. While in the Forwarding state, the port listens to the BPDUs to learn if there is a loop and, if dictated by normal STG behavior (following priorities, etc.), the port transitions into the Blocking state.
RMON	Enables or disables Remote Monitoring.
Link Trap	Enables or disables link trap.
Hold Off	Sets the hold off value.
Flow Control	Sets the port flow control for Gigabit Ethernet connection, as follows: other, transmit, receive, both, or none
BPDU Guard	Enables or disables BPDU Guard.
Flood Blocking	Enables or disables port flood blocking. When enabled, unicast and multicast packets with unknown destination MAC addresses are blocked from the port.
Error Disable	Enables or disables error disable recovery.
MAC Addr Notification	Enables or disables the MAC address notification syslog messages on the port.
EVB Profile	Sets the EVB profile.

Ports General Configuration

Device Console > Configure > Ports > Ports General

Use this tab to configure the general port properties.

Note: This tab or some of its fields might not be available for the selected switch type. Please disregard field descriptions that do not apply to your switch.

Table 286 Ports General field descriptions

Field	Description
Port	Port number.
VLAN Tag State	Enables or disables VLAN tag state.
PVID Tag State	Enables or disables VLAN tag persistence. When disabled, the VLAN tag is removed from packets whose VLAN tag matches the port PVID even if the port is a tagged member of that VLAN.
FDB Learning	Enables or disables FDB learning on the port.
Flooding	Enables or disables flooding on the port.
MAC Notification	Enables or disables MAC notification syslog messages on the port.
Link Logging	Enables or disables syslog for interface state change.

Threshold Rate Configuration

Device Console > Configure > Ports > Threshold Rate

Use this tab to configure the port threshold rates.

Note: This tab or some of its fields might not be available for the selected switch type. Please disregard field descriptions that do not apply to your switch.

Table 287 Threshold Rate field descriptions

Field	Description
Port	Port number.
Name	Port name.
State	Enables or disables the port.
Multicast Threshold	Enables or disables the port's multicast threshold. If disabled (<i>dis</i>), the port forwards all multicast packets.
Multicast Threshold Rate	Sets the number of multicast packets per second to the specified value.
Broadcast Threshold	Enables or disables the port's broadcast threshold. If disabled (<i>dis</i>), the port forwards all broadcast packets.
Broadcast Threshold Rate	Sets the number of broadcast packets per second to the specified value.
DLF Threshold	Enables or disables the port's unknown unicast threshold. If disabled (<i>dis</i>), the port forwards all unknown unicast packets.
DLF Threshold Rate	Sets the number of unknown unicast packets per second to the specified value.

Gigabit Link Configuration

Device Console > Configure > Ports > *Gigabit Link*

Use this tab to configure the port link parameters.

Note: This tab or some of its fields might not be available for the selected switch type. Please disregard field descriptions that do not apply to your switch.

Table 288 Gigabit Link field descriptions

Field	Description
Port	Port number.
Name	Port name.
State	Enables or disables the port.
Auto-Negotiation	Sets the auto-negotiation for Gigabit Ethernet connection (on or off).
Speed	Sets the port speed for Fast Ethernet connection as follows: 10Mbps, 100Mbps, 1000Mbps, any
Mode	Sets the port mode for Fast Ethernet connection as follows: full-duplex, half-duplex, full-or half-duplex
Flow Control	Sets the port flow control for Gigabit Ethernet connection as follows: other, transmit, receive, both, none
Clause 73 Auto Negotiation	Enables or disables Clause 73 auto-negotiation.
Fast Link Down Detection	Enables or disables the non-IEEE Fast Link Down detection.

Unidirectional Link Detection (UDLD) Configuration

Device Console > Configure > Ports > UDLD

Use this tab to configure Unidirectional Link Detection (UDLD) for the port.

Note: This tab or some of its fields might not be available for the selected switch type. Please disregard field descriptions that do not apply to your switch.

Table 289 Port UDLD field descriptions

Field	Description
Port	Port number.
Name	Port name.
State	Enables or disables the port.
UDLD	Enables or disables UDLD.
Mode	Sets the UDLD mode for the port (normal or aggressive).

Operations, Administration and Management (OAM) Configuration

Device Console > Configure > Ports > OAM

Use this tab to configure Operations, Administration and Management (OAM) parameters for the port.

Note: This tab or some of its fields might not be available for the selected switch type. Please disregard field descriptions that do not apply to your switch.

Table 290 Port OAM field descriptions

Field	Description
Port	Port number.
Name	Port name.
State	Enables or disables the port.
OAM	Enables or disables OAM discovery process.
Mode	Sets the OAM mode for the port (active or passive).

ACL Configuration

Device Console > Configure > Ports > ACL

Use this tab to configure Access Control Lists (ACLs) for the port.

Note: This tab or some of its fields might not be available for the selected switch type. Please disregard field descriptions that do not apply to your switch.

Table 291 Port ACL field descriptions

Field	Description
Port	Port number.
ACL	Adds the specified ACL to the port.
ACL Group	Adds the specified ACL group to the port.

STP Configuration

Device Console > Configure > Ports > STP

Use this tab to configure Spanning Tree (STP) parameters for the port.

Note: This tab or some of its fields might not be available for the selected switch type. Please disregard field descriptions that do not apply to your switch.

Table 292 Port STP field descriptions

Field	Description
Port	Port number.
Name	Port name.
State	Enables or disables the port.
Port Edge	Enables or disables the port as an edge port.
Link Type	Sets the link type for the selected port.
Guard Type	Sets the Spanning Tree Guard type (loop, root, none, default).

Port Priority Configuration

Device Console > Configure > Ports > *Port Priority*

Use this tab to configure port priority.

Note: This tab or some of its fields might not be available for the selected switch type. Please disregard field descriptions that do not apply to your switch.

Table 293 Port Priority field descriptions

Field	Description
Port	Port number.
Priority	Sets the priority for the selected port.

DHCP Snooping Configuration

Device Console > Configure > Ports > *DHCP Snooping*

Use this tab to configure DHCP Snooping for the port.

Note: This tab or some of its fields might not be available for the selected switch type. Please disregard field descriptions that do not apply to your switch.

Table 294 Port DHCP Snooping field descriptions

Field	Description
Port	Port number.
Trusted	Sets Port as DHCP Snooping trusted or untrusted port.
Rate Limit	Sets DHCP Packets rate limit for port.

WRED/ECN General Configuration

Device Console > Configure > Ports > WRED/ECN

Use the **WRED/ECN** tab to set WRED and ECN states for ports.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 295 WRED/ECN Port - General Configuration field descriptions

Field	Description
Port	The port index.
WRED	Turns WRED for the selected port on or off.
ECN	Turns ECN for the selected port on or off.

WRED/ECN Profile Configuration

Device Console > Configure > Ports > WRED/ECN Profiles

Use the **WRED/ECN Profiles** tab to configure WRED and ECS profile parameters for ports

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 296 WRED/ECN Port - Profile Configuration field descriptions

Field	Description
Port	The port index.
Transmit Queue	The global transmit queue index.
TCP Min Threshold Rate	Sets the minimum threshold value of the global TCP profile for the port.
TCP Max Threshold Rate	Sets the maximum threshold value of the global TCP profile for the port.
TCP Drop Rate	Sets the drop rate value of the global TCP profile for the port.
Non TCP Min Threshold Rate	Sets the minimum threshold value of the global non TCP profile for the port.
Non TCP Max Threshold Rate	Sets the maximum threshold value of the global non TCP profile for the port.
Non TCP Drop Rate	Sets the drop rate value of the global non TCP profile for the port.
WRED State	Turns on or off WRED state of the global transmit queue for the port.

Configuring QoS – WRED/ECN

The following sections describe the tasks associated with QoS WRED/ECN configuration:

- [“General Configuration” on page 564](#)
- [“Global Profile Configuration” on page 565](#)

General Configuration

Device Console > Configure > QoS > WRED/ECN > General

Use the **General** tab to set WRED and ECS states globally.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 297 WRED/ECN General Configuration field descriptions

Field	Description
WRED	Turns global WRED state on or off.
ECN	Turns global ECN state on or off.

Global Profile Configuration

Device Console > Configure > QoS > WRED/ECN > Global Profile

Use the **Global Profile** tab to configure WRED and ECS profile parameters

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 298 WRED/ECN Global Profile Configuration field descriptions

Field	Description
Transmit Queue	The global transmit queue index.
TCP Min Threshold Rate	Sets the minimum threshold value of the global TCP profile.
TCP Max Threshold Rate	Sets the maximum threshold value of the global TCP profile.
TCP Drop Rate	Sets the drop rate value of the global TCP profile.
Non TCP Min Threshold Rate	Sets the minimum threshold value of the global non TCP profile.
Non TCP Max Threshold Rate	Sets the maximum threshold value of the global non TCP profile.
Non TCP Drop Rate	Sets the drop rate value of the global non TCP profile.
WRED State	Turns on or off WRED state of the global transmit queue.

Configuring ACLs

This section covers the following ACL topics:

- [“General ACL Properties Configuration” on page 567](#)
- [“ACL Groups Configuration” on page 570](#)
- [“ACL Block Configuration” on page 571](#)
- [“Management ACL Configuration” on page 572](#)
- [“ACL Log Configuration” on page 573](#)
- [“ACL VMAPs Configuration” on page 574](#)
- [“MAC ACL Configuration” on page 577](#)
- [“IP ACL Configuration” on page 578](#)

General ACL Properties Configuration

Device Console > Configure > Access Control List > ACL

Use this feature to configure the general ACL properties.

Note: Some fields might not be available for the selected switch type. Please disregard field descriptions that do not apply to your switch.

The following table describes the fields of the **ACL** configuration tab.

Table 299 ACL field descriptions

Field	Description
ACL	Configures the ACL number
Block	Displays the ACL Block number
Group	Displays the ACL Group number
Egress Ports	Displays the egress port, if applicable.
Statistics	Enables or disables statistics collection for this ACL.
Filter Action	Configures a filter action for packets that match the ACL definitions. You can choose to permit (pass) or deny (drop) packets, or set the Class of Service queue that handles the packets.
Priority	Configures the 802.1p priority (none, 0-7).
Out Prof DSCP Enable	Enables or disables out profile DSCP
CoSq	Configures the Class of Service queue. This section applies only if you set the filter action to setcos.
Mirror Port	Sets the port as the mirror target.
Log	Enables or disables logging for the selected ACL.
Tcp Flags	Sets the TCP flags.
Tcp Flags Mask	Sets the TCP flags mask.
User Priority	Sets user defined priority for the ACL.

Adding an ACL

To add an ACL, click **Insert** in the ACL Configuration window. (**Device Console > Configure > Access Control List > ACL**).

The following table describes the fields of the Insert ACL window.

Table 300 Insert ACL field descriptions

Field	Description
ACL	Configures the ACL index number.
Egress Ports	Sets the Egress ports. Click Browse to select the ports.
Statistics	Enables or disables the ACL statistics.
Log	Enables or disables logging for the selected ACL.
Filter Action	Sets the filter action to <code>none</code> , <code>permit</code> , <code>deny</code> or <code>setprio</code> (set priority).
Priority	Sets the priority (<code>none</code> , <code>prio0-prio7</code>). Note that this field is enabled only when you set the Filter Action to <code>setprio</code> . The default setting is <code>none</code> .
Mirror Port	Sets the Mirror ports. Click Browse to select the ports.
Filter Action VLAN	Sets the VLAN to be changed. Note that this field is enabled only when you set the Filter Action to <code>changevlan</code> . Setting VLAN to 0 automatically disables <code>changevlan</code> for this VLAN.
Ethernet Format	Sets the Ethernet format (<code>none</code> , <code>Ethernet2</code> , <code>SNAP</code> , <code>LLC</code>).
Tag Format	Sets the Tag format (<code>disabled</code> , <code>any</code> , <code>none</code> , <code>tagged</code>).
IP Format	Sets the IP format (<code>none</code> , <code>ipv4</code> , <code>ipv6</code>).
Source MAC address	Sets the source MAC address.
Source MAC Mask	Sets the source MAC mask.
Destination MAC Address	Sets the destination MAC address.
Destination MAC Mask	Sets the destination MAC mask.
Ethernet Type	Sets the Ethernet type (<code>none</code> , <code>arp</code> , <code>ipv4</code> , <code>ipv6</code> , <code>mpls</code> , <code>rarp</code> , <code>any</code> , <code>other</code>).
Ethernet Value	Sets the Ethernet value. Note that this field is enabled only when you set the Ethernet type to <code>other</code> .
VLAN ID	Sets the VLAN Identifier.
VLAN Mask	Sets the VLAN mask.

Table 300 Insert ACL field descriptions

Field	Description
802.1p Priority	Sets 802.1p priority (<i>none</i> , 0–7).
Type Of Service	Sets the Type Of Service.
Protocol	Sets the protocol.
Source IP Address	Sets the source IP address.
Source IP Mask	Sets the source IP mask.
Destination IP Address	Sets the destination IP address.
Destination IP Mask	Sets the destination IP mask.
Source Port	Sets the source port.
Source Port Mask	Sets the source port mask.
Destination Port	Sets the destination port.
Destination Port Mask	Sets the destination port mask.
Tcp Flags	Sets the TCP flags.
Tcp Flags Mask	Sets the TCP flags mask.
Meter Action	Sets the meter action to unconfigured, outdrop or outpass.
Meter Status	Enables or disables port metering.
Committed Rate	Sets the committed rate.
Maximum Burst Size	Sets the maximum burst size.
In Prof User	Sets the in-profile user to 0-7.
In Prof Dscp	Sets the in-profile DSCP value to 0-63.
In Prof ToS	Enables or disables in-profile ToS.
Out Prof Dscp	Sets the out-profile DSCP value to 0-63.
In Profile User Enable	Enables or disables in-profile user.
In Profile Dscp Enable	Enables or disables in-profile DSCP.
Out Profile Dscp Enable	Enables or disables out-of-profile DSCP.

ACL Groups Configuration

Device Console > Configure > Access Control List > ACL Groups

Use this tab to compile one or more ACLs and ACL Blocks into an ACL Group. Once you create an ACL Group, you can assign the ACL Group to one or more ports.

Note: Some fields might not be available for the selected switch type. Please disregard field descriptions that do not apply to your switch.

The following table describes the fields of the **ACL Groups** configuration tab.

Table 301 ACL Groups field descriptions

Field	Description
ACL Group	Configures the ACL Group number.
ACLs	Add ACLs to the ACL Group, or remove ACLs from the ACL Group.
ACL Block	Add ACL Blocks to the ACL Group, or remove ACL Blocks from the ACL Group.

ACL Block Configuration

Device Console > Configure > Access Control List > *ACL Block*

Use the **ACL Block** tab for ACL Block configuration.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 302 ACL Block Configuration field descriptions

Field	Description
ACL Block	Sets the ACL Block number.
ACLs	Adds or removes ACLs to or from the ACL Block.

Management ACL Configuration

Device Console > Configure > Access Control List > *Management ACL*

Use the **Management ACL** tab for Management ACL configuration.

Note: This tab might not be available for the selected switch type. Please disregard this tab if it do not apply to your switch.

Table 303 Management ACL Configuration field descriptions

Field	Description
ACL	Sets the Management ACL number.
User Enable	Sets the user-specified update method for this ACL: disabled, enabled.
Statistics	Enables or disables the statistics collection for this ACL.
Filter Action	Sets a filter action for packets that match the ACL definitions. You can choose to permit (pass) or deny (drop) packets.
Protocol	Sets the protocol.
Source IP Address	Sets the source IP address.
Source IP Mask	Sets the source IP mask.
Destination IP Address	Sets the destination IP address.
Destination IP Mask	Sets the destination IP mask.
Source Port	Sets the source port.
Source Port Mask	Sets the source port mask.
Destination Port	Sets the destination port.
Destination Port Mask	Sets the destination port mask.

ACL Log Configuration

Device Console > Configure > Access Control List > Log

Use this tab to configure ACL logging.

Table 304 ACL Logging field descriptions

Field	Description
Interval	Sets filter log display interval.
Rate Limit	Sets filter log queue rate limit.

ACL VMAPs Configuration

Device Console > Configure > Access Control List > VMAP

Use this feature to add or remove a VLAN Map to ACLs.

Note: This tab is available only for VMready capable switches. Please disregard this information if it does not apply to your switch.

The following table describes the fields of the **VMAP** configuration tab.

Table 305 ACL VMAP field descriptions

Field	Description
Index	VMAP index
Egress Ports	Displays the egress ports.
Statistics	Enables or disables statistics collection for this ACL and VMAP.
Filter Action	Configures a filter action for packets that match the ACL VMAP definitions. You can choose to permit (pass) or deny (drop) packets, or set the Class of Service queue that handles the packets.

Adding VMAPs to an ACL

You can add VMAPs to ACL by clicking **Insert** in ACL VMAPs configuration window (**Device Console > Configure > Access Control List > VMAP**).

The following table describes the fields of the Insert VMAP window.

Table 306 Insert VMAP field descriptions

Field	Description
Index	The VMAP index.
Egress Ports	Sets the Egress ports. Use Browse button to select the ports.
Statistics	Enables or disables the statistics.
Filter Action	Sets the filter action (none, permit, deny, setprio).
Priority	Sets the priority (0-7, none). Note that this field is enabled only when you set the Filter Action to setprio. Or else, none is taken by default.
Filter Action VLAN	Sets the VLAN to be changed. Note that this field is enabled only when you set the Filter Action to <code>changevlan</code> . Setting VLAN to 0 automatically disables <code>changevlan</code> for this VLAN.
Ethernet Format	Sets the Ethernet format (none, ethernet2, snap, llc).
Tag Format	Sets the Tag format (disabled, any, none, tagged).
IP Format	Sets the IP format (none, ipv4, ipv6).
Source MAC Address	Sets the source MAC address.
Source MAC Mask	Sets the source MAC mask.
Destination MAC Address	Sets the destination MAC address.
Destination MAC Mask	Sets the destination MAC mask.
Ethernet Type	Sets the Ethernet type (none, arp, ipv4, ipv6, mpls, rarp, any, other)
Ethernet Value	Sets the Ethernet value. Note that this field is enabled only when you set the Ethernet type to "other".
802.1p Priority	Sets 802.1p priority (0-7, none).
Type of Service	Sets the Type of Service value.
Protocol	Sets the protocol type.
Source IP Address	Sets the source IP address.
Source IP Mask	Sets the source IP mask.
Destination IP Address	Sets the destination IP address.

Table 306 Insert VMAP field descriptions

Field	Description
Destination IP Mask	Sets the destination IP mask.
Source Port	Sets the source port.
Source Port Mask	Sets the source port mask.
Destination Port	Sets the destination port.
Destination Port Mask	Sets the destination port mask.
Port Metering Status	Enables or disables port metering.
Meter Action	Sets the meter action (unconfigured, outdrop, outpass).
Meter Status	Enables or disables meter status.
Committed Rate	Sets the committed rate.
Maximum Burst Size	Sets the maximum burst size.
In Prof User	Sets the in-profile user value.
In Prof Dscp	Sets the in-profile DSCP value.
In Prof ToS	Enables or disables in-profile ToS.
Out Prof Dscp	Sets the out-of-profile DSCP value.
In Prof User Enable	Sets the in-profile user (disabled, user defined state).
In Prof Dscp Enable	Sets the in-profile DSCP (disabled, user defined state).
Out Prof Dscp Enable	Enables or disables out-of-profile DSCP.
Mirror Port	Sets the port as the mirror target.
Tcp Flags	Sets the TCP flags.
Tcp Flags Mask	Sets the TCP flags mask.

MAC ACL Configuration

Device Console > Configure > Access Control List > MAC ACL

Use this tab to configure MAC ACLs.

Table 307 MAC ACL field descriptions

Field	Description
ACL	MAC ACL rule number.
In Ports	Sets the complete set of ports over which if the packet arrives the filter rule will be applicable. If the incoming port list is 0 (zero), the filter rule is applicable for all the incoming ports. By default in-port list is maintained as 0.
Out Ports	This field is applicable only if the filter action is set to <code>allow</code> . If the outgoing port list is non-zero, the packet will be sent over the specified ports only. If the outgoing port list is 0 (zero), the port over which the packet is to be switched will be based on further processing on the packet. By default, the out-port list is maintained as 0.
Protocol Type	Sets the non IP protocol type to be filtered. The values are: <code>aarp</code> , <code>amber</code> , <code>dec-spanning</code> , <code>decnet-iv</code> , <code>diagnostic</code> , <code>dsm</code> , <code>etype-6000</code> , <code>etype-8042</code> , <code>lat</code> , <code>lavc-sca</code> , <code>mop-console</code> , <code>mop-dump</code> , <code>msdos</code> , <code>mump</code> , <code>netbios</code> , <code>vines-echo</code> , <code>vines-ip</code> , <code>xns-idp</code> A value of 0 (zero) means the filter is applicable for all protocols.
Source Address	Sets the source MAC address to be matched with the packet.
Destination Address	Sets the destination MAC address to be matched with the packet.
VLAN	Sets the VLAN ID to be filtered. A value of 0 (zero) means no VLAN is configured for filtering
Action	Sets the action to be taken on the packet if the filter rule matches. If the action is <code>allow</code> , the packet will be forwarded according to the forwarding rules. If the action is <code>drop</code> , the packet will be discarded.
Statistics Status	Sets the stats status (true or false).
Mirror	Enables or disable port mirroring.
Mirror Port	Sets the port to which the packets matching the ACLs should be mirrored. This attribute is operational only when mirroring is enabled.
User Priority	Sets the user priority. A value of -1 means no user priority is configured.

IP ACL Configuration

Device Console > Configure > Access Control List > IP ACL

Use this tab to configure IP ACLs.

Table 308 IP ACL field descriptions

Field	Description
ACL	IP ACL rule number.
In Ports	Sets the complete set of ports over which if the packet arrives the filter rule will be applicable. If the incoming port list is 0 (zero), the filter rule is applicable for all the incoming ports. By default in-port list is maintained as 0.
Out Ports	This field is applicable only if the Filter Action is set to <code>allow</code> . If the outgoing port list is non-zero, the packet will be sent over the specified ports only. If the outgoing port list is 0 (zero), the port over which the packet is to be switched will be based on further processing on the packet. By default out-port list is maintained as 0.
Type	Sets the category of IP filters. Standard IP filter provides the basic IP filter option (IP address/mask) whereas extended IP filter provides additional options (Protocol, TCP/UDP Port numbers, TCP flags, TOS, DSCP and ICMP types). This attribute needs to be set before configuring the other attributes of this table.
Protocol Type	Sets the protocol type to be checked against the packet.
Message Type	Sets the message type to be checked against the packet.
Message Code	Sets the message code to be checked against the packet.
Source Address	Sets the source IP address to be matched with the packet.
Source Mask	Sets the IP subnet mask for source IP address.
Destination Address	Sets the destination IP address to be matched with the packet.
Destination Mask	Sets the IP subnet mask for destination IP address.
Min Source Protocol Port	Sets the minimum port in the source port range.
Min Destination Protocol Port	Sets the minimum port in the destination port range.
Max Source Protocol Port	Sets the maximum port in the source port range.
Max Destination Protocol Port	Sets the maximum port in the destination port range.
ACK Bit	Sets the TCP ACK bit to be checked against the packet.
RST Bit	Sets the TCP RST bit to be checked against the packet.

Table 308 IP ACL field descriptions

Field	Description
FIN Bit	Sets the TCP FIN bit to be checked against the packet.
SYN Bit	Sets the TCP SYN bit to be checked against the packet.
URG Bit	Sets the TCP URG bit to be checked against the packet.
PSH Bit	Sets the TCP PSH bit to be checked against the packet.
IP TOS Bit	Sets the IP TOS bit to be checked against the packet.
DSCP	Sets the IP DSCP value to be checked against the packet.
Action	Sets the action to be taken on the packet if the filter rule matches.
Statistics Status	Sets whether ACL's Hit Count to be maintained or not.
Mirror	Enables or disable port mirroring.
Mirror Port	Sets the port to which the packets matching the ACLs should be mirrored. This attribute is operational only when mirroring is enabled.

Configuring CEE (Converged Enhanced Ethernet)

The following sections describe the configuration tasks associated with CEE:

- [“CEE General Configuration” on page 581](#)
- [“Priority Allocation Configuration” on page 582](#)
- [“Bandwidth Allocation Configuration” on page 583](#)
- [“PFC \(Priority Flow Control\) Configuration” on page 584](#)
- [“PFC Status Configuration” on page 585](#)
- [“Port PFC Configuration” on page 586](#)
- [“Port PFC Status Configuration” on page 587](#)
- [“DCBX \(Data Center Bridging Capability Exchange\) Protocol Configuration” on page 588](#)

CEE General Configuration

Device Console > Configure > CEE > *General*

Use the **CEE General** tab to enable or disable the global state.

Note: This tab is available only for CEE capable switches. Please disregard this information if it does not apply to your switch.

Priority Allocation Configuration

Device Console > Configure > CEE > *Priority Allocation*

Use the **CEE Priority Allocation** tab to set Priority Group for the configured Priority.

Note: This tab is available only for CEE capable switches. Please disregard this information if it does not apply to your switch.

Table 309 Priority Allocation field descriptions

Field	Description
Priority	Priority value (0-7).
Priority Group	Priority Group configured for the priority (0-7, no bandwidth limit).

Bandwidth Allocation Configuration

Device Console > Configure > CEE > *Bandwidth Allocation*

Use the **CEE Bandwidth Allocation** tab to set Bandwidth for the Priority Groups.

Note: This tab is available only for CEE capable switches. Please disregard this information if it does not apply to your switch.

Table 310 Bandwidth Allocation field descriptions

Field	Description
Priority Group	Priority Group index.
Bandwidth	Bandwidth range (0-100).

PFC (Priority Flow Control) Configuration

Device Console > Configure > CEE > *PFC*

Use the PFC tab to enable or disable the global PFC state.

Note: This tab is available only for CEE capable switches. Please disregard this information if it does not apply to your switch.

PFC Status Configuration

Device Console > Configure > CEE > PFC Status

Use the **PFC Status** tab to enable or disable the global PFC status of individual priority.

Note: This tab is available only for CEE capable switches. Please disregard this information if it does not apply to your switch.

Table 311 PFC Status field descriptions

Field	Description
Priority	Priority value (0-7).
Global PFC Status	PFC status (enabled or disabled).

Port PFC Configuration

Device Console > Configure > CEE > Port PFC

Use the **Port PFC** tab to enable or disable the PFC status of individual ports.

Note: This tab is available only for CEE capable switches. Please disregard this information if it does not apply to your switch.

Table 312 Port PFC field descriptions

Field	Description
Port	Port number.
PFC status	PFC status for the port (enabled or disabled).

Port PFC Status Configuration

Device Console > Configure > CEE > *Port PFC Status*

Use the **Port PFC Status** tab to enable or disable the PFC status of port and priority combination.

Note: This tab is available only for CEE capable switches. Please disregard this information if it does not apply to your switch.

Table 313 Port PFC Status field descriptions

Field	Description
Port	Port number.
Priority	Priority value.
PFC status	PFC status (enabled or disabled).

DCBX (Data Center Bridging Capability Exchange) Protocol Configuration

Device Console > Configure > CEE > DCBX

Use the **DCBX** tab to configure various features of DCBX.

Note: This tab is available only for CEE capable switches. Please disregard this information if it does not apply to your switch.

Table 314 DCBX field descriptions

Field	Description
Port	Port number.
DCBX State	DCBX status (enabled or disabled).
ETS Willing	ETS Willing setting (enabled or disabled).
ETS Advertise	ETS Advertise setting (enabled or disabled).
PFC Willing	PFC Willing setting (enabled or disabled).
PFC Advertise	PFC Advertise setting (enabled or disabled).
App Protocol Willing	App Protocol Willing setting (enabled or disabled).
App Protocol Advertise	App Protocol Advertise setting (enabled or disabled).

Configuring Multicast Priority

Device Console > Configure > CEE > *Multicast Priority*

This provides information on Multicast Priority Allocation.

Note: This tab is available only for CEE capable switches. Please disregard this information if it does not apply to your switch.

Table 315 CEE Multicast priority field descriptions

Field	Description
Multicast Priority	Multicast Priority
Group Number	Multicast Priority Group Number

Configuring Multicast Bandwidth Allocation

Device Console > Configure > CEE > *Multicast Bandwidth Allocation*

This provides information on Multicast Bandwidth Allocation.

Note: This tab is available only for CEE capable switches. Please disregard this information if it does not apply to your switch.

Table 316 CEE Multicast Bandwidth Allocation field descriptions

Field	Description
Multicast Priority Group	Multicast Priority Group
Multicast Group Bandwidth	Multicast Group Bandwidth
Description	Description

Configuring FCoE (Fiber Channel over Ethernet)

The following sections describe the configuration tasks associated with FCoE:

- [“FIP Snooping Configuration” on page 592](#)
- [“FIP Snooping Port Configuration” on page 593](#)

FIP Snooping Configuration

Device Console > Configure > FCoE > *FIP Snooping*

Use the **FIP Snooping** tab to set the FIP Snooping global state and ACL timeout.

Note: This tab is available only for FCoE capable switches. Please disregard this information if it does not apply to your switch.

Table 317 FIP Snooping field descriptions

Field	Description
Global State	FIP state (on or off).
ACL Timeout	ACL Timeout setting (enabled or disabled).
Auto VLAN	Auto VLAN setting (enabled or disabled)

FIP Snooping Port Configuration

Device Console > Configure > FCoE > *FIP Snooping Port*

Use the **FIP Snooping** tab configure FIP Snooping Ports.

Note: This tab is available only for FCoE capable switches. Please disregard this information if it does not apply to your switch.

Table 318 FIP Snooping Port field descriptions

Field	Description
Port	Port number.
FCF Mode	Fiber Channel Forwarding mode (on, off, auto)
State	FIP Snooping state for the port (enabled or disabled)

Configuring Switch Partition

The following sections describe the configuration tasks associated with Switch Partition (SPAR). This section covers the following topics:

- [“SPAR IDs Configuration” on page 595](#)
- [“SPAR Local Domains Configuration” on page 596](#)

SPAR IDs Configuration

Device Console > Configure > SPAR > IDs

Use the **SPAR IDs** tab to configure SPAR IDs.

Note: This tab or some of its fields might not be available for the selected switch type. Please disregard this information if it does not apply to your switch.

Table 319 SPAR IDs field descriptions

Field	Description
ID	The SPAR ID.
Name	Sets the SPAR name.
State	Enables or disables the SPAR state.
Uplink Type	Sets the Uplink Type: Port, Trunk, or Admin Key.
Uplink Port	Sets the SPAR uplink port.
Uplink Trunk	Sets the SPAR uplink trunk.
Uplink Adminkey	Sets the SPAR uplink adminkey.
Domain Mode	Sets the SPAR domain mode: passthrough, local
Default Domain Server Port List	Sets the SPAR default domain server port list.
Default Domain SPAR VID	Sets the SPAR default domain SPAR VID.

SPAR Local Domains Configuration

Device Console > Configure > SPAR > *Local Domains*

Use the **Local Domains** tab to configure SPAR local domains.

Note: This tab or some of its fields might not be available for the selected switch type. Please disregard this information if it does not apply to your switch.

Table 320 SPAR Local Domains field descriptions

Field	Description
ID	The local domain SPAR ID.
IVID	The local domain IVID.
Server Port List	Sets the SPAR local domain server port list.
VID	Sets the SPAR local domain VID.
Name	Sets the SPAR local domain name.
State	Enables or disables the SPAR local domain state.

Configuring Virtualization

Use virtualization to configure VMready features. This section covers the following virtualization topics:

Note: The following features are available only for VMready capable switches. Please disregard this information if it does not apply to your switch. vNIC Configuration is presently available only on the VMready switches BNT Rackswitch G8124 and BNT 10-port 10Gb Ethernet Switch Module.

- [“General VM Configuration” on page 598](#)
- [“VMware vCenter Configuration” on page 599](#)
- [“VM Profiles Configuration” on page 600](#)
- [“VM Groups Configuration” on page 601](#)
- [“VM Bandwidth Configuration” on page 602](#)
- [“VM Check Configuration” on page 603](#)
- [“VM Hello Configuration” on page 604](#)
- [“VM Ports Configuration” on page 605](#)
- [“Virtual Machines Configuration” on page 606](#)
- [“VM Advanced Pre-Provisioning” on page 607](#)
- [“vNIC General Configuration” on page 608](#)
- [“vNIC Port Configuration” on page 609](#)
- [“vNIC Group Configuration” on page 610](#)
- [“EVB General Configuration” on page 611](#)
- [“EVB Profiles Configuration” on page 612](#)
- [“VSI DB Host Configuration” on page 613](#)
- [“vCenter Configuration” on page 615](#)
- [“Virtual Data Station Configuration” on page 616](#)

General VM Configuration

Device Console > Configure > Virtualization > General

Use this feature to enable or disable VM Groups.

The following table describes the fields of the Virtualization's **General** configuration tab.

Table 321 Virtualization General field descriptions

Field	Description
Virtual Machine Groups	Enables or disables VM Groups

Server port configuration allows you to set the server ports on RackSwitches, such as the G8000 and G8124.

Table 322 Virtualization Server Port field descriptions

Field	Description
Server ports	Selects the switch ports to assign as server ports.

VMware vCenter Configuration

Device Console > Configure > Virtualization > VMware vCenter Access

Use this feature to set UDP port number used by ESX/ESXi server to send heartbeat message periodically to Virtual Center and configure VMware Virtual Center access information.

The following table describes the fields of the **VMware vCenter Access** configuration tab.

Table 323 VMware vCenter Access field descriptions

Field	Description
ESX/ESXi server to vCenter heartbeat UDP port	Set ESX/ESXi server to vCenter heartbeat UDP port number
Server IP Address	IP address of the system on which Virtual Center is running. You can select the Server IP address from the drop-down list, which shows the Virtual Centers configured in SNSC.
User Name	User name for the Virtual Center
Password	Password for the Virtual Center
Certificate Authentication	Enables or disables certificate authentication.

VM Profiles Configuration

Device Console > Configure > Virtualization > Profiles

Use this feature to configure VM Profiles.

Configuration of VMs with the VM Agent requires the use of VM profiles, which ease the configuration and management of VM Agent-based VM groups. The VM profile contains a set of properties that will be configured on the Virtual Switch.

After a VM profile has been defined, it can be assigned to a VM group or exported to one or more VMware hosts

The following table describes the fields of the **Profiles** configuration tab.

Table 324 Virtualization Profiles field descriptions

Field	Description
Name	Name of the profile
Vlan	Sets the VM profile's VLAN ID
Traffic Shaping Parameters - Average Bandwidth	Sets the average traffic, in Kilobits per second for the hypervisor's traffic shaping parameter.
Traffic Shaping Parameters - Burst Size	Sets the maximum burst size, in Kilobytes, for the hypervisor's traffic shaping parameter.
Traffic Shaping Parameters - Peak Bandwidth	Sets the peak traffic, in Kilobits per second, for the hypervisor's traffic shaping parameter.
Egress Shaping Parameters - Egress Average Bandwidth	Sets the Egress average traffic, in Kilobits per second for the hypervisor's traffic shaping parameter.
Egress Shaping Parameters - Egress Burst Size	Sets the maximum Egress burst size, in Kilobytes, for the hypervisor's traffic shaping parameter.
Egress Shaping Parameters - Egress Peak Bandwidth	Sets the Egress peak traffic, in Kilobits per second, for the hypervisor's traffic shaping parameter.

VM Groups Configuration

Device Console > Configure > Virtualization > Groups

Use this feature to configure VM Groups.

A VM group is a collection of members, such as VMs, ports, or trunk groups. Members of a VM group share certain properties, including VLAN membership, ACLs (VMAP), and VM profiles.

The following table describes the fields of the **Groups** configuration tab.

Table 325 Virtualization Groups field descriptions

Field	Description
Group Number	VM group number
Validation Mode	Sets the group validation mode: disable, basic, advanced.
Profile	Adds the selected VM profile to the VM group.
Vlan	Assigns a VLAN to this VM group. If you do not assign a VLAN to the VM group, the switch automatically assigns an unused VLAN when adding a port or a VM to the VM Group. Note: If you add a VM profile to this group, the group will use the VLAN assigned to the profile.
Tag State	Enables or disables VLAN tagging on ports in this VM group.
Ports	Adds the selected port to the VM group. Note: Add a port to a VM group only if no VMs on that port are members of the VM group.
Trunk ID	Assigns the trunk group to the VM group.
LACP Adminkey	Assigns an LACP admin key to the VM group. LACP trunks formed with this admin key will be included in the VM group.
VMAP for Non Server Ports	Assigns the selected VLAN Map to this VM group, limiting the operation of the VLAN Map to non-server ports only.
VMAP for Server Ports	Assigns the selected VLAN Map to this VM group, limiting the operation of the VLAN Map to server ports only.
VMAP for All Ports	Assigns the selected VLAN Map to this VM group with the operation of the VLAN Map extending to non-server and Server ports.

VM Bandwidth Configuration

Device Console > Configure > Virtualization > *Bandwidth*

Use this feature to limit the Transmit Bandwidth for each VM.

The following table describes the fields of the **Bandwidth** configuration tab.

Note: Some fields might not be available for the selected switch type. Please disregard field descriptions that do not apply to your switch.

Table 326 Virtualization Bandwidth field descriptions

Field	Description
MAC	MAC address of the virtual machine.
ACL for Transmit Bandwidth	The ACL assigned to the transmission rate. The ACL is assigned automatically, in sequential order, if not specified. If there are no available ACLs, the Transmit Rate cannot be configured. Each Transmit Rate configuration reduces the number of available ACLs by one.
Control Status	Enables or disables bandwidth control on the VM policy
Committed TX Rate	The amount of bandwidth available to traffic transmitted from the VM to the switch, in kilobits per second. Enter the value in multiples of 64.
Maximum TX Burst Size	The maximum burst size for transmission, in Kilobits. Enter one of the following values: 32, 64, 128, 256, 512, 1024, 2048, 4096.
Committed RX Rate	The amount of bandwidth available to traffic received from the VM to the switch, in kilobits per second. Enter the value in multiples of 64.
Maximum RX Burst Size	The maximum burst size for receiving, in Kilobits. Enter one of the following values: 32, 64, 128, 256, 512, 1024, 2048, 4096.

VM Check Configuration

Device Console > Configure > Virtualization > VMready > VM Check

Use the **VM Check** tab for configuring the validations.

Note: This tab or some of its fields might not be available for the selected switch type. Please disregard field descriptions that do not apply to your switch.

Table 327 VM Check field descriptions

Field	Description
Basic Mode Validation	Sets basic checking mode: log, link
Advanced Mode Validation	Sets advanced checking mode: log, link, acl
Max ACLs for Spoofed MACs	Sets value for the maximum number of ACLs that can be used by MAC Spoofing Check feature.
Trusted Ports	Add ports to configured trusted port list or remove ports from the configured trusted port list.

VM Hello Configuration

Device Console > Configure > Virtualization > VMready > VM Hello

Use the **VM Hello** tab for configuring Hello advertising.

Note: This tab or some of its fields might not be available for the selected switch type. Please disregard field descriptions that do not apply to your switch.

Table 328 VM Hello field descriptions

Field	Description
Hello Advertisements	Sets the Hello advertising status.
Ports	Add ports to configured Hello port list or remove ports from the configured Hello port list.
Hello Address	Sets the VM Hello IP address.
Hello Periodicity	Sets the Hello packet send interval.

VM Ports Configuration

Device Console > Configure > Virtualization > Ports

Use this feature to assign the configured VM Group to non-server (Uplink) and server ports.

The following table describes the fields of the **Ports** configuration tab.

Table 329 Virtualization Ports field descriptions

Field	Description
Status	Color coded graphics showing the status: Green for up and Red for down.
Port	The non-server (Uplink) or server port number.
Group	Configured VM Group. Double-click the cell to configure a new value.
Trunk #	Trunk number to which the port is associated.
LACP Key #	LACP key number to which the port is associated.

Virtual Machines Configuration

Device Console > Configure > Virtualization > *Virtual Machines*

Use this feature to assign the configured VM Group to VMs.

The following table describes the fields of the **Virtual Machines** configuration tab.

Table 330 Virtual Machines field descriptions

Field	Description
Filter by Group	Lists only entries associated with the selected VM group.
Virtual MAC	MAC address of the virtual machine.
Group	Configured VM Group. Double-click the cell to configure a new value.
IP Address	IP Address of the Virtual Machine.
VM Name	Name of the discovered virtual machine. If the VM Management Server Connector is not configured, this field is blank.
Hypervisor	Name of the Hypervisor on which the VM is running. If the VM Management Server Connector is not configured, this field is blank.
VLAN	VLAN to which the Virtual Machine is associated.
Port	Server Port on which VM is discovered by the switch

VM Advanced Pre-Provisioning

Device Console > Configure > Virtualization > *Advanced Pre-Provisioning*

Use this feature to Pre-provision the VMs by assigning the VM Group to each selected VM.

Note: The VMs listed in the table are retrieved from Virtual Center and not learned by the switch. In addition, the VMs are listed only if the VM Management Server is configured.

The following table describes the fields of the **Advanced Pre-Provisioning** configuration tab.

Table 331 Advanced Pre-Provisioning field descriptions

Field	Description
Global Group	The VM group to use when VM group is NOT selected for the selected VM.
Virtual MAC	MAC address of the virtual machine.
Group	Configured VM Group. Double-click the cell to configure a new value.
IP Address	IP Address of the Virtual Machine.
VM Name	Name of the discovered virtual machine. If the VM Management Server Connector is not configured, this field is blank.
Hypervisor	Name of the Hypervisor on which the VM is running. If the VM Management Server Connector is not configured, this field is blank.
vCenter Name	The VM ware Virtual Center address
VLAN	VLAN to which the Virtual Machine is associated.
Port Group	Port Group to which the Virtual Machine is associated.

vNIC General Configuration

Device Console > Configure > Virtualization > vNIC > *General*

Use this tab to enable or disable vNIC configuration on the switch.

Table 332 vNIC General field descriptions

Field	Description
Global vNIC On/Off	Enables or disables the vNIC configuration feature.

vNIC Port Configuration

Device Console > Configure > Virtualization > vNIC > vNIC

Use this to configure vNICs on switch server ports.

Table 333 vNIC Port field descriptions

Field	Description
Port	Server port on which the vNIC is configured
vNIC	vNIC ID (1-4)
State	Operational state of the vNIC (enabled or disabled)
Max Bandwidth	Maximum bandwidth allocated to the vNIC

vNIC Group Configuration

Device Console > Configure > Virtualization > vNIC > vNIC Groups

Use this tab to configure vNIC groups on the switch.

Note: This tab or some of its fields might not be available for the selected switch. Please disregard this information if it does not apply to your switch.

Table 334 vNIC Groups field descriptions

Field	Description
Group Number	vNIC group ID (1-32).
State	Operational state of the vNIC group (enabled or disabled).
VLAN	VLAN associated with the vNIC group.
Failover state	Failover state of the vNIC group (enabled or disabled).
Key	Uplink LACP admin key in the vNIC group.
vNIC	vNICs associated with the vNIC group.
Server Ports	Server ports associated with the vNIC group.
Uplink Type	Sets the uplink type (port or trunk). Depending on the selection, SNSC chooses either port or trunk data while configuring vNIC groups on the switch.
Port	The port associated with the vNIC group. Note: Applicable only if the Uplink Type is set to <code>Port</code> .
Trunk	The trunk associated with the vNIC group. Note: Applicable only if the Uplink Type is set to <code>Trunk</code> .

EVB General Configuration

Device Console > Configure > Virtualization > EVB > General

Use this tab to configure Edge Virtual Bridging (EVB) retransmission interval and performing VSI DB update/clean operation.

Table 335 EVB General field descriptions

Field	Description
Retransmission Interval	Sets the retransmission interval in seconds.
VSI DB Operation	Sets the VSI DB Operation to none, update or clean. The default setting is <code>none</code> , which indicates no operation. If you select update option and click Submit , then the switch will pull VSI Types from the VSI DB Manager. If you select clean option and click Submit , the VSI Types on the switch will be deleted.
Clean Associated VSI	Cleans the associated VSI from the switch.

EVB Profiles Configuration

Device Console > Configure > Virtualization > EVB > Profiles

Use this tab to configure Edge Virtual Bridging (EVB) profiles.

Table 336 EVB Profiles field descriptions

Field	Description
Profile Number	The profile index number.
Reflective Relay	Enables or disables the reflective relay.
VSI Discovery	Enables or disables VSI discovery.

VSI DB Host Configuration

Device Console > Configure > Virtualization > EVB > VSI DB Host

Use this tab to configure the VSI Database Host.

Table 337 VSI DB Host field descriptions

Field	Description
Index	The index number. The index is always 1.
VSI DB Host Address	Sets the IP address of VSI DB Manager.
VSI DB Host Port	Sets the port on which VSI DB Manager is listening for processing RESTful requests.
Doc Path	Sets the resource path.
Doc File	Sets the resource name.
Interval	Sets the VSI DB automatic update interval (5-300 s). Set the interval to 0 (zero) to disable automatic updates.

Configuring iSwitch Virtual Data Station

The following sections describe iSwitch vCenter and Virtual Data Station configuration tasks you can perform:

- [“vCenter Configuration” on page 615](#)
- [“Virtual Data Station Configuration” on page 616](#)

vCenter Configuration

Device Console > Configure > Virtualization > iSwitch > vCenter

Use this tab to configure iSwitch vCenter parameters.

Table 338 vCenter field descriptions

Field	Description
vCenter IP Address	Sets the IP address of the vCenter.
User Name	Sets the user name associated with the vCenter.
Password	Sets the user password.
Port	Sets the port on which vCenter is listening.
Apply/Delete vCenter Configuration	Applies or deletes the vCenter configuration, depending on the radio button selection.

Virtual Data Station Configuration

Device Console > Configure > Virtualization > iSwitch > *Virtual Data Station*

Use this tab to configure iSwitch Virtual Data Station parameters.

Table 339 Virtual Data Station field descriptions

Field	Description
vDS Name	Sets the name for virtual data station (vDS).
DataCenter Name	Sets the name of the datacenter associated with the vDS.
Apply/Delete VDS Configuration	Applies or deletes the VDS configuration, depending on the radio button selection.

Configuring Unified Fabric Port (UFP)

The following sections describe the configuration tasks associated with UFP:

- [“UFP General Configuration” on page 618](#)
- [“UFP Ports Configuration” on page 619](#)
- [“UFP Virtual Ports Configuration” on page 620](#)

UFP General Configuration

Device Console > Configure > Virtualization > UFP > General

Use this tab to configure general UFP parameters.

Note: This tab might not be available for the selected switch type. Please disregard field descriptions that do not apply to your switch.

Table 340 UFP General field descriptions

Field	Description
UFP	Enables or disables UFP.

UFP Ports Configuration

Device Console > Configure > Virtualization > UFP > Ports

Use the **Ports** tab to configure UFP port parameters.

Note: This tab might not be available for the selected switch type. Please disregard field descriptions that do not apply to your switch.

Table 341 UFP Port field descriptions

Field	Description
Index	The port number.
State	Enables or disables UFP on the selected port.

UFP Virtual Ports Configuration

Device Console > Configure > Virtualization > UFP > *Virtual Ports*

Use the **Virtual Ports** tab to configure UFP virtual port parameters.

Note: This tab might not be available for the selected switch type. Please disregard field descriptions that do not apply to your switch.

Table 342 UFP Virtual Port field descriptions

Field	Description
Port Index	The port number of the vPort.
vPort Index	The virtual port number of the vPort.
State	Enables or disables virtual port State.
Network Mode	Sets the virtual port network mode.
Network Default VLAN	Sets the virtual port default VLAN.
Network Default Tag	Enables or disables the virtual port tag state.
QoS Min Guaranteed Bandwidth	Sets the QoS minimum guaranteed bandwidth.
QoS Max Allowed Bandwidth	Sets the QoS maximum allowed bandwidth.

Using the VMready Across the Datacenter Wizard

The VMready Across the Datacenter Wizard provides a step by step approach to configure VMready features across all supported switches. The features include VM Server configuration, Hypervisor configuration, VM Groups configuration, Virtual Machines configuration, VMAP configuration, Server Ports configuration (this is applicable only for RackSwitches), Port Groups, and vSwitch Configuration. It provides an interface to directly deploy the configuration created across the various VMready switches. Some of the steps are not mandatory and can be skipped during the configuration.

The Wizard steps you through the configuration process. The topics in this chapter cover the following procedures:

- [“Configuring VMready Across the Datacenter Wizard” on page 622](#)
- [“Step 2: Select VMready Switches” on page 626](#)
- [“Step 3: Define the VM Management Server” on page 628](#)
- [“Step 4: Select Hypervisors” on page 631](#)
- [“Step 5: Configure VM Groups” on page 633](#)
- [“Step 6: Configure Virtual Machines” on page 635](#)
- [“Step 7: VMAPs” on page 639](#)
- [“Step 8: Configure Server Ports” on page 645](#)
- [“Step 9: Configure Switch-Specific Settings” on page 648](#)
- [“Step 10: Configure Port Groups” on page 651](#)
- [“Step 11: Associate Port Group to a vSwitch” on page 654](#)
- [“Step 12: Review and Deploy the Configuration” on page 657](#)

Configuring VMready Across the Datacenter Wizard

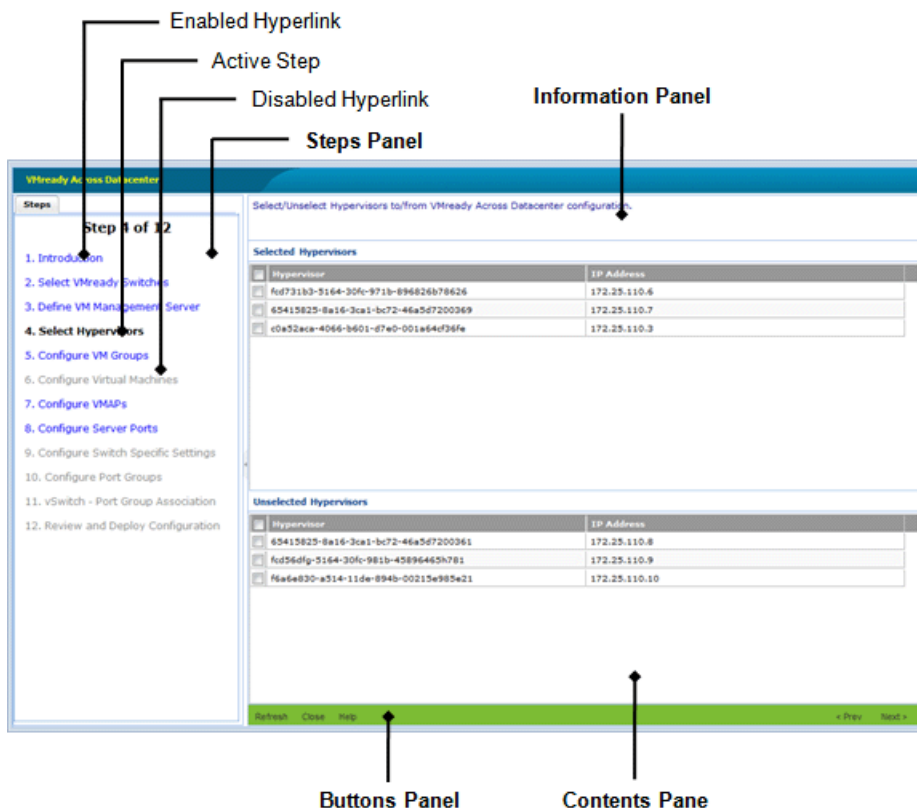
Device List > Virtualization Tools > *VMready Across Datacenter*

Figure 62 on page 622 shows the layout of the Wizard screen, which is comprised of two panels, a left panel indicating the steps of configuration available in the Wizard and a content panel showing the configurations for the corresponding step. Based on the content panel configuration, the corresponding step is highlighted in the left side panel. You also can navigate to any step by clicking on any step, which doubles as a hyperlink. Note that the hyperlink is activated only after visiting that step.

Note 1: Only admin-level users can perform Wizard configuration and deployment.

Note 2: Before you use the VMready Across the Datacenter Wizard for the RackSwitch G8000, G8052, G8124 and G8264, ensure that Virtual Machine Groups setting is enabled.

Figure 62 VMready Across the Datacenter—Wizard Layout



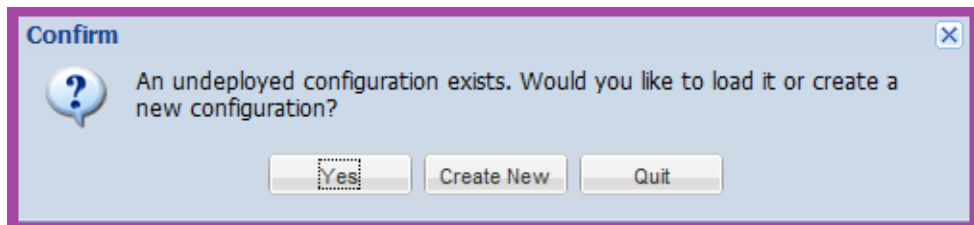
The content panel has three sections, as follows:

- Information panel at the top displays a summary of the configuration for the particular step.
- Content pane in the center allows you to view and edit the configuration. Note: When you modify data in a cell, the cell appears blue until the change is saved.
- Buttons menu at the bottom allows you perform various actions and traverse across the Wizard.

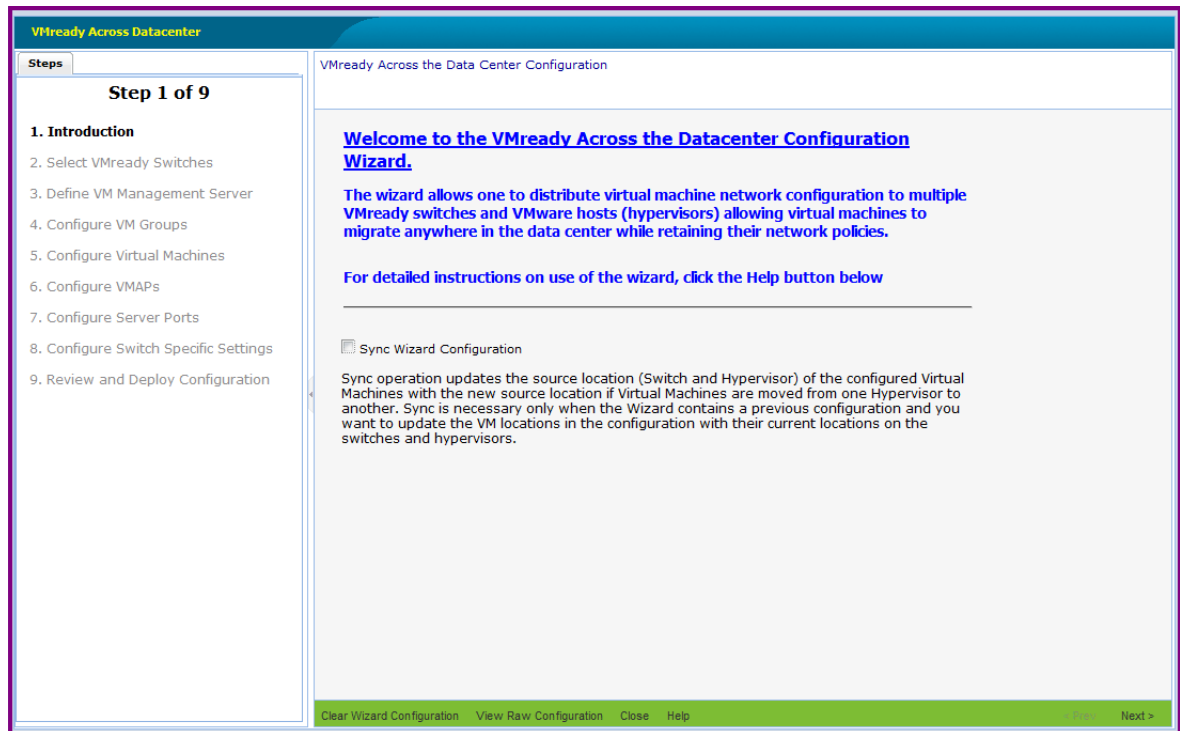
Note 1: The steps listed in the left panel are displayed when the VM Management Server is configured. If VM Management Server is not configured, then some steps are not visible.

Note 2: If an undeployed configuration exists, upon launch of the Wizard you are presented with a dialog box with options to load an existing configuration or create a new configuration as shown in [Figure 63 on page 623](#).

Figure 63 VMready Across the Datacenter—Launch Dialog



The introduction step of the Wizard does not perform any configuration. However, this step provides an option for the user to synchronize the previous configuration, clear any existing configuration or view the XML configuration in HTML format (see [Figure 64 on page 624](#)).

Figure 64 VMready Across the Datacenter—Wizard Introduction

Button/Checkbox	Description
Sync Wizard Configuration	Synchronizes the VM source addresses in the existing configuration by checking with VM Management Server and the configured VMready switches.
Clear Wizard Configuration	Clears the VMready Across the Datacenter Wizard configuration on the SNSC server.
View Raw Configuration	Opens a window showing the XML configuration, in HTML format (see Figure 66 on page 626).
Close	Closes the window. This action also gives an option for the user to keep or discard (delete) the undeployed configuration (XML).
Help	Opens the online Help page.
Next	Moves to the next step or page in the configuration.

Figure 65 VMready Across the Datacenter—XML Configuration in HTML Format

vm-domain							
name		deployment-status					
default		notyet					
switches-list							
vmready-switches							
status	ipaddress	deploy-status	is-deleted	vmap-deploy-status			
new	192.168.6.81	notyet	no	notyet			
current	192.168.6.82	succeeded	no	succeeded			
current	192.168.6.83	failed	no	succeeded			
vmgroups-list							
vmgroup							
status	id	desc	VLAN	tag-state			
new	1	vmg1	1	e			
vmgroup-switch-conf							
	switch-conf						
status	ipaddress	ports	lacp-adminkey	trunkid	vmap-ports-srvr	vmap-ports-nonsrvr	vmap-ports-all
new	192.168.6.81	INT1;MGT1	17-18				
current	192.168.6.82	INT2;MGT1	17-18				
current	192.168.6.83	INT3;MGT1	17-18				
vmgroup							
status	id	desc	VLAN	tag-state			
new	2	vmg2	2	e			
vmgroup-switch-conf							
	switch-conf						

Step 2: Select VMready Switches

This step lists all VMready switches discovered by System Networking Switch Center (SNSC) and allows you to select the VMready switches in the configuration. For a new configuration, the switches are listed in the Unselected VMready Switches table. You can drag-and-drop the switch(es) to the Selected VMready Switches table. You also can drag-and-drop the switch(es) from the Selected VMready Switches table to the Unselected VMready Switches table. See [Figure 66 on page 626](#).

Note: The **Next** button is enabled only when one or more switches are added to the Select VMready Switches table.

Figure 66 VMready Across the Datacenter—Select VMready Switches

VMready Across Datacenter

Steps

Step 2 of 9

1. Introduction
- 2. Select VMready Switches**
3. Define VM Management Server
4. Configure VM Groups
5. Configure Virtual Machines
6. Configure VMAPs
7. Configure Server Ports
8. Configure Switch Specific Settings
9. Review and Deploy Configuration

Select/Unselect VMready Switches to/from VMready Across Datacenter configuration.
Note: Drag-and-drop the rows between the tables for selecting/unselecting the switches.

Selected VMready Switches

Product Type	IP Address	System Name	Health Status
<input type="checkbox"/> BNT 10-port 10Gb Ethernet Switch	192.168.6.81		● Up
<input type="checkbox"/> BNT 10-port 10Gb Ethernet Switch	192.168.6.82		● Up
<input type="checkbox"/> BNT 10-port 10Gb Ethernet Switch	192.168.6.83		● Up
<input type="checkbox"/> BNT 10-port 10Gb Ethernet Switch	192.168.6.84		● Up

Unselected VMready Switches

Product Type	IP Address	System Name	Health Status
<input type="checkbox"/> BNT RackSwitch G8124	192.168.6.90	BHM	● Up
<input type="checkbox"/> BNT RackSwitch G8052	172.16.2.92	G8052_	✖ Down
<input type="checkbox"/> BNT RackSwitch G8264	172.16.2.91	G8264	● Up
<input type="checkbox"/> BNT/Nortel 1/10Gb Uplink Ethernet	192.168.6.75		● Up

Refresh Close Help < Prev Next >

Table 343 Selected VMready Switches field descriptions

Field	Description
Product Type	Switch type (for example, BNT 10-port 10Gb Ethernet Switch Module).
IP Address	IP address of the VMready switch.

Table 343 Selected VMready Switches field descriptions

Field	Description
System Name	Configured system name (sysName)
Health Status	Health status of the switch (Up, Down, Critical or Non-Critical).

This step provides the following primary options:

Button	Description
Refresh	Refreshes the list of switches in the Unselected VMready Switches table.
Close	Closes the window. This action also gives an option for the user to keep or discard (delete) the undeployed configuration (XML).
Help	Opens the online Help page.
Next	Moves to the next step or page in the configuration. Note that the Next button is disabled until you add a VMready switch.
Prev	Moves to the previous step or page in the configuration.

Step 3: Define the VM Management Server

This step is required only for a VMware environment, for which the VM Management Server (vCenter) can be configured and Hypervisors can be added in the VMready configuration. This step is optional and clicking **Next** will take you to step 4: Configuring VM Groups.

A VM Management Server (vCenter) can be configured by checking the checkbox and specifying the VM Management Server address, login credentials, protocol and port details. It gives an option to test the values configured by clicking **Test**. See [Figure 67 on page 629](#).

Note: The **Test** button is enabled only if the checkbox is selected and required values are entered.

Figure 67 VMready Across the Datacenter—Define VM Server

VMready Across Datacenter

Steps

Step 3 of 12

1. Introduction
2. Select VMready Switches
- 3. Define VM Management Server**
4. Select Hypervisors
5. Configure VM Groups
6. Configure Virtual Machines
7. Configure VMAPs
8. Configure Server Ports
9. Configure Switch Specific Settings
10. Configure Port Groups
11. vSwitch - Port Group Association
12. Review and Deploy Configuration

Configure the VM Management Server to access. Note that this is required only if you wish to also configure the virtual machine policies on VMware hypervisors. If you don't, you can skip this step.

VM Management Server Configuration

☒ Configure VM Management Server

IP Address/Host Name: 172.25.110.4 -- Select --

Protocol: HTTPS

Port: 443 1..65535

User Name: Administrator 1..127 characters

Password: 1..65 characters

SSL Certificate File Path: /opt/ibm/snem/certs/172_25_110_4_Vmware.crt Browse...

Test Close Help < Prev Next >

Table 344 Define VM Management Server field descriptions

Field	Description
Configure VM Management Server	Checkbox that enables/disables VM Management Server configuration. By default, it is unchecked (disabled).
Protocol	Protocol to use for communicating with VM Management Server. It is either HTTP or HTTPS.
Port	Port on which the VM Management Server is accessible when the above configured protocol is used.
IP Address/Host Name	IP address or host name of the VM Management Server. You can select the VM Management Server address from the drop-down list, which shows the VM Management Servers configured in SNSC.
User Name	User name to use for accessing the VM Management Server.
Password	Password associated with the user name.
SSL Certificate File Path	Path on the local system containing the SSL certificate to use in case of HTTPS Protocol setting.

Button	Description
Test	Tests the configured parameters for validity.
Close	Closes the window. This action also gives an option for the user to keep or discard (delete) the undeployed configuration (XML).
Help	Opens the online Help page.
Next	Moves to the next step or page in the configuration. Note that the Next button is disabled until you configure this step.
Prev	Moves to the previous step or page in the configuration.

Step 4: Select Hypervisors

This step is skipped if you did not configure a VM Management Server (vCenter) in step 3.

This page lists all hypervisors that are known to the configured VM Management Server (see [“Step 3: Define the VM Management Server” on page 628](#)). For a new configuration, the hypervisors are listed in the Unselected Hypervisors table. You can drag-and-drop the hypervisor(s) to the Selected Hypervisors table to select them. Likewise, you can drag-and-drop the hypervisor(s) from the Selected Hypervisors table to the Unselected Hypervisors. See [Figure 68 on page 631](#).

Note: The **Next** button is enabled only when one or more hypervisors are added to the Select Hypervisors table.

Figure 68 VMready Across the Datacenter—Select Hypervisors

VMready Across Datacenter

Steps

Step 4 of 12

1. Introduction
2. Select VMready Switches
3. Define VM Management Server
- 4. Select Hypervisors**
5. Configure VM Groups
6. Configure Virtual Machines
7. Configure VMAPs
8. Configure Server Ports
9. Configure Switch Specific Settings
10. Configure Port Groups
11. vSwitch - Port Group Association
12. Review and Deploy Configuration

Select/Unselect Hypervisors to/from VMready Across Datacenter configuration.
Note: Drag-and-drop the rows between the tables for selecting/unselecting the hypervisors.

Selected Hypervisors				
	Hypervisor	Name	IP Address	Type
<input checked="" type="checkbox"/>	c0a52aca-4066-b601-d7e0-001a	172.25.110.3	172.25.110.29	VMware ESX 4.0.0 build-208167

Unselected Hypervisors				
	Hypervisor	Name	IP Address	Type
<input checked="" type="checkbox"/>	65415825-8a16-3ca1-bc72-46a5	172.25.110.7	172.25.110.19	VMware ESX 4.0.0 build-208167
<input checked="" type="checkbox"/>	fcd731b3-5164-30fc-971b-8968	172.25.110.6	172.25.110.15	VMware ESX 4.0.0 build-208167

Refresh Close Help < Prev Next >

Table 345 Selected Hypervisors field descriptions

Field	Description
Hypervisor	Unique identifier (UUID) of the hypervisor.
Name	Name of the hypervisor.
IP Address	IP address of the hypervisor.
Type	Hypervisor type, including the version number and the build number.

This step provides the following primary options:

Button	Description
Refresh	Refreshes the list of switches in the Unselected Hypervisors table.
Close	Closes the window. This action also gives an option for the user to keep or discard (delete) the undeployed configuration (XML).
Help	Opens the online Help page.
Next	Moves to the next step or page in the configuration. Note that the Next button is disabled until you add a Hypervisor.
Prev	Moves to the previous step or page in the configuration.

Step 5: Configure VM Groups

This step lists the VM Groups configured by the Wizard. It also allows you to add new groups, modify any existing groups, and remove previously configured groups. See [Figure 69 on page 633](#).

Note: For a new configuration, the VM Groups table is blank and the **Next** button is disabled until a VM Group is added.

Figure 69 VMready Across the Datacenter—Configure VM Groups

VMready Across the Datacenter

Steps

Step 5 of 12

- 1. Introduction
- 2. Select VMready Switches
- 3. Define VM Management Server
- 4. Select Hypervisors
- 5. Configure VM Groups**
- 6. Configure Virtual Machines
- 7. Configure VMAPs
- 8. Configure Server Ports
- 9. Configure Switch Specific Settings
- 10. Configure Port Groups
- 11. vSwitch - Port Group Association
- 12. Review and Deploy Configuration

Add/Modify/Remove VM Groups to/from VMready Across Datacenter configuration. Note that you can only configure upto 32 VM Groups on a Switch.

VM Groups

VM Group #	Description	VLAN	Tag State
1	vmg - engineering	1	enabled
2	vmg - finance	2	enabled
3	vmg - admin	3	disabled

Add Modify Remove Close Help < Prev Next >

Table 346 Configure VM Groups field descriptions

Field	Description
VM Group #	VM Group number.
Description	Text description given to the VM Group for convenience. This description is local to SNSC and not relayed to the VMready switches.
VLAN	VLAN assigned to the VM Group.
Tag State	Tag state (enabled or disabled).

This step provides the following primary options:

Button	Description
Add	Opens a child window to add a VM Group.
Modify	Opens a child window that allows you to modify the selected VM Group. Note: This button is enabled only when a row is selected.
Remove	Removes the selected VM Group(s). Note: This button is enabled only when one or more rows are selected.
Close	Closes the window. This action also gives an option for the user to keep or discard (delete) the undeployed configuration (XML).
Help	Opens the online Help page.
Next	Moves to the next step or page in the configuration. Note that the Next button is disabled until you configure a VM group.
Prev	Moves to the previous step or page in the configuration.

Step 6: Configure Virtual Machines

This step lists the Virtual Machines (VMs) assigned to the VM groups created in step 5. For a new configuration the page is empty and you can add a VM or a pre-provisioned VM MAC to proceed with the Wizard configuration. You can filter the list based on the VM Group selected as shown in [Figure 70 on page 635](#).

Figure 70 VMready Across the Datacenter—Configure Virtual Machines

VMready Across Datacenter

Steps

Step 6 of 12

1. Introduction
2. Select VMready Switches
3. Define VM Management Server
4. Select Hypervisors
5. Configure VM Groups
- 6. Configure Virtual Machines**
7. Configure VMAPs
8. Configure Server Ports
9. Configure Switch Specific Settings
10. Configure Port Groups
11. vSwitch - Port Group Association
12. Review and Deploy Configuration

Add/Modify/Remove Virtual Machines (learned or pre-provisioned) to/from the configured VM Groups. Note that the configuration of Receive Bandwidth (RX) parameters is supported only for 'BNT Virtual Fabric 10G Switch Module' and 'BNT RackSwitch G8052' devices.

Virtual Machines

VM Group: All

	VM Name	IP Address	Virtual MAC	Source		Transmit Bandwidth		Receive Bandwidth		ACL ID For Meter	VM Group #
				Switch	Hypervisor	Committed TX Rate	Maximum TX Burst Size	Committed RX Rate	Maximum RX Burst Size		
<input type="checkbox"/>			00:50:56:8f:58:90			0	0	0	0	0	1
<input type="checkbox"/>			00:50:56:8f:58:91			0	0	0	0	0	1
<input type="checkbox"/>	VM5		00:50:56:8f:5f:6b		172.25.110.6	0	0	0	0	0	1
<input type="checkbox"/>	VM2		00:50:56:8f:70:67		172.25.110.3	0	0	0	0	0	1
<input type="checkbox"/>	VM4		00:50:56:8f:2b:10		172.25.110.3	0	0	0	0	0	1
<input type="checkbox"/>	VM3		00:50:56:8f:28:28		172.25.110.6	0	0	0	0	0	1
<input type="checkbox"/>	VM1		00:50:56:8f:51:30		172.25.110.7	0	0	0	0	0	1
<input type="checkbox"/>		172.25.110.1	00:50:56:75:e6:7c		172.25.110.7 (VM 0	0	0	0	0	0	1
<input type="checkbox"/>		172.25.110.2	00:50:56:70:29:e7		172.25.110.3 (VM 0	0	0	0	0	0	1
<input type="checkbox"/>		172.25.110.1	00:50:56:73:99:30		172.25.110.6 (VM 0	0	0	0	0	0	1

Pre-provisioned MAC Add Remove Close Help

< Prev Next >

Table 347 Configure Virtual Machines field descriptions

Field	Description
VM Group	The VM Group drop-down list displays the configured VM Groups, plus a selection for “All”, which shows the VMs configured for all VM Groups. Note: This field is not part of the table, but is available above the table.
VM Name	Name of the Virtual Machine assigned to the VM Group. Note: If the VM is pre-provisioned, this field is blank.
IP Address	IP address of the VM. Note: If VM is pre-provisioned, this field is blank.
Virtual MAC	The MAC address of the VM.
	Source

Table 347 Configure Virtual Machines field descriptions

Field	Description
Switch	VMready switch which has discovered this VM. Note: This field can be blank.
Hypervisor	Hypervisor which has discovered this VM. Note: This field can be blank.
	Bandwidth Control Parameters
Committed TX Rate	Committed transmission rate.
Maximum TX Burst Size	Maximum transmission burst size.
Committed RX Rate	Committed receive rate.
Maximum RX Burst Size	Maximum receive burst size.
ACL ID For Meter	The ACL identifier.
VM Group #	The VM Group for which this VM is added (useful when the "All" option is selected in VM Group filter).

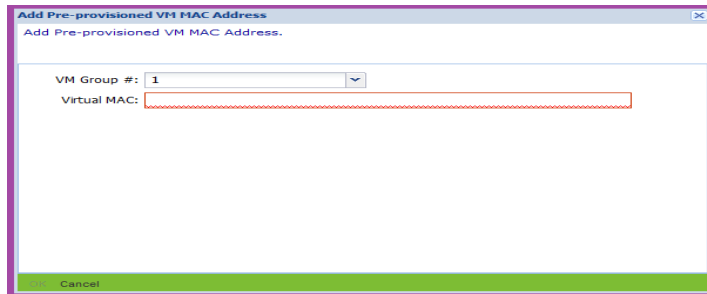
This step provides the following primary options:

Button	Description
Pre-provisioned MAC	Opens a child window to add a pre-provisioned VM MAC.
Add	Opens a child window to add a VM.
Modify	Opens a child window that allows you to modify the selected VM Bandwidth parameters. Note: This button is enabled only when a row is selected.
Remove	Removes the selected VM(s). Note: This button is enabled only when one or more rows are selected.
Close	Closes the window. This action also gives an option for the user to keep or discard (delete) the undeployed configuration (XML).
Help	Opens the online Help page.
Next	Moves to the next step or page in the configuration. Note that the Next button is disabled until you configure a Virtual Machine.
Prev	Moves to the previous step or page in the configuration.

Step 6.1: Pre-Provisioned VM MAC

You can pre-provision a VM which is not yet discovered by any of the VMready switches configured for this VMready configuration. On the Virtual Machines page, click **Pre-provisioned MAC**. This action launches a child window enabling the user to specify the VM MAC Address and the VM Group to which this pre-provisioned MAC is to be added. See [Figure 71 on page 637](#).

Figure 71 Add Pre-provisioned VM



The screenshot shows a dialog box titled "Add Pre-provisioned VM MAC Address" with a close button in the top right corner. Below the title bar, the text "Add Pre-provisioned VM MAC Address." is displayed. The main area of the dialog contains two fields: "VM Group #:" with a dropdown menu showing the value "1", and "Virtual MAC:" with an empty text input field. At the bottom of the dialog, there is a green bar containing a "Cancel" button.

Step 6.2: Add VMs Learned or Retrieved

Virtual Machines (VMs) can be learned by one or more VMready switches configured for this VMready configuration. VMs also can be retrieved from the VM Management Server (if it is configured). If these VMs are not yet discovered by VMready switches, from the Virtual Machine page you can click **Add**. This action launches a child window listing the VMs that are not yet added. See [Figure 72 on page 638](#).

Figure 72 Add Virtual Machines

Add Virtual Machines

Add VMs that are learned by each of the VMready switches and Hypervisors configured.

Add Virtual Machines

VM Group #: 1

	VM Name	IP Address	Virtual MAC	Source	
				Switch	Hypervisor
<input type="checkbox"/>	VMrad-VM3		00:50:56:93:46:7		172.20.95.200
<input type="checkbox"/>	New Virtual Machin		00:50:56:80:54:f0		172.20.95.200
<input type="checkbox"/>	VMrad-VM5		00:50:56:93:6a:2		172.20.89.15
<input type="checkbox"/>	VMrad-VM1		00:50:56:93:34:9		172.20.95.200
<input type="checkbox"/>	DEMO_VA		00:50:56:80:72:d		172.20.95.200
<input type="checkbox"/>		172.16.3.220	00:50:56:43:46:2	172.16.200.2, por	
<input type="checkbox"/>		172.16.3.227	00:50:56:7e:ba:f6	172.16.200.2, por	

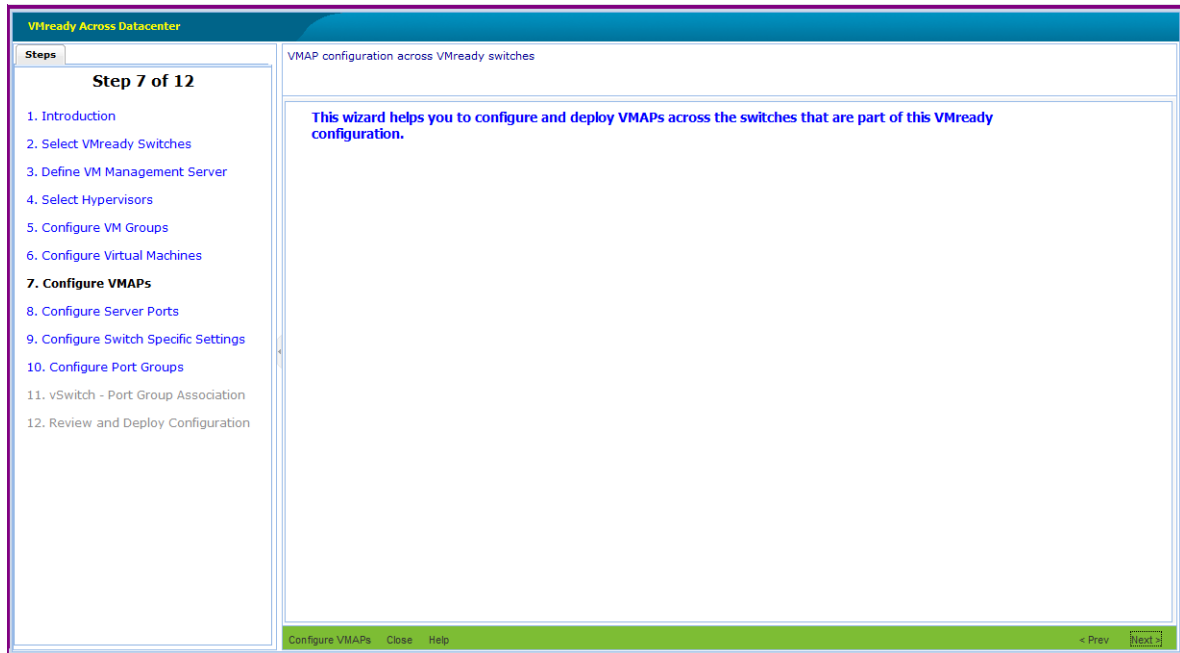
OK Cancel

Step 7: VMAPs

This step allows you to create VMAPs across VMready switches specific to the VMready configuration. You can view, configure, and deploy VMAPs across VMready switches contained in the Wizard. See [Figure 73 on page 639](#).

Note: This step is optional. Click **Next** to go to the Configure Switch Setting page.

Figure 73 VMready Across the Datacenter—VMAP Welcome Screen



This step provides the following options:

Button	Description
Configure VMAPs	Opens the window for configuring VMAPs.
Close	Closes the window. This action also gives an option for the user to keep or discard (delete) the undeployed configuration (XML).
Help	Opens the online Help page.
Next	Moves to the next step or page in the configuration.
Prev	Moves to the previous step or page in the configuration.

Step 7.1: Configure VMAPs

To configure VMAPs, click **Configure VMAP** from the step 6 Welcome page. The VMAP Configuration table lists those VMAPs that are configured. It shows both deployed and Undeployed VMAP configurations on VMready switches. You can add a new VMAP or modify/delete an existing VMAP by clicking the appropriate button. See [Figure 74 on page 640](#).

Note: The VMAP configuration table lists only few parameters associated with the VMAP. To view the complete data, click **Details**.

Figure 74 VMready Across the Datacenter—Configure VMAPs

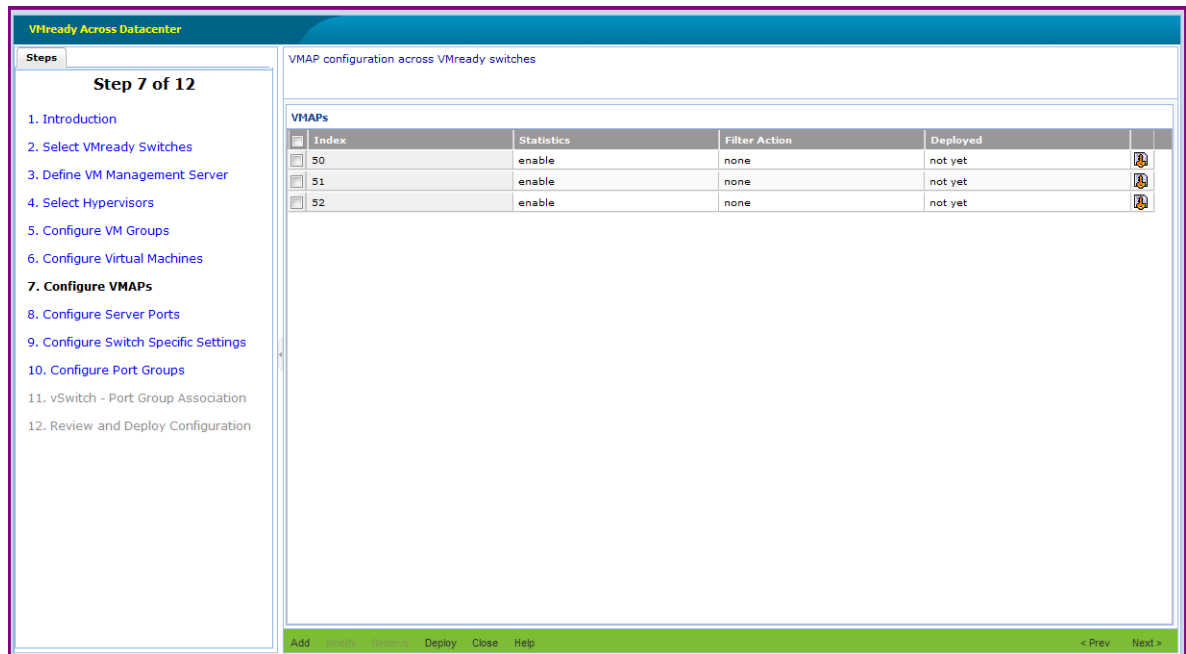


Table 348 Configure VMAPs field descriptions

Field	Description
Index	VMAP index number. Indices from 50 to 110 are reserved for the VMAP Wizard.
Statistics	Shows whether VMAP statistics is enabled or disabled.
Filter Action	Filter action setting.

Table 348 Configure VMAPs field descriptions

Field	Description
Deployed	Shows whether the VMAP is already configured/deployed (yes) on the switches or not (not yet).
Details	By clicking Details , you can view the complete VMAP configuration.

This step provides the following primary options:

Button	Description
Add	Opens a child window to add a new VMAP configuration.
Modify	Opens a child window to modify the VMAP configured. Note: This button is enabled only when a row is selected.
Remove	Removes the selected VMAP(S) configured. Note: This button is enabled only when a row is selected.
Deploy	Initiates the VMAP deployment to the VMready switches available in VMready configuration. Note: This button is enabled only if a VMAP entry exists. It deploys all the VMAPs that are in undeployed state.
Close	Closes the window. This action also gives an option for the user to keep or discard (delete) the undeployed configuration (XML).
Help	Opens the online Help page.
Next	Moves to the next step or page in the configuration.
Prev	Moves to the previous step or page in the configuration.

Step 7.2: Add VMAP Configuration

To create a new VMAP configuration, in the Configure VMAP page, click **Add**. This opens a new dialog with various parameters that can be provided for the VMAP configuration. See [Figure 75 on page 642](#). The fields are placed in different groups for ease of configuration. Enter the parameters in the dialog and click **Ok**.

Figure 75 Add New VMAP

Add New VMAP

Add a new VMAP to be part of this VMready configuration.

General Settings

Index: 53 50..110

Statistics: ☐ disable ☒ enable

Filter Action: none

Priority: none

Filtering Packet Format

Ethernet Format: none

Tag Format: disabled

IP Format: none

OK Cancel

Table 349 Add VMAPs field descriptions

Field	Description
Index	The VMAP index. The value 50 to 110 are reserved for SNSC VMready Wizard.
Statistics	Enables or disables the statistics.
Filter Action	Sets the filter action to none, permit, deny or setprio (set priority).
Priority	Sets the priority to none or 0-7. Note that this field is enabled only when you set the Filter Action to setprio. Or else, none is taken by default.
Ethernet Format	Sets the Ethernet format to none, Ethernet2, SNAP or LLC.
Tag Format	Sets the tag format (disabled, any, none, or tagged).
IP Format	Sets the IP format (none, ipv4 or ipv6).

Table 349 Add VMAPs field descriptions

Field	Description
Source MAC address	Sets the source MAC address.
Source MAC Mask	Sets the source MAC mask.
Destination MAC Address	Sets the destination MAC address.
Destination MAC Mask	Sets the destination MAC mask.
Ethernet Type	Sets the Ethernet type to none, arp, ipv4, ipv6, mpls, rarp, any or other.
Ethernet Value	Sets the Ethernet value. Note that this field is enabled only when you set the Ethernet type to “other”.
802.1p Priority	Sets 802.1p priority to none or 0-7.
Source IP Address	Sets the source IP address.
Source IP Mask	Sets the source IP mask.
Destination IP Address	Sets the destination IP address.
Destination IP Mask	Sets the destination IP mask.
Type Of Service	Sets the Type Of Service.
Protocol	Sets the protocol.
Source Port	Sets the source port.
Source Port Mask	Sets the source port mask.
Destination Port	Sets the destination port.
Destination Port Mask	Sets the destination port mask.
Committed Rate	Sets the committed rate.
Maximum Burst Size	Sets the maximum burst size.
Port Metering Status	Enables or disables port metering.
Meter Action	Sets the meter action to unconfigured, outdrop or outpass.
In Profile Dscp Enable	Enables or disables in-profile DSCP.
In Profile Dscp Value	Sets the in-profile DSCP value.
Out Profile Dscp Enable	Enables or disables out-of-profile DSCP.
Out Profile Dscp Value	Sets the out-of-profile DSCP value.
User Priority	Sets the user priority.
ToS Precedence	Enables or disables TOS precedence.

Step 7.3: Deploy VMAP Configuration

To deploy VMAPs on all VMready switches, in the VMAP Configuration page, click **Deploy**. This launches the confirmation dialog for deploying the configuration. If you click **Yes**, it initiates configuration of VMAPs on all the VMready switches of that VMready configuration.

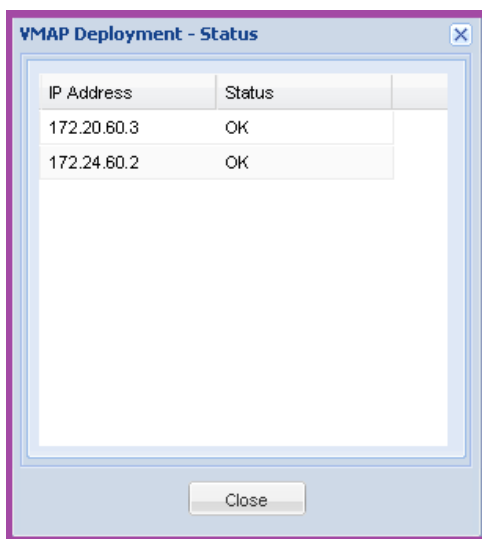
Note 1: Only those VMAPs that have their “Deployed” status set to not yet are deployed/configured.

Note 2: If a VMready switch is newly added, all the VMAPs are configured, regardless of their “Deployed on the Switch” setting.

Note 3: The messages associated with this deployment operation are logged in VMAP logs available from **Logs > VMready Deployment > VMready Across the DataCenter > VMAP Log**.

While the deployment operation is in progress, the wizard displays a progress bar and a log window of the deployment messages. After deployment is completed, a dialog appears that indicates the status of deployment (Ok, Failed, Device down) on each of the VMready switches. See [Figure 76 on page 644](#).

Figure 76 VMAP Deployment Status



Step 8: Configure Server Ports

Note: This is an optional step intended for RackSwitches.

This page lists RackSwitches that are selected for the VMready configuration. It allows you to view and configure the Server Ports for the listed RackSwitches. See [Figure 74 on page 640](#).

Figure 77 VMready Across the Datacenter—Configure Server Ports

VMready Across Datacenter

Steps

Step 8 of 12

1. Introduction
2. Select VMready Switches
3. Define VM Management Server
4. Select Hypervisors
5. Configure VM Groups
6. Configure Virtual Machines
7. Configure VMAPs
- 8. Configure Server Ports**
9. Configure Switch Specific Settings
10. Configure Port Groups
11. vSwitch - Port Group Association
12. Review and Deploy Configuration

Configure Server Ports.

Product Type	IP Address	Health Status	Server Ports	Details
<input type="checkbox"/> BNT RackSwitch G8124	192.168.6.90	Up		View Details
<input type="checkbox"/> BNT RackSwitch G8052	172.16.2.92	Up	Port1-Port3;Port6-Port7;Port10	View Details
<input type="checkbox"/> BNT RackSwitch G8264	172.16.2.91	Down		View Details

Close Help < Prev Next >

Table 350 Configure Server Ports field descriptions

Field	Description
Product Type	Displays the product description.
IP Address	IP address of the VMready switch.
Health Status	Health Status (Up, Non-Critical, Critical, or Down, depending on global health status of the switch).
Server Ports	Displays a list of configured server ports.
Details	Click View Details to display the list of configured server ports in a pop-up window.

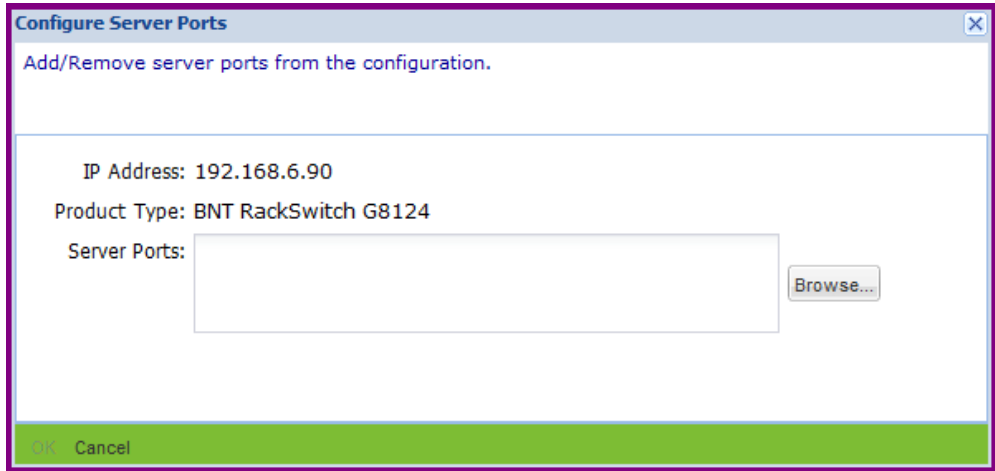
This step provides the following primary options:

Button	Description
Configure	Opens a window for configuring server ports for the selected RackSwitch.
Close	Closes the window. This action also gives an option for the user to keep or discard (delete) the undeployed configuration (XML).
Help	Opens the online Help page.
Next	Moves to the next step or page in the configuration.
Prev	Moves to the previous step or page in the configuration.

Step 8.1: Configuring Server Ports

To configure the server ports for the selected switch, click **Configure**. This action launches a window that allows you to add or remove the server ports. See [Figure 78 on page 647](#).

Figure 78 Configure Server Ports window



Note: Click **Browse...** to launch the port selection window, which lists the configured ports and the available ports. By check-boxing the rows, the selected entries can be added or removed.

Step 9: Configure Switch-Specific Settings

This step provides an option to configure settings such as Ports, LACP admin key, Trunk ID, and VMAPs on the VMready switches. See [Figure 79 on page 648](#).

Note: This step is optional. Click **Next** to skip this step.

Figure 79 VMready Across the Datacenter—Configure Switch-Specific Settings

VMready Across the Datacenter

Steps

Step 9 of 12

1. Introduction
2. Select VMready Switches
3. Define VM Management Server
4. Select Hypervisors
5. Configure VM Groups
6. Configure Virtual Machines
7. Configure VMAPs
8. Configure Server Ports
- 9. Configure Switch Specific Settings**
10. Configure Port Groups
11. vSwitch - Port Group Association
12. Review and Deploy Configuration

Configure switch specific settings for VM Groups that are part of this VMready configuration.

Switch Specific Settings

VM Group: 1

	Product Type	IP Address	Health Status	Ports	LACP Adminkey	TrunkID	VMAP for		
							Server Ports	Non-Server Ports	All Ports
<input type="checkbox"/>	BNT 10-port 10G	192.168.6.81	Up						
<input type="checkbox"/>	BNT 10-port 10G	192.168.6.82	Up						
<input type="checkbox"/>	BNT 10-port 10G	192.168.6.83	Up	INT14-MGT2	17-18				
<input type="checkbox"/>	BNT 10-port 10G	192.168.6.84	Up						
<input type="checkbox"/>	BNT RackSwitch	192.168.6.90	Up						
<input type="checkbox"/>	BNT RackSwitch	172.16.2.92	Up						
<input type="checkbox"/>	BNT RackSwitch	172.16.2.91	Down						
<input type="checkbox"/>	BNT/Nortel 1/10G	192.168.6.75	Up						

Close Help < Prev Next >

Table 351 Configure Switch-Specific Settings field descriptions

Field	Description
VM Group	VM Group drop-down list that displays the configured VM Groups. Selecting a VM Group shows the switch parameters that are specifically configured for that VM Group. Note: This field is not part of the table, but is available above the table.
Product Type	Switch type (for example, HP 1:10Gb Ethernet BL-c Switch).
IP Address	IP address of the VMready switch.
Health Status	Switch Health Status (Up or Down, depending on whether the switch is reachable or not).
Ports	The configured ports for that VM Group in a CSV format. An empty list indicates no configuration is present.

Table 351 Configure Switch-Specific Settings field descriptions

Field	Description
LACP Adminkey	The configured LACP admin key for that VM Group in CSV format. An empty list indicates no configuration is present.
Trunk ID	The configured Trunk IDs for the VM Group, in CSV format. An empty list indicates no configuration is present.
	VMAPs for
Server Ports	The configured VMAPs for Server (internal or downlink) ports.
Non-Server Ports	The configured VMAPs for Non-Server (external or uplink) ports.
All Ports	The configured VMAPs for Server and Non-Server ports.

This step provides the following primary options:

Button	Description
Modify/View	Opens a child window enabling the user to see or edit the switch specific settings. Note: This button is enabled only when a row is selected.
Close	Closes the window. This action also gives an option for the user to keep or discard (delete) the undeployed configuration (XML).
Help	Opens the online Help page.
Next	Moves to the next step or page in the configuration.
Prev	Moves to the previous step or page in the configuration.

Step 9.1: Modifying Switch-Specific Settings

To configure VMready switch specific settings for a VMready switch, first select VM Group and a VMready switch entry, then click **Modify** on the Switch Specific Settings page (step 7). This action launches a child window that allows you to edit the parameters. See [Figure 80 on page 650](#).

Figure 80 Modify VMready Switch-Specific Settings

Modify VMready Switch Specific Settings

Modify the settings such as Ports, LACP Adminkey, Trunk ID and VMAPs of the VMready switch

IP Address: 172.24.60.2

Product Type: BNT/Nortel 1/10Gb Uplink Ethernet Switch Module

VM Group#: 1

Ports: 1 : INT1-1 : INT2; 2 : INT1-2 : INT2 Browse...

LACP Adminkey: 17-19 Browse...

TrunkID: Browse...

VMAPs assigned to Ports

Server Ports: Browse...

Non-Server Ports: Browse...

All Ports: Browse...

OK Cancel

Step 10: Configure Port Groups

If VM Management Server is configured, when you click **Next** in the VMready Switch Specific Settings page, the Port Group Configuration screen is displayed. See [Figure 81 on page 651](#).

Note: If VM Management Server is not configured in step 3, the wizard skips this step.

Figure 81 VMready Across the Datacenter—Configure Port Groups

VMready Across the Datacenter

Steps

Step 10 of 12

1. Introduction
2. Select VMready Switches
3. Define VM Management Server
4. Select Hypervisors
5. Configure VM Groups
6. Configure Virtual Machines
7. Configure VMAPs
8. Configure Server Ports
9. Configure Switch Specific Settings
- 10. Configure Port Groups**
11. vSwitch - Port Group Association
12. Review and Deploy Configuration

Configure the Port Group settings for each of the VM Groups.

Port Group Listing

	PortGroup	VM Group #	Bandwidth Shaping Parameters		
			Average BW	Burst Size	Peak BW
<input type="checkbox"/>	pg - eng	1	51200	10240	61440
<input type="checkbox"/>	pg - finance	2	20480	10240	30720
<input type="checkbox"/>	pg - admin	3	20480	10240	30720

Close Help < Prev Next >

The Port Group Listing table lists the rows corresponding to each of the configured VM groups along with the associated Port Group. Initially, the Port Group cells are blank.

Note: The **Next** button is enabled only if Port groups are associated to each VM group.

Table 352 Configure Port Groups field descriptions

Field	Description
Port Group	Port Group name.
VM Group #	VM Group associated with the Port Group.
	Bandwidth Shaping Parameters
Average BW	Average bandwidth, in Kilobits per second.
Burst Size	Maximum burst size, in Kilobytes.
Peak BW	Peak bandwidth, in Kilobits per second.

This step provides the following options:

Button	Description
Close	Closes the window. This action also gives an option for the user to keep or discard (delete) the undeployed configuration (XML).
Help	Opens the online Help page.
Next	Moves to the next step or page in the configuration. Note that the Next button is disabled until you associate Port groups to each VM group.
Prev	Moves to the previous step or page in the configuration.

Step 10.1: Modify Port Group Settings

To configure Port Group settings for a VM Group, click **Modify** on the Port Groups page. This action launches a child window that allows you to edit the parameters. See [Figure 82 on page 653](#).

Figure 82 Configure Port Group

Configure Port Group

Configure the Port Group settings such as Name, VM Group and Bandwidth Shaping parameters.
Note that you are only allowed to change a blank Port Group name.

PortGroup:

VM Group #: 1

Bandwidth Shaping Parameters

Average BandWidth (kpbs):

Burst Size (KB):

Peak BandWidth (kpbs):

OK Cancel

Step 11: Associate Port Group to a vSwitch

This step allows you to configure Port Groups (defined in step 9) onto one vSwitch on each hypervisor (defined in step 4).

Note: If VM Management Server is not configured in step 3, the wizard skips this step.

Click **Next** in Port Groups to display the screen showing per Hypervisor based vSwitch association for each Port Group. Initially, the vSwitch column shows none, but you can assign a vSwitch using the drop-down list on double click. See [Figure 83 on page 655](#).

Figure 83 VMready Across the Datacenter—vSwitch - Port Group Association

VMready Across Datacenter

Steps

Step 11 of 12

1. Introduction
2. Select VMready Switches
3. Define VM Management Server
4. Select Hypervisors
5. Configure VM Groups
6. Configure Virtual Machines
7. Configure VMAPs
8. Configure Server Ports
9. Configure Switch Specific Settings
10. Configure Port Groups
- 11. vSwitch - Port Group Association**
12. Review and Deploy Configuration

Configure every Port Group defined as part of this VMready configuration onto one vSwitch in each hypervisor. Note that you are allowed to change Port Group name only once.

vSwitch - Port Group Association

PortGroup	vSwitch
[-] Hypervisor: 172.25.110.3,c0a52aca-4066-b601-d7e0-001a64cf36fe	
pg - eng	vSwitch0
pg - finance	vSwitch0
pg - admin	vSwitch0
[-] Hypervisor: 172.25.110.6,acd731b3-5164-30fc-971b-896826b78626	
pg - eng	vSwitch0
pg - finance	vSwitch0
pg - admin	vSwitch0
[-] Hypervisor: 172.25.110.7,65415825-8a16-3ca1-bc72-46a5d7200369	
pg - eng	vSwitch0
pg - finance	vSwitch0
pg - admin	vSwitch0

Close Help < Prev Next >

Table 353 vSwitch - Port Group Association field descriptions

Field	Description
Hypervisor	Hypervisor displayed in the following format: Hypervisor: <Name>, <UUID> Note: Hypervisor cell spans each entire row. Each Hypervisor row lists the Port Groups and the vSwitch of the Hypervisor with which it is associated.
Port Group	Port Group. For each Hypervisor, each Port Group configured is shown in a separate row.
vSwitch	vSwitch of the Hypervisor with which the Port Group is associated. This field contains a drop-down list, which lists all the vSwitches of that Hypervisor along with an additional 'none' option.

Note: Each Hypervisor added to the configuration is shown in a separate row. Below each Hypervisor row are the rows for each configured Port Group and the associated vSwitch. The Hypervisor row contains a button that can be used for hiding or showing the Port Group and vSwitch rows associated with that Hypervisor. The **Next** button is enabled only when every Port Group is associated with a Hypervisor vSwitch.

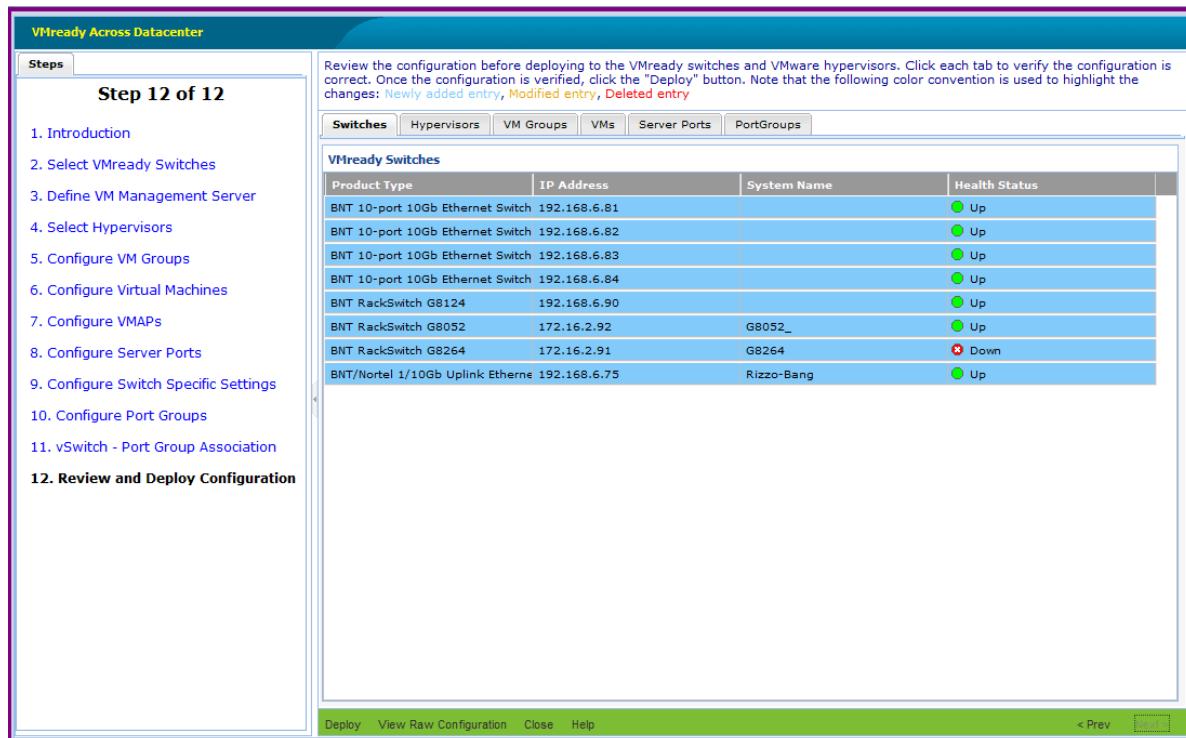
This step provides the following options:

Button	Description
Close	Closes the window. This action also gives an option for the user to keep or discard (delete) the undeployed configuration (XML).
Help	Opens the online Help page.
Next	Moves to the next step or page in the configuration. Note that the Next button is disabled until you associate Port groups with a vSwitch.
Prev	Moves to the previous step or page in the configuration.

Step 12: Review and Deploy the Configuration

This step allows you to review the configuration. The reviewing page is a multi-tabbed pane and some of the tabs are present or absent depending on whether VM Management Server is configured. See [Figure 84 on page 657](#).

Figure 84 VMready Across the Datacenter—Review Configuration



The following table provides a summary of the Review tabs.

Table 354 VMready Review tab descriptions

Tab	Description
Switches	Lists the configured VMready switches.
Hypervisors	Lists the configured Hypervisors. Note: This tab is present only when the VM Management Server is configured.
VM Groups	Lists the configured VMready switches and the VM Group specific Switch Settings.
VMs	Lists the configured Virtual Machines.

Table 354 VMready Review tab descriptions

Tab	Description
Server Ports	Lists the configured Server Ports for the RackSwitches.
Port Groups	Lists the configured Port Groups and the vSwitch – Port Group association.

Step 12.1: Deploying the VMready Configuration

Once you have reviewed the configurations, click **Deploy** to display a confirmation dialog. Click **Ok** to initiate the deployment of the VMready configuration to the switches.

When you click **Ok**, the content frame displays a summary of the deployment across the configured VMready switches and Hypervisors (if VM Management Server is configured). See [Figure 85 on page 659](#).

A log window shows the messages logged during deployment. You can view the logs at any time, as explained in [“How to View Logs” on page 134](#).

Figure 85 VMready Across the Datacenter—Deployment Summary

VMready Across Datacenter

Steps

Step 12 of 12

1. Introduction
2. Select VMready Switches
3. Define VM Management Server
4. Select Hypervisors
5. Configure VM Groups
6. Configure Virtual Machines
7. Configure VMAPs
8. Configure Server Ports
9. Configure Switch Specific Settings
10. Configure Port Groups
11. vSwitch - Port Group Association
- 12. Review and Deploy Configuration**

Review the configuration before deploying to the VMready switches and VMware hypervisors. Click each tab to verify the configuration is correct. Once the configuration is verified, click the "Deploy" button. Note that the following color convention is used to highlight the changes: Newly added entry, Modified entry, Deleted entry

Deployment Summary

VMready Switches - Deployment Summary

IP Address	Product Type	Deployment Status
192.168.6.81	BNT 10-port 10Gb Ethernet Switch Module	OK
192.168.6.82	BNT 10-port 10Gb Ethernet Switch Module	FAILED
192.168.6.83	BNT 10-port 10Gb Ethernet Switch Module	In Progress
192.168.6.84	BNT 10-port 10Gb Ethernet Switch Module	Queued
192.168.6.90	BNT RackSwitch G8124	Queued
172.16.2.92	BNT RackSwitch G8052	Queued
172.16.2.91	BNT RackSwitch G8264	Queued
192.168.6.75	BNT/Nortel 1/10Gb Uplink Ethernet Switch Mod	Queued

Hypervisors - Deployment Summary

Hypervisor	IP Address	Deployment Status
fdcd731b3-5164-30fc-971b-896826b78626	172.25.110.6	OK
65415825-8a16-3ca1-bc72-46a5d7200369	172.25.110.7	In Progress
c0a52aca-4066-b601-d7e0-001a64cf36fe	172.25.110.3	Queued

Cancel Help

Centralized VSI Database

Some IBM BLADE Switches, such as the *Virtual Fabric 10Gb Switch Module for IBM BladeCenter*, support the *pull* model for deploying 802.1Qbg configuration. The pull model enables those switches to get (or pull) the network configuration such as Virtual Switch Instance (VSI) type and 802.1Qbg parameters from a centralized repository using RESTfulAPI, whenever the switches detects new VMs added to Hypervisors connected to them.

You can configure System Networking Switch Center (SNSC) to host centralized VSI database repository, which exposes VSI DB resources through a RESTful API. The following topics describe the centralized VSI database:

- [“VSI Database Overview” on page 662](#)
- [“How to Configure VSI DB from the VSI DB Console” on page 663](#)
- [“How to Administer VSI Database Using RESTful APIs” on page 669](#)

VSI Database Overview

Figure 86 illustrates how System Networking Switch Center can serve as the centralized VSI database repository.

Figure 86 VSI database

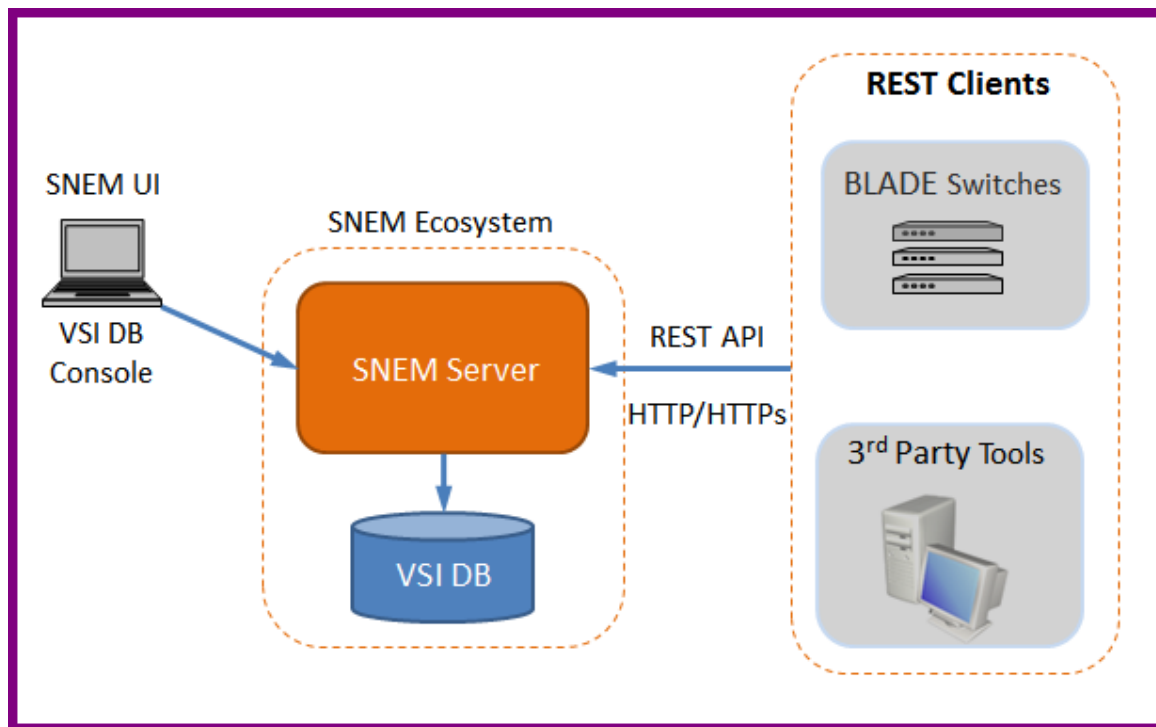


Figure 86 shows the VSI database structure, as follows:

- System Networking Switch Center Server hosts the VSI database.
- You can configure VSI database by launching VSI DB Console from System Networking Switch Center UI as an administrative privileged user. The VSI DB Console allows you to create, modify or delete VSI Type and 802.1Qbg specific parameters.
- You can also configure VSI database by utilizing RESTful API through any home-grown or 3rd party REST client (Note that System Networking Switch Center is not shipped with any REST clients).
- You can configure those IBM BLADE switches supporting REST clients with System Networking Switch Center address so that they can retrieve VSI Type and 802.1Qbg policies.

How to Configure VSI DB from the VSI DB Console

From the VSI DB Console, you can configure a VSI database using the following steps:

- 1** Create (configure) ACLs.
- 2** Create VSI Type by including ACLs that were created in step 1.

The following sections describe configuring VSI Type and 802.1Qbg parameters in VSI DB from the VSI DB Console:

- [“VSI ACL Configuration” on page 664](#)
- [“VSI Type Configuration” on page 667](#)

VSI ACL Configuration

You can insert, modify or delete ACLs, using the following steps (see [Figure 87](#)):

- 1 Login to System Networking Switch Center as an administrator privileged user.
- 2 Launch VSI DB Console by choosing menu **Virtualization Tools > VSI DB Console**.
- 3 Select ACL tab.

You can add an ACL by clicking **Insert**.

You can click **Modify** or **Delete** on an existing ACL.

Figure 87 VSI DB Console – ACL Configuration

VSI DB Console

ACL | VSI Type

ACL

Index	Filter Action	Priority	Ethernet					IPv4							TCP/UDP							
			Source MAC	Source MAC Mask	Destinat MAC	Destinat MAC Mask	VLAN	Ethernet Type	Ethernet Value	Source IP Address	Source IP Mask	Destinat IP Address	Destinat IP Mask	Protocol	Protocol Value	Type Of Service	Source Port	Source Port Mask	Destinat Port	Destinat Port Mask	Flags	Flags Mask
1	setprio	2	60:EB:6:	FF:FF:FI	60:EB:6:	FF:FF:FI	1	ipv4	0x0800	192.168	255.255	192.168	255.255	tcp	6	1	40000	0xffff	40000	0xffff	0x0	0x3f
2	none		any					any														

ACL - Insert Form

General Settings

Index: 3 1..4095

Filter Action: none

Priority: 1..4095

Ethernet

Source MAC:

Source MAC Mask:

Destination MAC:

Destination MAC Mask:

VLAN: 1..4095

Ethernet Type: any

Ethernet Value: 0x0600-0xffff

OK Cancel

Insert | Undo | Redo | Export | Print | Help

Table 355 VSI DB – ACL Configuration field descriptions

Field	Description
Index	The ACL index.
Filter ACTION	Sets the filter action as follows: none, permit, deny, setprio
Priority	Sets the priority in the range 0-7. Note that this field is enabled only when you set the Filter Action to setprio.
Source MAC	Sets the source MAC.
Source MAC Mask	Sets the source MAC mask.
Destination MAC	Sets the destination MAC.
Destination MAC Mask	Sets the destination MAC mask.
VLAN	Sets the VLAN number.
Ethernet Type	Sets the Ethernet type as follows: any, arp, ipv4, ipv6, mpls, rarp, user-defined

Table 355 VSI DB – ACL Configuration field descriptions

Field	Description
Ethernet Value	Sets the Ethernet value in the range 0x0600-0xffff. Note that this field can be used if you set the Ethernet Type to <code>user-defined</code> .
Source IP Address	Sets the source IP address.
Source IP Mask	Sets the source IP mask.
Destination IP Address	Sets the destination IP address.
Destination IP Mask	Sets the destination IP mask.
Protocol	Sets the protocol type as follows: <code>any</code> , <code>tcp</code> , <code>udp</code> , <code>user-defined</code>
Protocol Value	Sets the protocol value in the range 1-255. Note that this field can be used if you set the Protocol to <code>user-defined</code> .
Type of Service	Sets the type of service in the range 0-255.
Source Port	Sets the source port in the range 1-65535.
Source Port Mask	Sets the source port mask in the range 0x0000-0xffff.
Destination Port	Sets the destination port in the range 1-65535.
Destination Port Mask	Sets the destination port mask in the range 0x0000-0xffff.
Flags	Sets the TCP flags in the range 0x0-0x3f. Note that this is enabled only when you set the Protocol to <code>tcp</code> .
Flags Mask	Sets the TCP flags mask in the range 0x0-0x3f. Note that this is enabled only when you set the Protocol to <code>tcp</code> .

VSI Type Configuration

You can insert, modify or delete VSI Types, using the following steps (see [Figure 88](#)):

- 1 Login to System Networking Switch Center as an administrator privileged user.
- 2 Launch VSI DB Console by choosing menu **Virtualization Tools > VSI DB Console**.
- 3 Select VSI Type tab.

You can add a VSI Type by clicking **Insert**.

You can click **Modify** or **Delete** on an existing VSI Type.

Figure 88 VSI DB Console – VSI Type Configuration

Index	Version	Manager ID	Name	VLAN(s)	ACL(s)	Transmit Bandwidth		Receive Bandwidth	
						TX Rate	TX Burst Size	RX Rate	RX Burst Size
1	1	1		100		64	64	64	64
2	1	1		2	1	64	32	64	32
3	1	1	Test VSI 2	10,11,40	1,2	64	32	64	32

VSI Type - Insert Form

Index: 4 1..16777215

Version: 1 1..255

Manager ID: 1 1..255

Name: 0..32 characters

VLAN(s): (comma separated)

ACL(s): Browse...

TX Rate: 0 64..10000000 (multiples of 64)

TX Burst Size: 0 32..4096

RX Rate: 0 64..10000000 (multiples of 64)

RX Burst Size: 0 32..4096

OK Cancel

Table 356 VSI DB – VSI Type Configuration field descriptions

Field	Description
Index	VSI Type index (1-16777215).
Version	VSI Type version (1-255).

Table 356 VSI DB – VSI Type Configuration field descriptions

Field	Description
Manager ID	The manager ID (1-255) to which this VSI Type is associated.
Name	The VSI Type name (0-32).
VLAN(s)	The VLANs configured for this VSI Type.
ACL(s)	The ACLs configured for this VSI Type. Click Browse... to launch ACL selection window, which lists the configured ACLs.
TX Rate	Committed transmission rate (64-10000000 kbps). It must be a multiple of 64.
TX Burst Size	Maximum transmission burst size (32-4096 kilobits).
RX Rate	Committed receive rate (64-10000000 kbps). It must be a multiple of 64.
RX Burst Size	Maximum receive burst size (32-4096 kilobits).

How to Administer VSI Database Using RESTful APIs

System Networking Switch Center exposes RESTful APIs that can be used by those IBM BLADE switches supporting 802.1Qbg for deploying VSI Type configuration. You can also use these RESTful APIs to configure VSI DB in System Networking Switch Center.

The following HTTP/HTTPS methods are supported by RESTful APIs:

- GET – For retrieving VSI Types
- POST – For creating new VSI Types
- PUT – For updating an existing VSI Type
- DELETE – For deleting an existing VSI Type

This chapter covers the following topics:

- [“VSI Types RESTful APIs” on page 670](#)
- [“Access Control for RESTful APIs” on page 671](#)
- [“XML Schema for VSI Types” on page 672](#)

VSI Types RESTful APIs

The following table provides the brief description of various RESTful APIs supported by System Networking Switch Center:

Table 357 RESTful APIs Supported by System Networking Switch Center

Resource URI	HTTP Method	Supported Protocol	Description
/vsitypes/	GET	HTTP, HTTPS	Returns a list of VSI Types associated with different versions.
/vsitypes/{version}/	GET	HTTP, HTTPS	Returns the list of VSI Types associated with the specified {version}.
/vsitypes/{version}/{id}	GET	HTTP, HTTPS	Returns the VSI Type created for {version} having the id as {id}.
/vsitypes/{version}/{id}	POST	HTTPS	Creates the VSI Type {id} for the version {version}.
/vsitypes/{version}/{id}	PUT	HTTPS	Modifies the VSI Type {id} created for the version {version}.
/vsitypes/{version}/{id}	DELETE	HTTPS	Deletes the VSI Type {id} created for the version {version}.

Note: The Resource URIs in the above table are listed in relative path. For example, /vsitypes/ maps to:

http://<server>:40080/snsc/rest/vsitypes/

or

https:// <server>:40443/snsc/rest/vsitypes/

Where <server> is the IP address of the system on which System Networking Switch Center is installed.

Access Control for RESTful APIs

The RESTful APIs offered by System Networking Switch Center requires authentication for creation (POST), modification (SET) and deletion (DELETE) methods.

System Networking Switch Center uses Basic HTTP authentication, which requires the RESTful client to send the authentication information in the Authorization request header.

If you send a POST, PUT and DELETE request without proper authentication credential, System Networking Switch Center's RESTful service returns back a 401 response code (the challenge). The following snippet shows the challenge response send by System Networking Switch Center in case of a bad authentication request:

```
HTTP/1.1 401 Authorization Required
Server: HTTPd/1.0
Date: Thu, 14 Jul 2011 12:23:15 GMT
WWW-Authenticate: Basic realm="VSI Types"
```

Note: In addition to authentication, POST, SET and DELETE requests for VSI Types resources should be sent over HTTPs. If you use HTTP for sending POST, SET and DELETE operations, System Networking Switch Center's RESTful service returns the following error:

```
405 Method Not Allowed
```

XML Schema for VSI Types

The following list shows the XML schema associated with RESTfulVSI Type Request and Response:

```
<?xml version="1.0"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="vsi-types">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="vsi-type" minOccurs="0" maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="vsi-type">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="id" type="xs:string" minOccurs="1"
          maxOccurs="1"/>
        <xs:element name="version" type="xs:string" minOccurs="1" maxOccurs="1"/>
        <xs:element name="managerid" type="xs:string" minOccurs="1" maxOccurs="1"/>
        <xs:element name="name" type="xs:string" minOccurs="1" maxOccurs="1"/>
        <xs:element name="vlanid" type="xs:string" minOccurs="1" maxOccurs="unbounded"/>
        <xs:element ref="bandwidth" minOccurs="1" maxOccurs="1"/>
        <xs:element ref="acl" minOccurs="0" maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="bandwidth">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="txrate" minOccurs="1" maxOccurs="1"/>
        <xs:element ref="rxrate" minOccurs="1" maxOccurs="1"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="acl">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="action" type="filterActionType" minOccurs="0"
          maxOccurs="1"/>
        <xs:element name="prio" type="priorityType" minOccurs="0" maxOccurs="1"/>
        <xs:element ref="ethernet" minOccurs="0" maxOccurs="1"/>
        <xs:element ref="ipv4" minOccurs="0" maxOccurs="1"/>
        <xs:element ref="tcpudp" minOccurs="0" maxOccurs="1"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>

```



```

<xs:element name="txrate">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="txcommittedrate" type="xs:string" minOccurs="1"
        maxOccurs="1"/>
      <xs:element name="txburst" type="xs:string" minOccurs="1" maxOccurs="1"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="rxrate">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="rxcommittedrate" type="xs:string" minOccurs="1"
        maxOccurs="1"/>
      <xs:element name="rxburst" type="xs:string" minOccurs="1" maxOccurs="1"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="ethernet">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="smac" type="macAddressType" minOccurs="0" maxOccurs="1"/>
      <xs:element name="smacmask" type="macAddressType" minOccurs="0"
        maxOccurs="1"/>
      <xs:element name="dmac" type="macAddressType" minOccurs="0" maxOccurs="1"/>
      <xs:element name="dmacmask" type="macAddressType" minOccurs="0"
        maxOccurs="1"/>
      <xs:element name="vlan" type="xs:string" minOccurs="0" maxOccurs="1"/>
      <xs:element name="ethtype" type="xs:string" minOccurs="0" maxOccurs="1"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="ipv4">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="sip" type="ipAddressType" minOccurs="0" maxOccurs="1"/>
      <xs:element name="sipmask" type="ipAddressType" minOccurs="0"
        maxOccurs="1"/>
      <xs:element name="dip" type="ipAddressType" minOccurs="0" maxOccurs="1"/>
      <xs:element name="dipmask" type="ipAddressType" minOccurs="0"
        maxOccurs="1"/>
      <xs:element name="ipproto" type="xs:string" minOccurs="0" maxOccurs="1"/>
      <xs:element name="tos" type="xs:string" minOccurs="0" maxOccurs="1"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="tcpudp">
  <xs:complexType>
    <xs:sequence>

```

```

    <xs:element name="sport" type="xs:string" minOccurs="0" maxOccurs="1"/>
    <xs:element name="sportmask" type="xs:string" minOccurs="0" maxOccurs="1"/>
    <xs:element name="dport" type="xs:string" minOccurs="0" maxOccurs="1"/>
    <xs:element name="dportmask" type="xs:string" minOccurs="0" maxOccurs="1"/>
    <xs:element name="flags" type="xs:string" minOccurs="0" maxOccurs="1"/>
    <xs:element name="flagsmask" type="xs:string" minOccurs="0" maxOccurs="1"/>
  </xs:sequence>
</xs:complexType>
</xs:element>

<xs:simpleType name="filterActionType">
  <xs:restriction base="xs:string">
    <xs:pattern value="none|permit|deny|setpriority"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="priorityType">
  <xs:restriction base="xs:string">
    <xs:pattern value="0|1|2|3|4|5|6|7"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="ipAddressType">
  <xs:restriction base="xs:string">
    <xs:pattern value="(( [0-1] )? [0-9] ( [0-9] )? | 2 [0-4] [0-9] | 25 [0-5] ) \. ( ( [0-1] )? [0-9] ( [0-9] )? | 2 [0-4] [0-9] | 25 [0-5] ) \. ( ( [0-1] )? [0-9] ( [0-9] )? | 2 [0-4] [0-9] | 25 [0-5] ) \. ( ( [0-1] )? [0-9] ( [0-9] )? | 2 [0-4] [0-9] | 25 [0-5] ) "/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="macAddressType">
  <xs:restriction base="xs:string">
    <xs:pattern value="[0-9a-fA-F]{2} (: [0-9a-fA-F]{2} ) {5}"/>
  </xs:restriction>
</xs:simpleType>
</xs:schema>

```

VSI Types RESTful API Reference - Examples

The following sections provide usage references for the supported VSI DB RESTful APIs.

- [“GET Request to Retrieve VSI Types Configured with a Specific Version” on page 676](#)
- [“GET Request to Retrieve an Individual VSI Type” on page 679](#)
- [“GET Request to Retrieve All Configured VSI Types” on page 681](#)
- [“POST Request to Create a VSI Type” on page 685](#)
- [“PUT Request to Modify an Existing VSI Type” on page 687](#)
- [“DELETE Request to Delete an Existing VSI Type” on page 688](#)

GET Request to Retrieve VSI Types Configured with a Specific Version

Resource URI	http://<server>:40080/snsc/rest/vsitypes/{version} (for HTTP) https://<server>:40443/snsc/rest/vsitypes/{version} (for HTTPS)
Method	HTTP GET
Supported Protocols	HTTP and HTTPS
Request Body	Not applicable
Returns	<ul style="list-style-type: none"> 202 OK and XML data (if data is available). 404 Not Found (if VSI Types are not available for specified version).

Example:

GET VSI Types configured for version 2 from System Networking Switch Center running on 192.168.1.1

http://192.168.1.1:40080/snsc/rest/vsitypes/2 (for HTTP)
https://192.168.1.1:40443/snsc/rest/vsitypes/2 (for HTTPS)

Response Template:

```
<?xml version="1.0" encoding="UTF-8"?>
<vsi-types>
  <vsi-type>
    <id>10</id>
    <version>2</version>
    <managerid>1</managerid>
    <name>VSI 1</name>
    <vlanid>11</vlanid>
    <vlanid>12</vlanid>
    <vlanid>13</vlanid>
    <vlanid>14</vlanid>
    <bandwidth>
      <txrate>
        <txcommittedrate>64</txcommittedrate>
        <txburst>32</txburst>
      </txrate>
      <rxrate>
        <rxcommittedrate>64</rxcommittedrate>
        <rxburst>32</rxburst>
      </rxrate>
    </bandwidth>
```

```

<acl>
  <action>setpriority</action>
  <prio>1</prio>
  <ethernet>
    <smac>A1:BC:33:44:55:D6</smac>
    <smacmask>ff:ff:ff:ff:ff:ff</smacmask>
    <dmac>A2:DD:33:44:55:E7</dmac>
    <dmacmask>ff:ff:ff:ff:ff:ff</dmacmask>
    <vlan>12</vlan>
    <ethtype>0x0800</ethtype>
  </ethernet>
  <ipv4>
    <sip>192.168.6.1</sip>
    <sipmask>255.255.255.0</sipmask>
    <dip>192.168.6.2</dip>
    <dipmask>255.255.255.0</dipmask>
    <ipproto>6</ipproto>
    <tos>0</tos>
  </ipv4>
  <tcpudp>
    <sport>1</sport>
    <sportmask>0xffff</sportmask>
    <dport>3</dport>
    <dportmask>0xffff</dportmask>
    <flags>0x0</flags>
    <flagsmask>0x1</flagsmask>
  </tcpudp>
</acl>
</vsi-type>
<vsi-type>
  <id>11</id>
  <version>2</version>
  <managerid>1</managerid>
  <name>VSI 1</name>
  <vlanid>20</vlanid>
  <bandwidth>
    <txrate>
      <txcommittedrate>128</txcommittedrate>
      <txburst>32</txburst>
    </txrate>
    <rxrate>

```

```

        <rxcommittedrate>128</rxcommittedrate>
        <rxburst>32</rxburst>
    </rxrate>
</bandwidth>
<acl>
    <action>setpriority</action>
    <prio>1</prio>
    <ethernet>
        <smac>B1:BC:33:44:55:D6</smac>
        <smacmask>ff:ff:ff:ff:ff:ff</smacmask>
        <dmac>B2:DD:33:44:55:E7</dmac>
        <dmacmask>ff:ff:ff:ff:ff:ff</dmacmask>
        <vlan>22</vlan>
        <ethtype>0x0800</ethtype>
    </ethernet>
    <ipv4>
        <sip>192.168.6.1</sip>
        <sipmask>255.255.255.0</sipmask>
        <dip>192.168.6.2</dip>
        <dipmask>255.255.255.0</dipmask>
        <ipproto>6</ipproto>
        <tos>0</tos>
    </ipv4>
    <tcpudp>
        <sport>1</sport>
        <sportmask>0xffff</sportmask>
        <dport>3</dport>
        <dportmask>0xffff</dportmask>
        <flags>0x0</flags>
        <flagsmask>0x1</flagsmask>
    </tcpudp>
</acl>
</vsi-type>
</vsi-types>

```

GET Request to Retrieve an Individual VSI Type

Resource URI	http://<server>:40080/snsc/rest/vsitypes/{version}/{id} (for HTTP) https://<server>:40443/snsc/rest/vsitypes/{version}/{id} (for HTTPS)
Method	HTTP GET
Supported Protocols	HTTP and HTTPS
Request Body	Not applicable
Returns	<ul style="list-style-type: none"> 202 OK and XML data (if data is available). 404 Not Found (if VSI Types are not available for specified version).

Example:

GET an individual VSI Type 2 configured for version 1 from System Networking Switch Center running on 192.168.1.1

http://192.168.1.1:40080/snsc/rest/vsitypes/1/2 (for HTTP)
https://192.168.1.1:40443/snsc/rest/vsitypes/1/2 (for HTTPS)

Response Template:

```
<?xml version="1.0" encoding="UTF-8"?>
<vsi-types>
  <vsi-type>
    <id>2</id>
    <version>1</version>
    <managerid>1</managerid>
    <name>VSI 1</name>
    <vlanid>1</vlanid>
    <vlanid>2</vlanid>
    <vlanid>3</vlanid>
    <vlanid>4</vlanid>
    <bandwidth>
      <txrate>
        <txcommittedrate>64</txcommittedrate>
        <txburst>32</txburst>
      </txrate>
      <rxrate>
        <rxcommittedrate>64</rxcommittedrate>
        <rxburst>32</rxburst>
      </rxrate>
    </bandwidth>
    <acl>
```

```

<action>setpriority</action>
<prio>1</prio>
<ethernet>
  <smac>11:22:33:44:55:66</smac>
  <smacmask>ff:ff:ff:ff:ff:ff</smacmask>
  <dmac>11:22:33:44:55:56</dmac>
  <dmacmask>ff:ff:ff:ff:ff:ff</dmacmask>
  <vlan>2</vlan>
  <ethtype>0x0800</ethtype>
</ethernet>
<ipv4>
  <sip>192.168.6.1</sip>
  <sipmask>255.255.255.0</sipmask>
  <dip>192.168.6.2</dip>
  <dipmask>255.255.255.0</dipmask>
  <ipproto>6</ipproto>
  <tos>0</tos>
</ipv4>
<tcpudp>
  <sport>1</sport>
  <sportmask>0xffff</sportmask>
  <dport>3</dport>
  <dportmask>0xffff</dportmask>
  <flags>0x0</flags>
  <flagsmask>0x1</flagsmask>
</tcpudp>
</acl>
</vsi-type>
</vsi-types>

```


GET Request to Retrieve All Configured VSI Types

Resource URI	http://<server>:40080/snsc/rest/vsitypes (for HTTP) https://<server>:40443/snsc/rest/vsitypes (for HTTPS)
Method	HTTP GET
Supported Protocols	HTTP and HTTPS
Request Body	Not applicable
Returns	<ul style="list-style-type: none"> 202 OK and XML data (if data is available). 404 Not Found (if VSI Types are not available for specified version).

Example:

GET all configured Types from System Networking Switch Center running on 192.168.1.1

http://192.168.1.1:40080/snsc/rest/vsitypes (for HTTP)
https://192.168.1.1:40443/snsc/rest/vsitypes (for HTTPS)

Response Template:

```
<?xml version="1.0" encoding="UTF-8"?>
<vsi-types>
  <vsi-type>
    <id>2</id>
    <version>1</version>
    <managerid>1</managerid>
    <name>VSI 1</name>
    <vlanid>1</vlanid>
    <vlanid>2</vlanid>
    <vlanid>3</vlanid>
    <vlanid>4</vlanid>
    <bandwidth>
      <txrate>
        <txcommittedrate>64</txcommittedrate>
        <txburst>32</txburst>
      </txrate>
      <rxrate>
        <rxcommittedrate>64</rxcommittedrate>
        <rxburst>32</rxburst>
      </rxrate>
    </bandwidth>
    <acl>
```

```

<action>setpriority</action>
<prio>1</prio>
<ethernet>
  <smac>11:22:33:44:55:66</smac>
  <smacmask>ff:ff:ff:ff:ff:ff</smacmask>
  <dmac>11:22:33:44:55:56</dmac>
  <dmacmask>ff:ff:ff:ff:ff:ff</dmacmask>
  <vlan>2</vlan>
  <ethtype>0x0800</ethtype>
</ethernet>
<ipv4>
  <sip>192.168.6.1</sip>
  <sipmask>255.255.255.0</sipmask>
  <dip>192.168.6.2</dip>
  <dipmask>255.255.255.0</dipmask>
  <ipproto>6</ipproto>
  <tos>0</tos>
</ipv4>
<tcpudp>
  <sport>1</sport>
  <sportmask>0xffff</sportmask>
  <dport>3</dport>
  <dportmask>0xffff</dportmask>
  <flags>0x0</flags>
  <flagsmask>0x1</flagsmask>
</tcpudp>
</acl>
</vsi-type>
<vsi-type>
<id>10</id>
<version>2</version>
<managerid>1</managerid>
<name>VSI 1</name>
<vlanid>11</vlanid>
<vlanid>12</vlanid>
<vlanid>13</vlanid>
<vlanid>14</vlanid>
<bandwidth>
  <txrate>
    <txcommittedrate>64</txcommittedrate>
    <txburst>32</txburst>
  
```

```

</txrate>
<rxrate>
  <rxcommittedrate>64</rxcommittedrate>
  <rxburst>32</rxburst>
</rxrate>
</bandwidth>
<acl>
  <action>setpriority</action>
  <prio>1</prio>
  <ethernet>
    <smac>A1:BC:33:44:55:D6</smac>
    <smacmask>ff:ff:ff:ff:ff:ff</smacmask>
    <dmac>A2:DD:33:44:55:E7</dmac>
    <dmacmask>ff:ff:ff:ff:ff:ff</dmacmask>
    <vlan>12</vlan>
    <ethtype>0x0800</ethtype>
  </ethernet>
  <ipv4>
    <sip>192.168.6.1</sip>
    <sipmask>255.255.255.0</sipmask>
    <dip>192.168.6.2</dip>
    <dipmask>255.255.255.0</dipmask>
    <ipproto>6</ipproto>
    <tos>0</tos>
  </ipv4>
  <tcpudp>
    <sport>1</sport>
    <sportmask>0xffff</sportmask>
    <dport>3</dport>
    <dportmask>0xffff</dportmask>
    <flags>0x0</flags>
    <flagsmask>0x1</flagsmask>
  </tcpudp>
</acl>
</vsi-type>
<vsi-type>
  <id>11</id>
  <version>2</version>
  <managerid>1</managerid>
  <name>VSI 1</name>
  <vlanid>20</vlanid>

```

```

    <bandwidth>
      <txrate>
        <txcommittedrate>128</txcommittedrate>
        <txburst>32</txburst>
      </txrate>
      <rxrate>
        <rxcommittedrate>128</rxcommittedrate>
        <rxburst>32</rxburst>
      </rxrate>
    </bandwidth>
  <acl>
    <action>setpriority</action>
    <prio>1</prio>
    <ethernet>
      <smac>B1:BC:33:44:55:D6</smac>
      <smacmask>ff:ff:ff:ff:ff:ff</smacmask>
      <dmac>B2:DD:33:44:55:E7</dmac>
      <dmacmask>ff:ff:ff:ff:ff:ff</dmacmask>
      <vlan>22</vlan>
      <ethtype>0x0800</ethtype>
    </ethernet>
    <ipv4>
      <sip>192.168.6.1</sip>
      <sipmask>255.255.255.0</sipmask>
      <dip>192.168.6.2</dip>
      <dipmask>255.255.255.0</dipmask>
      <ipproto>6</ipproto>
      <tos>0</tos>
    </ipv4>
    <tcpudp>
      <sport>1</sport>
      <sportmask>0xffff</sportmask>
      <dport>3</dport>
      <dportmask>0xffff</dportmask>
      <flags>0x0</flags>
      <flagsmask>0x1</flagsmask>
    </tcpudp>
  </acl>
</vsi-type>
</vsi-types>

```

POST Request to Create a VSI Type

Resource URI	https://<server>:40443/snsc/rest/vsitypes/{version}/{id}
Method	HTTP POST
Supported Protocols	HTTPS
Request Body	XML (see the Request Template below)
Returns	<ul style="list-style-type: none"> • 201 Created & Location (returns header containing the URL of the newly created VSI Type). • 401 Unauthorized (if authentication/authorization fails). • 405 Method Not Supported (if the request is sent over HTTP). • 415 Unsupported Media Type (if incorrect XML configuration is sent).

Example:

Create (POST) VSI Type 2 for version 1 from System Networking Switch Center running on 192.168.1.1

https://192.168.1.1:40443/snsc/rest/vsitypes/1/2

Request Template:

```
<?xml version="1.0" encoding="UTF-8"?>
<vsi-types>
  <vsi-type>
    <id>2</id>
    <version>1</version>
    <managerid>1</managerid>
    <name>VSI 1</name>
    <vlanid>1</vlanid>
    <vlanid>2</vlanid>
    <vlanid>3</vlanid>
    <vlanid>4</vlanid>
    <bandwidth>
      <txrate>
        <txcommittedrate>64</txcommittedrate>
        <txburst>32</txburst>
      </txrate>
      <rxrate>
        <rxcommittedrate>64</rxcommittedrate>
        <rxburst>32</rxburst>
      </rxrate>
    </bandwidth>
  </vsi-type>
</vsi-types>
```

```

<acl>
  <action>setpriority</action>
  <prio>1</prio>
  <ethernet>
    <smac>11:22:33:44:55:66</smac>
    <smacmask>ff:ff:ff:ff:ff:ff</smacmask>
    <dmac>11:22:33:44:55:56</dmac>
    <dmacmask>ff:ff:ff:ff:ff:ff</dmacmask>
    <vlan>2</vlan>
    <ethtype>0x0800</ethtype>
  </ethernet>
  <ipv4>
    <sip>192.168.6.1</sip>
    <sipmask>255.255.255.0</sipmask>
    <dip>192.168.6.2</dip>
    <dipmask>255.255.255.0</dipmask>
    <ipproto>6</ipproto>
    <tos>0</tos>
  </ipv4>
  <tcpudp>
    <sport>1</sport>
    <sportmask>0xffff</sportmask>
    <dport>3</dport>
    <dportmask>0xffff</dportmask>
    <flags>0x0</flags>
    <flagsmask>0x1</flagsmask>
  </tcpudp>
</acl>
</vsi-type>
</vsi-types>

```

PUT Request to Modify an Existing VSI Type

Resource URI	<code>https://<server>:40443/snsc/rest/vsitypes/{version}/{id}</code>
Method	HTTP PUT
Supported Protocols	HTTPS
Request Body	XML (see the Request Template below)
Returns	<ul style="list-style-type: none"> • 201 Created & Location (returns header containing the URL of the newly created VSI Type). • 401 Unauthorized (if authentication/authorization fails). • 404 Not Found (if specified VSI Type is not configured). • 405 Method Not Supported (if the request is sent over HTTP). • 415 Unsupported Media Type (if incorrect XML configuration is sent).

Example:

Update (PUT) few parameters of VSI Type 2 for version 1 in System Networking Switch Center running on 192.168.1.1

`https://192.168.1.1:40443/snsc/rest/vsitypes/1/2`

Request Template:

Note: Only those parameters that need to be modified can be included in XML body.

```
<?xml version="1.0" encoding="UTF-8"?>
<vsi-types>
  <vsi-type>
    <id>2</id>
    <version>1</version>
    <managerid>1</managerid>
    <name>VSI NEW NAME 1</name>
    <bandwidth>
      <txrate>
        <txcommittedrate>128</txcommittedrate>
        <txburst>64</txburst>
      </txrate>
      <rxrate>
        <rxcommittedrate>128</rxcommittedrate>
        <rxburst>64</rxburst>
      </rxrate>
    </bandwidth>
  </vsi-type>
</vsi-types>
```

DELETE Request to Delete an Existing VSI Type

Resource URI	<code>https://<server>:40443/snsc/rest/vsitypes/{version}/{id}</code>
Method	HTTP DELETE
Supported Protocols	HTTPS
Request Body	Not applicable
Returns	<ul style="list-style-type: none">• 204 No Content (if successful, with no content in the response object).• 401 Unauthorized (if authentication/authorization fails).• 404 Not Found (if specified VSI Type is not configured).• 405 Method Not Supported (if the request is sent over HTTP).

Example:

Delete VSI Type 2 for version 1 from System Networking Switch Center running on 192.168.1.1

`https://192.168.1.1:40443/snsc/rest/vsitypes/1/2`

Performing Device-Specific Actions

System Networking Switch Center (SNSC) allows you to perform specific actions per switch including synchronizing the configuration, launching telnet and web interfaces and invoking the global `apply`, `save` and `diff` commands.

The topics in this chapter cover the following main switch configuration features:

- [“Synchronizing the Configuration - Sync Config” on page 690](#)
- [“Global Actions” on page 694](#)
- [“Launching Device Access Utilities” on page 695](#)

Synchronizing the Configuration - Sync Config

The Sync Config feature gives you the option to replicate certain configuration such as VLAN and Port settings from one switch to multiple switches at the same time.

Restrictions:

- You can only copy data to and from switches that have a health status of Up.
- You can only use the Sync Config feature if previously-made configuration changes are saved to switch flash.

To launch Sync Config page:

- 1 Select a switch in the device list (see [Figure 6 on page 63](#)).
- 2 Choose **Device > Sync Config** menu.

The Sync Config page (see [Figure 89 on page 691](#)) consists of two framed windows: the Destination Devices frame (left) and the Content frame (right).

The Destination Devices frame lists the discovered switches with type matching with the selected target switch for which the Sync Config operation can be performed. By default, the destination devices are deselected. The Content frame shows the sub-features in the form of tabs and the corresponding details in a panel along with panel specific menu bar at the bottom.

Figure 89 Sync Config Page

Destination Devices

Tabs

Destination Devices

- 172.31.1.3, BNT-SW-2
- 172.31.1.4, BNT-SW-3
- 172.31.1.5, BNT-SW-4
- 172.31.1.6, BNT-SW-5

VLAN and Ports

VLAN	Name	Ports	State	STG
1	Default VLAN	1-23;25-64	enabled	1
2	VM Group 100 (T)	2	enabled	1
200	VLAN 200		enabled	1
300	VLAN 300		enabled	1
400	VLAN 400		enabled	1
1000	VLAN 1000	5-6;24	enabled	1
4095	Mgmt VLAN	65	enabled	128

Synchronize Refresh New Log Help Note: Select destination devices and click Synchronize

Panel Menu Bar

This section covers the following Sync Config topics:

- [“VLAN and Port Synchronization” on page 692](#)

VLAN and Port Synchronization

You can synchronize the following parameters from the selected source switch to the chosen set of destination switches:

- VLAN tag state
- VLAN table
- Default VLAN
- Management VLAN
- PVID

Restrictions:

- You can only synchronize data to and from switches that have a health status of Up and are of the same type.
- This operation will not be attempted on switches if previously-made configuration changes are not yet saved to switch flash. That is, it will not synchronize the configuration to switches that are in the “save pending” state.
- This feature is not supported on stacked switches.

Notes:

- If Sync operation fails on a device, System Networking Switch Center reverts any Sync Config changes done on that device.
- Since Sync Config changes the VLAN and Port information on target switches, there are chances of upsetting the network configuration, if the target switch is in live network. So, care should be taken. Having said so, Sync Config is best suited for those switches having factory default configuration.

You can launch VLAN and Port Synchronization page using the below steps:

- 1 Select the switch that has the VLAN and Port configuration that you want to replicate on other devices.
- 2 Choose menu **Device > Sync Config** and click VLAN and Ports feature.
- 3 From the Select Devices list, select/deselect the switches in the Select Devices list.
- 4 Click **Synchronize**.
- 5 Click **Yes** to confirm that you want to synchronize the devices, or click **No** to cancel synchronization.
- 6 Click **View Log** to see the status of the Sync Config process.

The following table describes the fields of the **VLAN and Ports** synchronization tab.

Table 358 Sync Config VLAN and Ports field descriptions

Field	Description
VLAN	The VLAN Id configured on the source switch
Name	VLAN name
Ports	Ports associated with the VLAN Id
State	Enabled/Disabled state
STG	Associated Spanning Tree Protocol Group

Global Actions

The global actions feature allows you to invoke switch specific global commands. These commands are mainly used for rebooting the switch, applying and saving the changes to the configuration, viewing the diff and reversing the configuration changes.

You can invoke these commands per-switch by using one of the following options:

- Select the switch and choose one of the items in **Device > Actions** menu.
- From the Device Console window, choose one of the items in **Actions** menu.

The following table lists the actions menus and the corresponding actions initiated on the switch:

Table 359 Actions menus

Action	Description
Apply	Applies any changes that you have made to the switch configuration
Save	Saves the current configuration to the flash memory.
Diff Config	Opens a window to display any pending configuration changes
Diff Flash	Opens a window to display any pending configuration changes and the affected configuration stored in flash memory on the switch.
Config Dump	Opens a window to display a dump of the current switch configuration.
Syslog Dump	Opens a window to display the syslogs available on the switch.
Revert	Reverts the switch to the current active configuration. This command is available if you did not apply the new configuration settings.
Revert Apply	Reverts the switch to the current saved configuration. This is available if you applied but did not save the new configuration settings.
Reboot Switch	Reboots the switch by reloads and saving the current RAM memory.
Delete	Deletes the switch entry from SNSC device list. Note: This option is not available in Device Console window.

Launching Device Access Utilities

You can launch access utilities such as CLI interface or Web interface using this facility.

This section covers the following launch topics:

- [“Launching CLI Interface” on page 696](#)
- [“Launching Web Interface” on page 697](#)

Launching CLI Interface

This feature allows you to launch a Telnet or SSH session to the switch. For example, you might use this feature to configure SNMP settings on a switch before you perform the discovery procedure. Before you can use this feature, you must know the administrator password to log in to the switch.

Note: This feature uses the local Telnet/SSH application to launch CLI session to the switch and hence, you must configure the browser appropriately. See [“Configuring Console \(SSH/Telnet Client\) Application” on page 130](#).

- 1 Select a switch.
- 2 Choose menu **Device > Launch > Console**. System Networking Switch Center launches the local application to open up CLI session (Telnet/SSH based).

Launching Web Interface

This feature allows you to launch a web (Browser Based Interface, or BBI) session to the switch. For example, you might use this feature to configure SNMP settings on a switch before you perform the discovery procedure.

- 1 Select a switch.
- 2 Choose menu **Device > Launch > Web > HTTP or Device > Launch > Web > HTTPs** to launch HTTP or HTTPs based Web UI respectively. System Networking Switch Center launches a BBI window in a new browser page (see [Figure 90 on page 697](#)).

Figure 90 BBI window

The screenshot displays the BLADE OS web interface. The top navigation bar includes tabs for CONFIGURE, STATISTICS, and DASHBOARD (which is active). Below the tabs are links for Apply, Save, Revert, Diff, Dump, Show Log, Help, and Logout. A status bar at the top shows the date and time (9 Sep 27 5:05:22), the switch name (N7k-8264), and the user (mgmt: /c/cee/port 9/pfc/pri 3). On the left, a tree view shows the system hierarchy, with 'BNT RackSwitch G8264' selected. The main content area is titled 'Switch Dashboard' and contains a table of switch information.

Switch Name	N7k-8264
Switch Location	
Switch Type	Blade Network Technologies RackSwitch G8264
Switch Up Time	33 days, 18 hours, 58 minutes and 43 seconds.
Last Boot Time	14:12:34 Sun Jul 29, 2000 (reset from console)
Time and date	5:05:40, 9/27/2011
Timezone Location	Americas-USA-PacificTime
Daylight Savings Time Status	enabled
MAC Address	08:17:f4:2d:97:00
IP Address	10.173.145.129
Hardware Revision	0
Switch Serial No	MY2101002X
Hardware Part No	BAC-00017-00
Manufacturing Date	11/03
Software Rev	6.7.2.27 (FLASH image2)
Flash Configuration	FLASH image2, active configuration.
Unit Fans Status	Fans are in Back-To-Front AirFlow, Warning at 75 C and Recover at 90 C
Unit Temperature	Sensor 1: 41.0; Sensor 2: 34.0; Sensor 3: 37.5; Sensor 4: 31.0;
Unit Fans Speed	Fan 1: 8411 RPM (15 PWM); Fan 2: 4671 RPM (15 PWM); Fan 3: 8752 RPM (15 PWM); Fan 4: 4379 RPM (15 PWM); Fan 5: 9152 RPM (15 PWM); Fan 6: 4643 RPM (15 PWM); Fan 7: 9574 RPM (15 PWM); Fan 8: 4615 RPM (15 PWM);

Maintenance

Use the maintenance facility to backup System Networking Switch Center's critical data. You can also take a runtime snap shot that would help the developers to debug issues noticed with System Networking Switch Center (SNSC).

The topics in this chapter cover the following maintenance features:

- [“Taking System Networking Switch Center's Critical Data Backup” on page 700](#)
- [“Restoring the Data from the Critical Data Backup” on page 703](#)
- [“Taking IBM System Networking Switch Center Support Dump” on page 705](#)

Taking System Networking Switch Center's Critical Data Backup

The critical data needed for running System Networking Switch Center spans across the following areas:

- Configuration Files
- Database

Configuration Files:

The configuration files can be further classified in to two groups namely, static data and dynamic data.

- Static Data – The data, which is not changed by System Networking Switch Center during the course of operation. It primarily consists of mapping and rules files.
- Dynamic Data – The data that changes when System Networking Switch Center is in operation.

The configuration files reside in conf directory under *<SNSC INSTALLATION>* location.

Database:

The database stores the user credentials, device data including monitoring and performance parameters. For System Networking Switch Center's day-to-day device administration/monitoring operation, the data stored in the DB is very critical.

The database including purged data resides in database directory under *<SNSC INSTALLATION>* location.

In addition to the above mentioned critical data, the log messages play an important role in finding the status of the operation.

When System Networking Switch Center backs up the critical data, it includes conf, database and logs directories.

The backup operation involves in the following steps:

- [“Setting Backup Directory on IBM System Networking Switch Center Server” on page 701](#)
- [“Initiating Critical Data Backup” on page 702](#)

Setting Backup Directory on IBM System Networking Switch Center Server

System Networking Switch Center stores the back up in the user specified repository/ directory residing or mounted on the system where System Networking Switch Center is installed. You can specify the directory for storing the backup operation using the following steps:

Note: This facility is available only to those users logged in as an administrator (if the Root user is disabled), or to those users who know root password (if the Root user is enabled).

- 1** Choose **Maintenance > Data Backup > Set Data Backup Directory** to launch the window for specifying the backup directory.
- 2** Specify the directory where to save.
- 3** If the Root user is enabled, enter the root password in the Root Password field (this field is not visible if the Root user is disabled).
- 4** Click **Set**.

Initiating Critical Data Backup

Any user can initiate critical data backup provided the backup directory is set. You can initiate critical data backup using the following steps:

- 1 Choose **Maintenance > Data Backup > Take Data Backup** to launch the data backup window. This window shows data backup file path.
- 2 Click **OK**.

System Networking Switch Center uses the standard ZIP format to compress the contents in backup file. The backup file is named as follows:

`SNSC_<version>_<date>_<time>.zip`

Where:

`<version>` is the System Networking Switch Center version in a.b.c.d format.

`<date>` is the date on the System Networking Switch Center server system in `yyyymmdd` format, on which the backup operation was initiated.

`<time>` is the time on the System Networking Switch Center server system in `HHMMSS` format, at which the backup operation was initiated.

For example, if the backup operation is initiated in System Networking Switch Center 5.2.1.0 on 23rd July 2010 at 14:01:43 hours, the backup file is named as:

`SNSC.2.1.0_20100723_140143.zip`

Note: While data backup is in progress, the database-related operations are queued until the backup operation, which might take from few seconds to couple of minutes depending on the database size, is completed.

Restoring the Data from the Critical Data Backup

You can restore the backed up data on any other System Networking Switch Center installation, provided you are restoring the data for same version of System Networking Switch Center:

- [“Restoring the Data for IBM System Networking Switch Center Installed on a Linux System” on page 704](#)

Restoring the Data for IBM System Networking Switch Center Installed on a Linux System

- 1 Log in as root on the Linux system installed with System Networking Switch Center, where you want to restore the data.
- 2 Stop SNSC services by issuing the following command:

```
# /opt/ibm/snsc/bin/shutdown.sh
```
- 3 Change directory to System Networking Switch Center installation directory by issuing the following command:

```
# cd /opt/ibm/snsc
```
- 4 Remove conf, database, and logs folders by issuing the following command:

```
# rm -rf conf database logs
```
- 5 Copy the backup file (ref: 3.1.2.2) to the following directory:

```
/opt/ibm/snsc
```
- 6 Extract the backup file contents by issuing the following command:

```
# j2re/bin/jar xvf <backup file name>
```

For example, if the backup file name is
SNSC_5.2.1.0_20100723_140143.zip, then the command should be as follows:

```
# j2re/bin/jar xvf SNSC_5.2.1.0_20100723_140143.zip
```
- 7 Start SNSC services by issuing the following command:

```
# /opt/ibm/snsc/bin/startup.sh
```


Taking IBM System Networking Switch Center Support Dump

System Networking Switch Center support dump helps debugging the problem associated with configuration files and database. You can take the support dump using the following steps:

- 1 Choose **Maintenance > Data Backup > SNSC Support Dump** to launch the window.
- 2 (Optional) If you wish to include database, check **Include Database**.
- 3 Click **Save**, which brings up the save dialog.
- 4 Select the directory where you want to save the System Networking Switch Center support dump and click **OK**.

The support dump file is named as follows:

`SNSC_SupportDump_<version>_<date>_<time>.zip`

Where:

`<version>` is the System Networking Switch Center version in a.b.c.d format.

`<date>` is the date on the System Networking Switch Center server system in `yyyymmdd` format, on which the backup operation was initiated.

`<time>` is the time on the System Networking Switch Center server system in `HHMMSS` format, at which the backup operation was initiated.

For example, if the support dump is initiated in System Networking Switch Center 6.1.0 on 23rd July 2010 at 14:01:43 hours, the support dump file is named as:

`SNSC_SupportDump_5.2.1.0_20100723_140143.zip`

Manager of Managers

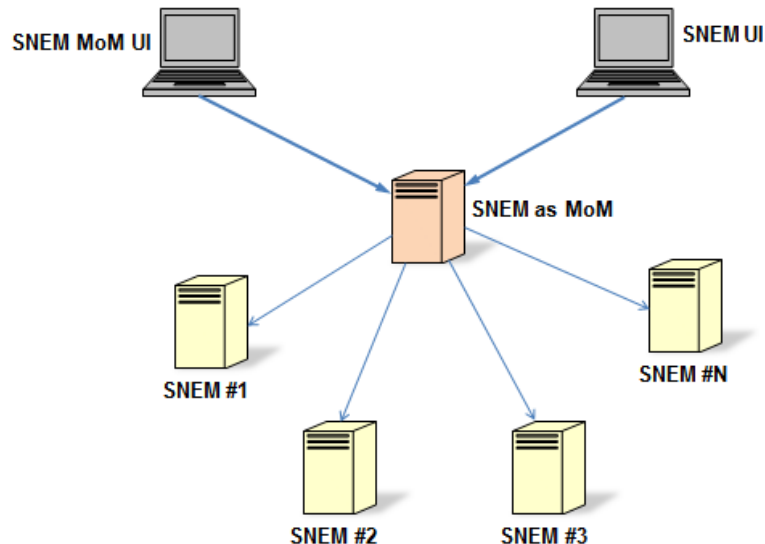
If you plan to deploy multiple instances of System Networking Switch Center (SNSC), such as when managing thousands of devices, you can configure an additional instance of System Networking Switch Center to function as a Manager of Managers (MoM).

- [“Manager of Managers Overview” on page 708](#)
- [“Enabling the Manager of Managers Service” on page 709](#)
- [“Logging In to the Manager of Managers” on page 710](#)
- [“About Manager of Managers Windows and Panels” on page 711](#)
- [“Performing Actions in the Manager of Managers” on page 716](#)

Manager of Managers Overview

Figure 91 on page 708 illustrates how System Networking Switch Center can serve as Manager of Managers (MoM),

Figure 91 IBM System Networking Switch Center as MoM



As seen in the overview picture:

- One of the System Networking Switch Center instances is configured to support MoM functionality.
- The System Networking Switch Center enabled with MoM collects selected attributes from all the devices discovered in other instances of System Networking Switch Center (SNSC #1 through SNSC #N).
- The System Networking Switch Center MoM consolidates the collected information, which can be viewed using a separate user interface (SNSC MoM UI).
- The System Networking Switch Center instance with MoM enabled on it also serves, in parallel, as a regular System Networking Switch Center. This functionality can be accessed using the regular System Networking Switch Center UI.

Enabling the Manager of Managers Service

By default, the Manager of Managers (MoM) service is disabled. You can enable this service on any one instance using the following steps:

1 Stop SNSC Service:

On a Linux system, issue the following command:

```
# /opt/ibm/snsc/bin/shutdown.sh
```

2 Navigate to the following directory:

```
<SNSC INSTALLATION DIR>/conf
```

3 Open the following file in a text editor: `server_conf.properties`

4 Set `enable_mom_service` to `true`.

5 By default, System Networking Switch Center MoM collects the data from other configured instances once every five minutes. You can change this value using setting `mom_server_polling_interval`.

6 Start SNSC Service:

On a Linux system, issue the following command:

```
# /opt/ibm/snsc/bin/startup.sh
```

Logging In to the Manager of Managers

You can login to Manager of Managers (MoM) UI using the following steps:

- 1 Launch a browser and enter the following URL:

If you want to use HTTP, the URL is `http://<hostname>:40080/snscmom`

If you prefer secure HTTP (HTTPS), the URL is `https://<hostname>:40443/snscmom`

- 2 Use the same credentials that you use for logging in to System Networking Switch Center to gain access to MoM features.

About Manager of Managers Windows and Panels

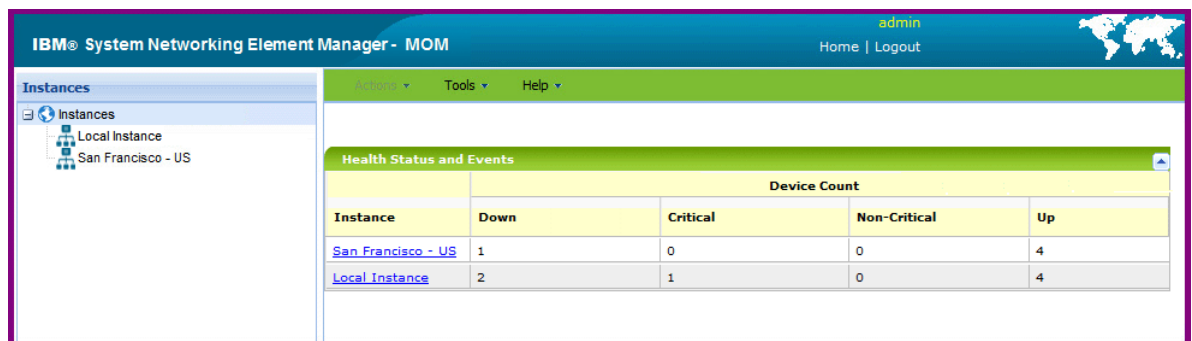
The following material describes the various Manager of Managers (MoM) user interface panels.

Main Window

Once you successfully login to the MoM, you will be presented with the Main Window (see [Figure 92 on page 712](#)).

The Main Window lists configured instances in the navigation panel on the left side of the window. The main content pane shows the health status summary associated with the configured instances. This health status summary is equivalent to Summary Status window shown in that instance of System Networking Switch Center (see [“The Summary Status Pane” on page 73](#)).

Figure 92 MoM Main Window



Note: You can navigate back to the Main Window from the rest of the windows by clicking the **Instances** node in the Instances navigation tree.

Instance View Window

From the Main Window, you can open the Instance View window (see [Figure 93 on page 713](#)) using one of the following steps:

- Click on any System Networking Switch Center instance in the navigation tree (Instances), or
- Click any Instance link in Health Status table view.

Figure 93 MoM Instance View Window

IBM® System Networking Element Manager - MOM

admin Home | Logout

Instances

Local Instance

ENG

NCMS

HR

Non-BNT Devices

Summary Status

Health

Down 2

Critical 0

Non-Critical 0

Up 50

List Device(s): All Go To:

Local Instance

Product Name	IP Address	System Name	Health Status	Save Pending	Running Software Version
Root (28 devices)					
BNT RackSwitch G8000	192.168.131.111		Down	noSaveNeeded	5.2.0.1
BNT RackSwitch G8124	192.168.132.111		Down	noSaveNeeded	5.0.1.0
BNT RackSwitch G8100	192.168.130.11		Up	saveSuccessful	1.0.7.0
BNT RackSwitch G8100	192.168.130.21		Up	saveSuccessful	1.0.7.0
BNT RackSwitch G8000	192.168.130.91		Up	noSaveNeeded	1.1.1.0
BNT RackSwitch G8000	192.168.130.111		Up	noSaveNeeded	1.1.1.0
BNT RackSwitch G8000	192.168.131.11		Up	noSaveNeeded	5.1.1.0
BNT RackSwitch G8000	192.168.131.21		Up	noSaveNeeded	5.1.1.0
BNT RackSwitch G8000	192.168.131.91		Up	noSaveNeeded	5.2.0.1
BNT RackSwitch G8000	192.168.131.51		Up	noSaveNeeded	6.3.1.0
BNT RackSwitch G8000	192.168.131.71		Up	noSaveNeeded	6.3.1.0
BNT RackSwitch G8000	192.168.131.61		Up	noSaveNeeded	6.3.1.0
	192.168.131.61		InStack		
	192.168.131.61		InStack		
	192.168.131.61		InStack		
	192.168.131.61		InStack		
	192.168.131.61		InStack		
BNT RackSwitch G8000	192.168.131.81		Up	noSaveNeeded	6.3.1.0
	192.168.131.81		InStack		
	192.168.131.81		InStack		
	192.168.131.81		InStack		

The instance view window shows the following set of panels:

- Instances tree (upper-left panel) showing the nodes/domains configured in that instance of System Networking Switch Center.
- Summary Status (lower-left panel) showing the summary information (similar to what is shown in case of System Networking Switch Center).
- Content pane showing the list of devices discovered in that instance of System Networking Switch Center, along with the brief summary.

Note: Unlike the System Networking Switch Center window, the device list allows you to select only one device at a time.

Summary Panel

From Instance View window, you can launch the summary panel for any listed device (see [Figure 94 on page 714](#)) using one of the following steps:

- Select a device in the content pane and click **Actions > Summary**, OR
- Click the **IP Address** link in device list table.

Figure 94 MoM Summary Panel

Summary	
Name	Value
Instance	Local Instance
Domain	Center-1/MA/Boston
Rack	IBM-Rack2
Chassis	Chassis1
IP Address	192.168.141.1
Health Status	Down
System Description	Nortel 10 Gb ESM
System Name	
Location	
Contact	
System Up Since	0 days, 7 hours, 32 minutes and 41 seconds
MAC address	09:01:08:14:11:0F
Image 1 Software Version	version 1.0.7.0, downloaded 15:20:00 Mon May 26 2008
Image 2 Software Version	version 5.0.0.6, downloaded 17:32:10 Mon May 26 2008
Refresh Export Print Help	

Table 360 MOM Summary field descriptions

Field	Description
Instance	The SNSC instance in which the switch is discovered
Domain	The Domain name in which the switch is listed in the navigation tree.
Rack	The Rack name (in the navigation tree) in which the switch is contained
Chassis	The Chassis name (in the navigation tree) in which the switch is contained
IP Address	The IP address of the switch.
Health Status	Status showing whether the switch is currently up or down.
System Description	Displays the product name of the switch.
System Name	The administrative-assigned name for the switch.
Location	The physical location of the switch.

Table 360 MOM Summary field descriptions

Field	Description
Contact	The switch contact for support
Image1 Software Version	The software version of the image stored in the first image storage area.
Image2 Software Version	The software version of the image stored in the second image storage area.
Boot Version	The software version of the switch boot code.
Running Software Version	The version of the software image that is currently running on the system.
Hardware Serial Number	The hardware serial number of the switch.
Image for Next Reset	The firmware to choose for the next switch reset
Config For Next Reset	The configuration to choose for the next switch reset.
Save Pending	Gives information whether any applied changes are not yet saved to FLASH memory on the switch.
Apply Pending	Displays information whether any changes are not yet applied on the switch.
Module Bay	The module bay in which the switch is installed.
Manufacture Date	Date the device was manufactured.
Panic Dump	Displays panic dump status.
Time and Reason for last boot	Displays information about the last reboot cycle. For example, the reason might be power cycle.

Performing Actions in the Manager of Managers

You can perform various actions through the Manager of Managers (MoM), such as Adding an instance, Deleting or Renaming an existing instance, Launching Switch Version Report, or launching System Networking Switch Center for an instance or a device.

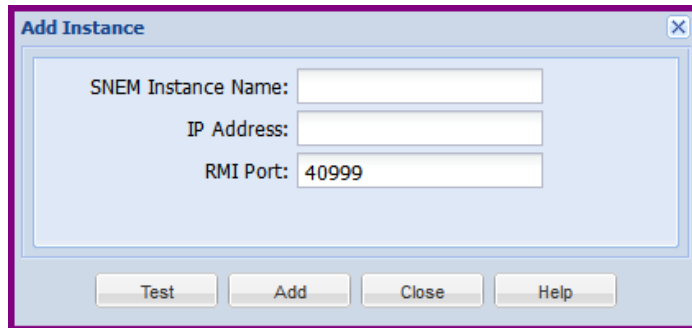
Adding an Instance of IBM System Networking Switch Center

Note: This facility is available only to those users logged in as an administrator (if the Root user is disabled), or to those users who know root password (if the Root user is enabled).

This procedure adds an instance of System Networking Switch Center to the MoM.

- 1 Click **Tools > Add Instance** to launch the window for adding an instance (see [Figure 95 on page 717](#)).
- 2 Enter a unique name for the System Networking Switch Center instance.
- 3 Enter the IP address of the server on which the System Networking Switch Center instance is running.
- 4 If the System Networking Switch Center instance to be added uses a different RMI port, change it accordingly.
- 5 If the Root user is enabled, enter the root password in the Root Password field (this field is not visible if the Root user is disabled).
- 6 (Optional) To verify the IP address and RMI port configuration, click **Test**. When you click the Test button, MoM checks whether the specified instance is accessible.
- 7 Click **Add** to add the instance.

Figure 95 MoM Add Instance Window



The screenshot shows a standard Windows-style dialog box titled "Add Instance". Inside the dialog, there are three text input fields arranged vertically. The first is labeled "SNEM Instance Name:" and is empty. The second is labeled "IP Address:" and is empty. The third is labeled "RMI Port:" and contains the text "40999". Below these fields, there is a horizontal row of four buttons: "Test", "Add", "Close", and "Help". The dialog box has a light blue background and a purple border.

Renaming an Instance of IBM System Networking Switch Center

Note: This facility is available only to those users logged in as an administrator (if the Root user is disabled), or to those users who know root password (if the Root user is enabled).

This procedure renames an existing instance of System Networking Switch Center.

- 1 Navigate to the MoM Main Window.
- 2 Right-click an instance you want to rename, and select **Rename Instance**.
- 3 Enter a new name.
- 4 If the Root user is enabled, enter the root password in the Root Password field (this field is not visible if the Root user is disabled).
- 5 Click **OK**.

Note: Renaming is not allowed for the default Local Instance.

Deleting an Instance of IBM System Networking Switch Center

Note: This facility is available only to those users logged in as an administrator (if the Root user is disabled), or to those users who know root password (if the Root user is enabled).

This procedure deletes an existing instance of System Networking Switch Center.

- 1** Navigate to the MoM Main Window.
- 2** Right-click an instance you want to delete, and select **Delete Instance**
- 3** If the Root user is enabled, enter the root password in the Root Password field (this field is not visible if the Root user is disabled).
- 4** Click **OK**.

Note: Deletion is not allowed for the default Local Instance.

Launching Switch Version Report

The Switch Version Report (see [Figure 96 on page 720](#)) provides a summary of data about all discovered switches across one or more System Networking Switch Center instances that are added in the MoM.

To launch the Switch Version Report showing the summary of data from all the added instances:

- Right-click **Instances** node in Instances tree and select **Switch Version Report**, OR
- Click **Instances** node in Instances tree and select **Tools > Switch Version Report**.

Figure 96 MoM Switch Version Report

Instance	Domain	Rack	Chassis	IP Address	Status	System Description	System Name	Location
Local Instance		IBM-Rack1	Chassis1	192.168.140.1	Down	Nortel Layer 2-3 GbESM		
Local Instance		IBM-Rack1	Chassis2	192.168.140.2	Up	Nortel Layer 2-3 GbESM		
Local Instance		IBM-Rack1	Chassis3	192.168.140.3	Up	Nortel 10 Gb Uplink ESM		
Local Instance		IBM-Rack1	Chassis4	192.168.140.4	Down	Nortel 10 Gb Uplink ESM		
Local Instance		HP-Rack1	Chassis1	192.168.140.5	Down	HP GbE2c/HP GbE2c L2-L3		
Local Instance		HP-Rack1	Chassis2	192.168.140.6	Up	HP GbE2c/HP GbE2c L2-L3		
Local Instance		HP-Rack1	Chassis3	192.168.140.7	Up	HP ProLiant BL p-Class Gb		
Local Instance		HP-Rack1	Chassis4	192.168.140.8	Up	HP ProLiant BL p-Class Gb		
Local Instance		NEC-Rack1	Chassis1	192.168.140.9	Down	NEC 1Gb L2 Switch		
Local Instance		NEC-Rack1	Chassis2	192.168.140.10	Down	NEC 1Gb L2 Switch		
Local Instance		NEC-Rack1	Chassis3	192.168.140.11	Up	NEC 1Gb L3 Switch		
Local Instance		NEC-Rack1	Chassis4	192.168.140.12	Down	NEC 1Gb L3 Switch		
Local Instance				192.168.140.13	Up	BLADE Network Technologi		
Local Instance				192.168.140.14	Down	BLADE Network Technologi		
Local Instance				192.168.140.15	Down	BLADE Network Technologi		
Local Instance				192.168.140.16	Down	BLADE Network Technologi		
Local Instance		IBM-Rack2	Chassis1	192.168.141.1	Down	Nortel 10 Gb ESM		
Local Instance		IBM-Rack2	Chassis2	192.168.141.2	Down	Nortel 10 Gb ESM		
Local Instance		IBM-Rack2	Chassis3	192.168.141.3	Up	Nortel 1/10Gb Uplink Ethe		
Local Instance		IBM-Rack2	Chassis4	192.168.141.4	Down	Nortel 1/10Gb Uplink Ethe		
Local Instance		HP-Rack2	Chassis1	192.168.141.5	Down	HP 1:10 GbE BL-c		
Local Instance		HP-Rack2	Chassis2	192.168.141.6	Down	HP 1:10 GbE BL-c		

Table 361 MOM Switch Version Report field descriptions

Field	Description
Instance	The SNSC instance in which the switch is discovered
Domain	The Domain name in which the switch is listed in the navigation tree.

Table 361 MOM Switch Version Report field descriptions

Field	Description
Rack	The Rack name (in the navigation tree) in which the switch is contained
Chassis	The Chassis name (in the navigation tree) in which the switch is contained
IP Address	The IP address of the switch.
Health Status	Status showing whether the switch is currently up or down.
System Description	Displays the product name of the switch.
System Name	The administrative-assigned name for the switch.
Location	The physical location of the switch.
Contact	The switch contact for support
Image1 Software Version	The software version of the image stored in the first image storage area.
Image2 Software Version	The software version of the image stored in the second image storage area.
Boot Version	The software version of the switch boot code.
Running Software Version	The version of the software image that is currently running on the system.
Hardware Serial Number	The hardware serial number of the switch.
Image for Next Reset	The firmware to choose for the next switch reset
Config For Next Reset	The configuration to choose for the next switch reset.
Save Pending	Gives information whether any applied changes are not yet saved to FLASH memory on the switch.
Apply Pending	Displays information whether any changes are not yet applied on the switch.
Module Bay	The module bay in which the switch is installed.
Manufacture Date	Date the device was manufactured.
Panic Dump	Displays panic dump status.
Time and Reason for last boot	Displays information about the last reboot cycle. For example, the reason might be power cycle.

Launching IBM System Networking Switch Center

You can launch System Networking Switch Center for any instance or for any specific device.

To launch System Networking Switch Center for an instance:

- Right-click an instance in the Instances tree and select **SNSC Launch**, OR
- Select an instance in the Instances tree and click **Tools > SNSC Launch**.

To launch System Networking Switch Center for a specific device:

- 1 Navigate to Instance View Window.
- 2 Select the device for which you wish to launch System Networking Switch Center.
- 3 Click **Tools > SNSC Launch**.

Note: When System Networking Switch Center is launched, it prompts you to login. If System Networking Switch Center is launched for a specific device, after successful login, the Summary page associated with the selected device is displayed.

Using the Command Line Interface

System Networking Switch Center (SNSC) provides a command line interface (CLI), an equivalent to the System Networking Switch Center UI, which user can invoke on the system where System Networking Switch Center is installed.

The CLI can be launched a single command or in a CLI shell that allows you to execute multiple commands. Here is an example of how the CLI shell works:

The CLI session is started by issuing the following command: `snsccli`

The command results in the following user/password prompts:

```
Enter user-id:
Enter password:
```

Once the user-id and password combination is validated, the CLI shell comes into existence. For admin user, the prompt will be displayed as `snsccli#` and for non-admin users, it will be `snsccli>`

You can execute the supported commands such as 'help', which displays the general help listing the supported commands. You can also type-in `<command> help`, which results in the help display for that command. This is more or less similar to DOS Commands on Windows CMD shell.

```
snsccli# help
usage:
device      Displays the device configuration options for SNSC.
firmware    Provides backup/upgrade options.
options     Configures the general configurations on SNSC.
reports     Display the individual reports information.
stats       Display the statistics for the selected option.
info        Display the information table for the selected option.
show        Displays the current configurations on SNSC for the selected
            option.
help        Displays the global help information.
exit        Exits from SNSCCLI session.

snsccli# exit
```

Launching the CLI Shell

You can launch the CLI shell on the system where System Networking Switch Center is installed using the following On a Linux installation:

- From any shell terminal, issue the following command:
`/opt/ibm/snsc/bin/snsccli`

Note: When the CLI shell is launched, the system prompts you to enter username and password to gain access.

Using the CLI for Individual Command Execution

The CLI allows you to execute an individual command if you supply all the required information in one statement. When the CLI completes the operation, it sets the exit status to either 0 or other integer value indicating, respectively, the success or the failure of the operation. For example, you can invoke the CLI in the following way:

<Path to CLI> **-username** *<user>* **-password** *<password>* [**command**]

The above type of invocation results in executing the CLI command outside the shell and setting the exit status. You can check the exit status using the following steps:

On Windows installation, execute the command in CMD shell:

- `echo %ERROR_LEVEL%`

On AIX or Linux installation, execute the following shell command:

- `echo $?`

CLI Command Reference

This entire section provides the usage references for the supported System Networking Switch Center CLI commands.

Restrictions: If the `root` user is disabled, all `options` and `firmware` commands are accessible only to admin privileged users. In case, if the `root` user is enabled, the `options` commands that require the `root` password for execution are available to all users.

options general

Command Syntax and Usage

`options general`

Displays the usage information.

`options general -concurrent_limit [<value>]`

Sets the Concurrent Limit with the given value. If the value is not specified, it displays the current setting and prompts you to enter a new value.

SNSC UI Equivalent: Options > General Properties

`options general -session_timeout [<value>]`

Sets the Session Timeout with the given value. If the value is not specified, it displays the current Session Timeout setting and prompts you to enter a new value.

SNSC UI Equivalent: Options > General Properties

`options general -temp_mode [C|F]`

Sets the temperature sensor display to show the reading in Celsius (C) or Fahrenheit (F).

SNSC UI Equivalent: Options > General Properties

`options general -concurrent_limit <value> - session_timeout <value> - temp_mode [C|F]`

Sets the Concurrent Limit, the Session Timeout, and the Temperature Display Mode parameters.

SNSC UI Equivalent: Options > General Properties

options refresh

Command Syntax and Usage

`options refresh`

Displays the usage information.

`options refresh -time_interval [<value>]`

Sets the Refresh Time Interval with the given value. If the value is not specified, it displays the current Refresh Time Interval setting and prompts you to enter a new value.

SNSC UI Equivalent: Options > Refresh Configuration

options security

Command Syntax and Usage

`options security`

Displays the usage information.

`options security -password [<user>]`

Sets the password of the given user. If the user is not specified, the system prompts you to enter the user name. While setting the password, the system prompts you to type-in admin password to complete the operation.

SNSC UI Equivalent: Options > Security Configuration

Command Syntax and Usage

```
options security mechanism -type [local|radius|tacacs]
    [-admin_pass | -root_pass <value>]
    [-pri_srv <value>]
    [-sec_srv <value>]
    [-pri_sec <value>]
    [-sec_sec <value>]
    [-port <value>]
    [-auth_level <default|alternate>]
    [-timeout <value>]
    [-retries <value>]
```

Sets the authentication mechanism (local, TACACS+ or RADIUS). In case of TACACS+ or RADIUS, it also requires you to specify the values for other parameters such as primary/secondary servers, primary/secondary secrets, and so on.

Notes:

In case of TACACS+ or RADIUS, if other parameters are not supplied in the command input, the system prompts you to specify the following:

- (i) If root user is enabled, then the system prompts for the root password or else, prompts for admin password.
- (ii) Primary and Secondary server addresses
- (iii) Secrets for Primary and Secondary servers
- (iv) Server port
- (v) Authorization Level (only for TACACS+)
- (vi) Timeout to use
- (vii) Number of retries

SNSC UI Equivalent: Options > Authentication Configuration

options purge

Command Syntax and Usage

options purge

Displays the usage information.

options purge -days <value>

Sets the purge type to “days” and sets the number of days with the given value.

SNSC UI Equivalent: Options > DB Data Purge Configuration

options purge -events <value>

Sets the purge type to “events” and sets the events count with the given value.

SNSC UI Equivalent: Options > DB Data Purge Configuration

options logfile

Command Syntax and Usage

options logfile

Displays the usage information.

options logfile -max [<value>]

Sets the maximum number of backup files to use while logging. If the value is not specified, it displays the current setting and prompts you to enter a new value.

SNSC UI Equivalent: Options > Log File Configuration

options logfile -size [<value>]

Sets the maximum size in MB for the log file. If the value is not specified, it displays the current setting and prompts you to enter a new value.

SNSC UI Equivalent: Options > Log File Configuration

options logfile -max <value> -size <value>

Sets the maximum number of backup files and the maximum size in MB for the log file.

SNSC UI Equivalent: Options > Log File Configuration

options data_collection

Command Syntax and Usage

options data_collection

Displays the usage information.

options data_collection -health [<value>]

Sets the polling interval for health check service. If the value is not specified, it displays the current setting and prompts you to enter a new value.

SNSC UI Equivalent: Options > Data Collection Configuration

options data_collection -perf [<value>]

Sets the polling interval for performance statistics collection. If the value is not specified, it displays the current setting and prompts you to enter a new value.

SNSC UI Equivalent: Options > Data Collection Configuration

options data_collection -health <value> **-perf** <value>

Sets the polling interval for health check service and performance statistics collection.

SNSC UI Equivalent: Options > Data Collection Configuration

options cli_conf

Command Syntax and Usage

options cli_conf

Displays the usage information.

options cli_conf -attempts [<value>]

Sets the number of unsuccessful login attempts the CLI session will allow. If the value is not specified, it displays the current setting and prompts for a new value.

options cli_conf -idle [<value>]

Sets the idle session timeout value in minutes. If the value is not specified, it displays the current setting and prompts you to enter a new value.

Command Syntax and Usage

options cli_conf -attempts <value> -idle <value>

Sets the number of unsuccessful login attempts and the idle session timeout value in minutes.

options hpsim

Command Syntax and Usage

options hpsim

Displays the usage information.

Note: This feature might not be available in your software edition. If so, please disregard this information.

options hpsim -write_comm [<value>]

Sets the write community to use with the devices discovered/synchronized by/ from HP SIM. If the value is not specified, it displays the current setting and prompts you to enter a new value.

SNSC UI Equivalent:

Options > HP SIM Connector > Set SNMP Write Community

Command Syntax and Usage

```
options hpsim sync -status {on|off}  
    [-ip <value>]  
    [-user <value>]  
    [-pass <value>]  
    [-poll_intr <value>]  
    [-test]
```

Turns on or turns off the HP SIM sync feature. If the value (on/off) is not specified, it displays the current setting and prompts you to enter a new value.

When the sync feature is set to “on” and if the other parameters are not specified, the command prompts you to specify HP SIM Server IP address, user name and password to access HP SIM and the polling interval in minutes.

You can also specify the `-test` option at the end of the command. The `-test` option directs the system to first validate whether the parameters are correct. The changes are saved only if the parameters are valid, otherwise an error message is displayed.

SNSC UI Equivalent: Options > HP SIM Connector > Configuration

options dial_home

Command Syntax and Usage

options dial_home

Displays the usage information.

Note: This feature might not be available in your software edition. If so, please disregard this information.

options dial_home email_conf

```
[-srv_addr <value>]
[-srv_port <value>]
[-format {Plain-Text|XML}]
[-sender_email <value>]
[-recipient_email <value>]
[-user <value>]
[-pass <value>]
[-conn {No|TLS|SSL}]
[-test]
```

Configures the email parameters to use for generating email alerts. You can also specify the -test option at the end of the command. The -test option directs the system to first validate whether the parameters are correct. The changes are saved only if the parameters are valid, otherwise an error message is displayed.

Note:

If other parameters are not supplied, the system prompts you to specify:

- (i) Email Server Address, Port, User and Password details, connection type
- (ii) Format to use while sending the alerts
- (iii) Sender and Recipient Email Addresses

SNSC UI Equivalent: Options > Dial Home > Email Configuration

Command Syntax and Usage

options dial_home trap_conf

[-dev_type <value>]
[-trap_type <value>]
[-ip <value>]
[-descr <value>]

Configures the trap parameters to use for generating email alerts.

Note:

If other parameters are not supplied, the system prompts you to specify:

- (i) Device type
- (ii) Trap type
- (iii) IP addresses
- (iv) Trap Description

SNSC UI Equivalent: Options > Dial Home > Traps Configuration

options dial_home trap_del

[-dev_type <value>]
[-trap_type <value>]
[-ip <value>]

Deletes the configured Dial Home entry for the specified device type and the trap.

Note:

If other parameters are not supplied, the system prompts you to specify:

- (i) Device type
- (ii) Trap type
- (iii) IP addresses

SNSC UI Equivalent: Options > Dial Home > Traps Configuration

options vm

Command Syntax and Usage

options vm

Displays the usage information.

options vm -poll_int [*<value>*]

Allows you to configure the VM polling interval.

SNSC UI Equivalent:

Options > VM Management Server Connector > Configuration

Command Syntax and Usage

```
options vm add -type [http|https]
    [-port <value>]
    [-ip <value>]
    [-user <value>]
    [-pass <value>]
    [-ssl_cert <value>]
    [-test]
```

Allows you to configure the protocol to use by System Networking Switch Center to communicate with VM Server. You can also specify the `-test` option at the end of the command. The `-test` option directs the system to first validate whether the parameters are correct. The changes are saved only if the parameters are valid, otherwise an error message is displayed.

Note:

If optional parameters are not specified, the system prompts you to specify:

- (i) Protocol to use
- (ii) Port
- (iii) IP Address of the VM Server
- (iv) User name and Password for VM Server
- (v) SSL Certificate

SNSC UI Equivalent:

Options > VM Management Server Connector > Configuration

Command Syntax and Usage

```
options vm del -type [http|https]  
[-port <value>]  
[-ip <value>]  
[-user <value>]
```

Allows you to delete the configured entry used by System Networking Switch Center to communicate with VM Server.

Note:

If optional parameters are not specified, the system prompts you to specify:

- (i) Protocol to use
- (ii) Port
- (iii) IP Address of the VM Server
- (iv) User name and Password for VM Server

SNSC UI Equivalent:

Options > VM Management Server Connector > Configuration

show

Command Syntax and Usage

show

Displays the usage information.

show auth_conf

Displays the current authentication mechanism and its configuration.

SNSC UI Equivalent: Options > Authentication Configuration

show cli_conf

Displays the current CLI configuration.

show data_collection_conf

Displays the current Data collection settings.

SNSC UI Equivalent: Options > Data Collection Configuration

show data_purge_conf

Displays the current data purging settings.

SNSC UI Equivalent: Options > DB Data Purge Configuration

show dial_home -email

Displays the email settings for Dial Home.

Note: This feature might not be available in your software edition. If so, please disregard this information.

SNSC UI Equivalent: Options > Dial Home > Email Configuration

show dial_home -traps

Displays the traps settings for Dial Home.

Note: This feature might not be available in your software edition. If so, please disregard this information.

SNSC UI Equivalent: Options > Dial Home > Traps Configuration

Command Syntax and Usage

show general_conf

Displays the general settings such as concurrent limit and session timeout.

SNSC UI Equivalent: Options > General Properties

show hpsim_conf -hpsim_server

Displays the HP SIM sync configuration.

Note: This feature might not be available in your software edition. If so, please disregard this information.

SNSC UI Equivalent: Options > HP SIM Connector > Configuration

show hpsim_conf -write_comm

Displays the write community to use for devices discovered through HP SIM sync.

Note: This feature might not be available in your software edition. If so, please disregard this information.

SNSC UI Equivalent:

Options > HP SIM Connector > Set SNMP Write Community

show license_info

Displays the license information

SNSC UI Equivalent: Help > About IBM System Networking Switch Center

show logfile_conf

Displays the current log settings

SNSC UI Equivalent: Options > Log File Configuration

show refresh_conf

Displays the current refresh configuration

SNSC UI Equivalent: Options > Refresh Configuration

Command Syntax and Usage

show vm_conf -ssl_cert

Displays the SSL certificate file details used in VM Management Server configuration.

SNSC UI Equivalent:

Options > VM Management Server Connector > Configuration

show vm_conf -vm_server

Displays the VM Management Server configuration details.

SNSC UI Equivalent:

Options > VM Management Server Connector > Configuration

device add

Command Syntax and Usage

device add

Displays the usage information.

```
device add -ip <IP address>
[-version {v1|v2c|v3}]
[-rcomm <value>]
[-wcomm <value>]
[-user <SNMPv3 username>]
[-auth_proto {MD5|SHA1|NONE}]
[-auth_pass <password>]
[-priv_proto {DES|NONE}]
[-priv_pass <password>]
[-root_pass <password>]
```

Discovers the given device, if supported, in System Networking Switch Center.

Notes: If not supplied in the command input, the system prompts you to specify the following:

- (i) The SNMP version to use (v1, v2c or v3)
- (ii) If v1 or v2c is selected, the system prompts for:
 - (a) Read community string
 - (b) Write community string
- (iii) If v3 is specified, the system prompts for:
 - (a) SNMPv3 user name
 - (b) Authentication protocol to use
 - (c) Authentication password (only if Authentication protocol is NOT set to NONE)
 - (d) Privacy protocol to use (only if Authentication protocol is NOT set to NONE)
 - (e) Privacy password (only if Privacy protocol is NOT set to NONE).
- (iv) If root user is enabled, then the system prompts for the root password.

SNSC UI Equivalent:

Right-click any Domain and click **Add Device** or

Options > Discovery > Discovery Configuration > Insert

Command Syntax and Usage

```

device add -range <IP address range>
  [-version {v1|v2c|v3}]
  [-rcomm <value>]
  [-wcomm <value>]
  [-user <SNMPv3 username>]
  [-auth_proto {MD5|SHA1|NONE}]
  [-auth_pass <password>]
  [-priv_proto {DES|NONE}]
  [-priv_pass <password>]
  [-root_pass <password>]

```

Discovers BNT devices in the given IP address range. The IP address range should be specified as <Start IP Address>-<End Octet>. For example, the input 192.168.1.1-20 indicates the range from 192.168.1.1 to 192.168.1.20

Notes:

If not supplied in the command input, the system prompts you to specify the following:

- (i) The SNMP version to use (v1, v2c or v3)
- (ii) If v1 or v2c is selected, the system prompts for:
 - (a) Read community string
 - (b) Write community string
- (iii) If v3 is specified, the system prompts for:
 - (a) SNMPv3 user name
 - (b) Authentication protocol to use
 - (c) Authentication password (only if Authentication protocol is NOT set to NONE)
 - (d) Privacy protocol to use (only if Authentication protocol is NOT set to NONE)
 - (e) Privacy password (only if Privacy protocol is NOT set to NONE).
- (iv) If root user is enabled, then the system prompts for the root password.

SNSC UI Equivalent: Options > Discovery > Discovery Configuration > Insert

device delete

Command Syntax and Usage

device delete

Displays the usage information.

device delete -ip *<IP address>* [**-root_pass** *<password>*]

Deletes the given device, if discovered in System Networking Switch Center.

Note: If the root user is enabled and the password parameter is not supplied within the command, then the system prompts for the root password.

SNSC UI Equivalent:

Device > Actions > Delete

Group Operations > Group Actions > Delete

device delete -range *<IP address range>* [**-root_pass** *<password>*]

Deletes the discovered BNT devices that falls in the given IP address range. The IP address range should be specified as *<Start IP Address>-<End Octet>*. For example, the input *192.168.1.1-20* indicates the range from 192.168.1.1 to 192.168.1.20

Note: If the root user is enabled and the password parameter is not supplied within the command, then the system prompts for the root password.

SNSC UI Equivalent:

Although, there is no range based delete in System Networking Switch Center UI, but this CLI command is more or less similar to selecting multiple devices and deleting them using the folloiwng menu:

Group Operations > Group Actions > Delete

device import

Command Syntax and Usage

device import

Displays the usage information.

```
device import -file <filename>
  [-version {v1 | v2c | v3}]
  [-rcomm <value>]
  [-wcomm <value>]
  [-user <SNMPv3 username>]
  [-auth_proto {MD5 | SHA1 | NONE}]
  [-auth_pass <password>]
  [-priv_proto {DES | NONE}]
  [-priv_pass <password>]
  [-timeout <value>]
  [-retries <value>]
  [-root_pass <password>]
```

Discovers the IP addresses listed in the file provided the given IP address represents a supported device.

Notes: If not supplied in the command input, the system prompts you to specify the following:

- (i) The SNMP version to use (v1, v2c or v3)
- (ii) If v1 or v2c is selected, the system prompts for:
 - (a) Read community string
 - (b) Write community string
- (iii) If v3 is specified, the system prompts for:
 - (a) SNMPv3 user name
 - (b) Authentication protocol to use
 - (c) Authentication password (only if Authentication protocol is NOT set to NONE)
 - (d) Privacy protocol to use (only if Authentication protocol is NOT set to NONE)
 - (e) Privacy password (only if Privacy protocol is NOT set to NONE).
- (iv) If root user is enabled, then the system prompts for the root password.

SNSC UI Equivalent: Options > Discovery > Import Device List

device export

Command Syntax and Usage

device export

Displays the usage information.

device export -file *<filename>*

Exports the discovered devices information to a file.

SNSC UI Equivalent: Options > Discovery > Export Device List

reports event

Command Syntax and Usage

reports event

Displays the usage information.

Note: This feature might not be available in your software edition. If so, please disregard this information.

reports event -snsc *<IP address>*

Displays the System Networking Switch Center alerts associated with the given IP address.

reports event -snsc all

Displays the System Networking Switch Center alerts associated with all the discovered devices.

SNSC UI Equivalent: Reports > SNSC Alerts

reports event -snmp *<IP address>*

Displays the SNMP events received from the given IP address.

SNSC UI Equivalent: {Device Console} > Monitor > Summary > View Events

reports event -snmp all

Displays the SNMP events received from all the discovered devices.

SNSC UI Equivalent: Reports > Event List

Command Syntax and Usage

reports event -syslog *<IP address>*

Displays the Syslog messages received from the given IP address.

SNSC UI Equivalent: {Device Console} > Monitor > Summary > View Syslogs

reports event -syslog all

Displays the Syslog messages received from all the discovered devices.

SNSC UI Equivalent: Reports > Syslog List

reports svr

Command Syntax and Usage

reports svr

Displays the usage information.

reports svr -ip all

Displays the switch version report of all the discovered devices

SNSC UI Equivalent: Reports > Switch Version Report.

reports svr -ip *<IP Address List>*

Displays the switch version report of those switches specified in the IP Address List in comma separated value (CSV) format.

SNSC UI Equivalent: Group Operations > Switch Version Report.

reports vmr

Command Syntax and Usage

reports vmr

Displays the usage information.

reports vmr -datacenter

Displays the VMs retrieved from the VM Data Center.

SNSC UI Equivalent: Reports > VM Data Center Report

reports vmr -group

Displays the VM Groups details associated with Virtual Switch Groups.

SNSC UI Equivalent: Reports > VMready VM Report > VM Groups

reports vmr -ports

Displays the Port Groups details associated with Virtual Switch Groups.

SNSC UI Equivalent: Reports > VMready VM Report > Port Groups

stats acl

Command Syntax and Usage

stats acl

Displays the usage information.

stats acl -acl_stats [*<IP address>*]

Displays the ACL statistics of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Access Control List > ACL Statistics

Command Syntax and Usage

stats acl -port_stats [*<IP address>*]

Displays the ACL Port statistics of the given switch.

Note: If the IP address is not specified, the system prompts you to type-in the IP address.

SNSC UI Equivalent: {Device Console} > Monitor > Access Control List > ACL Port Statistics

stats bridge

Command Syntax and Usage

stats bridge

Displays the usage information.

stats bridge -forwarding [*<IP address>*]

Displays the Bridge Forwarding statistics of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Bridge > Forwarding Statistics

stats port

Command Syntax and Usage

stats port

Displays the usage information.

stats port -8021x [*<IP address>*]

Displays the Port 802.1x statistics of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Port > 802.1x Statistics

stats port -authdiag [*<IP address>*]

Displays the Port Authenticator Diagnostics statistics of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Port > Authenticator Diagnostics Statistics

stats port -bridge [*<IP address>*]

Displays the Port Bridge statistics of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Port > Bridge Statistics

Command Syntax and Usage

stats port -ethernet [*<IP address>*]

Displays the Port Ethernet Error statistics of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Port > Ethernet Error Statistics

stats port -interface [*<IP address>*]

Displays the Port Interface statistics of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Port > Interface Statistics

stats port -ip [*<IP address>*]

Displays the Port IP statistics of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Port > IP Statistics

stats port -lACP [*<IP address>*]

Displays the Port LACP statistics of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Port > LACP Statistics

stats routing

Command Syntax and Usage

stats routing

Displays the usage information.

stats routing -arp [*<IP address>*]

Displays the ARP statistics of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Routing > ARP Statistics

stats routing -dns [*<IP address>*]

Displays the DNS statistics of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Routing > DNS Statistics

stats routing -icmp_in [*<IP address>*]

Displays the ICMP In statistics of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Routing > ICMP In Statistics

stats routing -icmp_out [*<IP address>*]

Displays the ICMP Out statistics of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Routing > ICMP Out Statistics

stats routing -igmp_snoop [*<IP address>*]

Displays the IGMP Snooping statistics of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Routing > IGMP Snooping Statistics

Command Syntax and Usage

stats routing -ip [*<IP address>*]

Displays the IP statistics of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Routing > IP Statistics

stats routing -ip_intf [*<IP address>*]

Displays the IP Interface statistics of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Routing > IP Interface Statistics

stats routing -ospf_area [*<IP address>*]

Displays the OSPF Area statistics of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Routing > OSPF Area Statistics

stats routing -ospf_area_intf [*<IP address>*]

Displays the OSPF Area Interface statistics of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Routing > OSPF Area Interface Statistics

stats routing -ospf_area_intf_rcv_err [*<IP address>*]

Displays the OSPF Area Interface Receive Error statistics of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent:

{Device Console} > Monitor > Routing > OSPF Area Interface Receive Error Statistics

Command Syntax and Usage

stats routing -ospf_area_rcv_err [*<IP address>*]

Displays the OSPF Area Receive Error statistics of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Routing > OSPF Area Receive Error Statistics

stats routing -ospf_gen [*<IP address>*]

Displays the OSPF general statistics of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Routing > OSPF General Statistics

stats routing -ospf_intf_change [*<IP address>*]

Displays the OSPF Interface Change statistics of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Routing > OSPF Interface Change Statistics

stats routing -ospf_intf_neigh [*<IP address>*]

Displays the OSPF Interface Neighbor statistics of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Routing > Interface Neighbor Statistics

stats routing -ospf_intf_trans [*<IP address>*]

Displays the OSPF Interface Transmission statistics of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent:

{Device Console} > Monitor > Routing > OSPF Interface Transmission Statistics

Command Syntax and Usage

stats routing -ospf_neigh [*<IP address>*]

Displays the OSPF Area Neighbor statistics of the given switch.

Note: If the IP address is not specified, the system prompts you to type-in the IP address.

SNSC UI Equivalent: {Device Console} > Monitor > Routing > OSPF Area Neighbor Statistics

stats routing -ripv2 [*<IP address>*]

Displays the RIP v2 statistics of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Routing > RIP V2 Statistics

stats routing -route [*<IP address>*]

Displays the Routes statistics of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Routing > Route Statistics

stats routing -tcp [*<IP address>*]

Displays the TCP statistics of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Routing > TCP Statistics

stats routing -udp [*<IP address>*]

Displays the UDP statistics of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Routing > UDP Statistics

stats switch

Command Syntax and Usage

stats switch

Displays the usage information.

stats switch -mpcpu [*<IP address>*]

Displays the MP CPU statistics of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Switch > MP CPU Statistics

stats switch -ntp [*<IP address>*]

Displays the NTP statistics of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Switch > NTP Statistics

stats switch -packet [*<IP address>*]

Displays the Packet statistics of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Switch > Packet Statistics

stats switch -snmp [*<IP address>*]

Displays the SNMP statistics of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Switch > SNMP Statistics

stats switch -stp [*<IP address>*]

Displays the STP statistics of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Switch > STP Statistics

Command Syntax and Usage

stats switch -ufd [*<IP address>*]

Displays the UFD statistics of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Switch > UFD Statistics

stats virtual_routing

Command Syntax and Usage

stats virtual_routing

Displays the usage information.

stats virtual_routing -virt_stats [*<IP address>*]

Displays the Virtual Routing statistics of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Virtual Routing > Virtual Routing Statistics

info 8021

Command Syntax and Usage

info 8021

Displays the usage information.

info 8021 -cosq [*<IP address>*]

Displays the 802.1x Priority COSq information of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > 802.1x/p > 802.1x Priority COSq

info 8021 -gen [*<IP address>*]

Displays the 802.1x general information of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > 802.1x/p > 802.1x General

info 8021 -port_priority [*<IP address>*]

Displays the 802.1x Port Priority information of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > 802.1x/p > Port Priority

info bridge

Command Syntax and Usage

info bridge

Displays the usage information.

info bridge -base_port [*<IP address>*]

Displays the Base Port information of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Bridge > Base Port Information

Command Syntax and Usage

info bridge -cist_bridge [*<IP address>*]

Displays the CIST Bridge information of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Bridge > CIST Bridge Information

info bridge -cist_port [*<IP address>*]

Displays the CIST Port information of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Bridge > CIST Port Information

info bridge -fdb [*<IP address>*]

Displays the Forwarding Database information of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Bridge > Forwarding Database Information

info bridge -stp [*<IP address>*]

Displays the STP information of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Bridge > STP

info hotlinks

Command Syntax and Usage

info hotlinks

Displays the usage information.

info hotlinks -hl_stats [*<IP address>*]

Displays the Hotlinks statistics of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Hotlinks Statistics > Statistics

info port

Command Syntax and Usage

info port

Displays the usage information.

info port -lACP_aggr [*<IP address>*]

Displays the LACP aggregator information of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Port > LACP Aggregator

info port -lACP_port_aggr [*<IP address>*]

Displays the LACP port aggregator information of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Port > LACP Port Aggregator

info routing

Command Syntax and Usage

info routing

Displays the usage information.

info routing -arp [*<IP address>*]

Displays the ARP information of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Routing > ARP

info routing -bgp_peers [*<IP address>*]

Displays the BGP peers summary information of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Routing > Peers Summary

info routing -bgp_route [*<IP address>*]

Displays the BGP routing table information of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Routing > Routing Table

info routing -gateway [*<IP address>*]

Displays the Gateway information of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Routing > Gateway Information

info routing -igmp [*<IP address>*]

Displays the IGMP information of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Routing > IGMP Information

Command Syntax and Usage

info routing -igmp_multicast [*<IP address>*]

Displays the Multicast Router information of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Routing > Multicast Router Information

info routing -interface [*<IP address>*]

Displays the Interface information of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Routing > Interface Information

info routing -ip_addr [*<IP address>*]

Displays the IP address information of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Routing > IP Address Information

info routing -ospf_area [*<IP address>*]

Displays the OSPF Area information of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Routing > OSPF Area Information

info routing -ospf_ext_lsdb [*<IP address>*]

Displays the OSPF External Link State information of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Routing > OSPF External Link State Information

Command Syntax and Usage

info routing -ospf_intf [*<IP address>*]

Displays the OSPF interface information of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Routing > OSPF Interface Information

info routing -ospf_lsdb [*<IP address>*]

Displays the OSPF Link-State DB information of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Routing > OSPF Link-State DB Information

info routing -ospf_neigh_intf [*<IP address>*]

Displays the OSPF Neighbor interface information of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Routing > OSPF Neighbor Interface Information

info routing -ospf_route [*<IP address>*]

Displays the OSPF route information of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Routing > OSPF Routes Information

info routing -ospf_stats2 [*<IP address>*]

Displays the OSPF Stats2 information of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Routing > OSPF Stats2 Information

Command Syntax and Usage

info routing -ospf_summ_range [*<IP address>*]

Displays the OSPF Summary Range information of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Routing > OSPF Summary Range Information

info routing -ospf_virt_intf [*<IP address>*]

Displays the OSPF Virtual Interface information of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Routing > OSPF Virtual Interface Information

info routing -rip_route [*<IP address>*]

Displays the RIP Router information of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Routing > RIP Route Information

info routing -routes [*<IP address>*]

Displays the Routes information of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Routing > Routes

info routing -routes_std [*<IP address>*]

Displays the Routes standard information of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Routing > Routes Standard

Command Syntax and Usage

info routing -tcp [*<IP address>*]

Displays the TCP connections information of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Routing > TCP Connections

info routing -udp [*<IP address>*]

Displays the UDP information of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Routing > UDP Information

info switch

Command Syntax and Usage

info switch

Displays the usage information.

info switch -trunk [*<IP address>*]

Displays the Trunk Group information of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Port > Trunk Group Information

info switch -ufd [*<IP address>*]

Displays the UFD information of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Port > UFD Information

info virtual_routing

Command Syntax and Usage

info virtual_routing

Displays the usage information.

info virtual_routing -state [*<IP address>*]

Displays the Virtual Routing State information of the given switch.

Note: If the IP address is not specified, the system will prompt you for it.

SNSC UI Equivalent: {Device Console} > Monitor > Port > Virtual Routing State Information

firmware apply

Command Syntax and Usage

firmware apply

Displays the usage information.

firmware apply -ip *<IP address>*

Issues `apply` on the given switch.

SNSC UI Equivalent: Device > Actions > Apply

firmware apply -domain *<name>*

Issues `apply` on all switches contained in that domain. The domain refers to the groups/domains created in System Networking Switch Center UI.

SNSC UI Equivalent: Group Operations > Group Actions > Apply

firmware apply -list *<IP addresses list>*

Issues `apply` on all switches in the list of IP Addresses, specified in comma separated value (CSV) format.

SNSC UI Equivalent: Group Operations > Group Actions > Apply

firmware backup



Command Syntax and Usage

firmware backup

Displays the usage information.

```
firmware backup -ip <IP address>
  [-host <FTP/SFTP/TFTP Server address>]
  [-user <FTP username>]
  [-password <FTP password>]
  [-image {image1|image2|boot}]
  [-port {data|mgt|ext}]
  [-timeout <value>]
```

Transfers (saves) the specified firmware from the switch to the FTP/SFTP/TFTP server.

The default image backup file stored on FTP/SFTP/TFTP server is <IPAddress>_ddMMMyyyy_HHmms. For example, the image backed up from the switch at IP address 192.168.1.1 on 7th March 2008 at 23:59:01 hours will be named 192.168.1.1_07Mar2008_235901.

Notes:

If not supplied in the command input, the system prompts you to specify the following:

- (i) The firmware to backup (image1, image2 or boot)
- (ii) FTP/SFTP/TFTP host address
- (iii) User Name and Password in case of FTP server (user can choose to press Enter without a value to indicate TFTP server).
- (iv) Timeout value (if not specified, the default value is used).
- (v) Port to use on the switch (this is an optional and is prompted only if the given switch supports it).

SNSC UI Equivalent: Group Operations > Deployment > Image Backup

Command Syntax and Usage

```
firmware backup -domain <name>
  [-host <FTP/SFTP/TFTP Server address>]
  [-user <FTP username>]
  [-password <FTP password>]
  [-image {image1|image2|boot}]
  [-port {data|mgt|ext}]
  [-timeout <value>]
```

Transfers (saves) the specified firmware from the switches listed in the domain to the FTP/SFTP/TFTP server. The domain refers to the groups/domains created in System Networking Switch Center UI.

The default image backup file stored on FTP/SFTP/TFTP server is <IP Address>_ddMMMyyyy_HHmmss.img. For example, the image backed up from the switch at IP address 192.168.1.1 on 7th March 2008 at 23:59:01 hours will be named 192.168.1.1_07Mar2008_235901.img.

Notes:

If not supplied in the command input, the system prompts you to specify the following:

- (i) The firmware to backup (image1, image2 or boot)
- (ii) FTP/SFTP/TFTP host address
- (iii) User Name and Password in case of FTP server (user can choose to press Enter without a value to indicate TFTP server).
- (iv) Timeout value (if not specified, the default value is used).
- (v) Port to use on the switch (this is an optional and is prompted only if the given switch supports it).

SNSC UI Equivalent: Group Operations > Deployment > Image Backup

Command Syntax and Usage

firmware backup -list *<IP addresses as comma separate values>*

[-host *<FTP/SFTP/TFTP Server address>*]

[-user *<FTP username>*]



[-password *<FTP password>*]

[-image {**image1** | **image2** | **boot**}

[-port {**data** | **mgt** | **ext**}]

[-timeout *<value>*]

Transfers (saves) the specified firmware from the list of switches to the FTP/SFTP/TFTP server.

The default image backup file stored on FTP/SFTP/TFTP server is *<IPAddress>_ddMMMyyy_HHmms.img*. For example, the image backed up from the switch at IP address 192.168.1.1 on 7th March 2008 at 23:59:01 hours will be named *192.168.1.1_07Mar2008_235901.img*.

Notes:

If not supplied in the command input, the system prompts you to specify the following:

(i) The firmware to backup (image1, image2 or boot)

(ii) FTP/SFTP/TFTP host address

(iii) User Name and Password in case of FTP server (user can choose to press Enter without a value to indicate TFTP server).

(iv) Timeout value (if not specified, the default value is used).

(v) Port to use on the switch (this is an optional and is prompted only if the given switch supports it).

SNSC UI Equivalent: Group Operations > Deployment > Image Backup

firmware conf_backup

Command Syntax and Usage

firmware conf_backup

Displays the usage information.

firmware conf_backup -ip *<IP address>*

[-host *<FTP/SFTP/TFTP Server address>*]

[-user *<FTP username>*]

[-password *<FTP password>*]

[-port {**data**|**mgt**|**ext**}]

[-timeout *<value>*]

Transfers (saves) the switch configuration from the switch to the FTP/SFTP/TFTP server.

The configuration file that you backed up is stored on an FTP, TFTP, or SFTP server. The default naming convention of the back-up file is `config_<IPAddress>_ddMMMyyy_HHmms.txt`. For example, the configuration backed up from the switch at 192.168.1.1 on 7th March 2008 at 23:59:01 hours is stored as `config_192.168.1.1_07Mar2008_235901.txt`.

Notes:

If not supplied in the command input, the system prompts you to specify the following:

(i) FTP/SFTP/TFTP host address

(ii) User Name and Password in case of FTP server (user can choose to press Enter without a value to indicate TFTP server).

(iii) Timeout value (if not specified, the default value is used).

(iv) Port to use on the switch (this is an optional and is prompted only if the given switch supports it).

SNSC UI Equivalent: Group Operations > Deployment > Configuration Backup

Command Syntax and Usage

```
firmware conf_backup -domain <name>
  [-host <FTP/SFTP/TFTP Server address>]
  [-user <FTP username>]
  [-password <FTP password>]
  [-port {data|mgt|ext}]
  [-timeout <value>]
```

Transfers (saves) the switch configuration of the switches listed in the domain to the FTP/SFTP/TFTP server. The domain refers to the groups/domains created in System Networking Switch Center UI.

The configuration file that you backed up is stored on an FTP, TFTP, or SFTP server. The default naming convention of the back-up file is `config_<IP Address>_ddMMMyyy_HHmmss.txt`. For example, the configuration backed up from the switch at 192.168.1.1 on 7th March 2008 at 23:59:01 hours is stored as `config_192.168.1.1_07Mar2008_235901.txt`.

Notes:

If not supplied in the command input, the system prompts you to specify the following:

- (i) FTP/SFTP/TFTP host address
- (ii) User Name and Password in case of FTP server (user can choose to press Enter without a value to indicate TFTP server).
- (iii) Timeout value (if not specified, the default value is used).
- (iv) Port to use on the switch (this is an optional and is prompted only if the given switch supports it).

SNSC UI Equivalent: Group Operations > Deployment > Configuration Backup

Command Syntax and Usage

```
firmware conf_backup -list <IP addresses as comma separate values>
  [-host <FTP/SFTP/TFTP Server address>]
  [-user <FTP username>]
  [-password <FTP password>]
  [-port {data|mgt|ext}]
  [-timeout <value>]
```

Transfers (saves) the switch configuration from the list of switches to the FTP/SFTP/TFTP server.

The configuration file that you backed up is stored on an FTP, TFTP, or SFTP server. The default naming convention of the back-up file is `config_<IP Address>_ddMMMyyy_HHmms.txt`. For example, the configuration backed up from the switch at 192.168.1.1 on 7th March 2008 at 23:59:01 hours is stored as `config_192.168.1.1_07Mar2008_235901.txt`.

Notes:

If not supplied in the command input, the system prompts you to specify the following:

- (i) FTP/SFTP/TFTP host address
- (ii) User Name and Password in case of FTP server (user can choose to press Enter without a value to indicate TFTP server).
- (iii) Timeout value (if not specified, the default value is used).
- (iv) Port to use on the switch (this is an optional and is prompted only if the given switch supports it).

SNSC UI Equivalent: Group Operations > Deployment > Configuration Backup

firmware conf_upload

Command Syntax and Usage

firmware conf_upload

Displays the usage information.

```
firmware conf_upload -ip <IP address>
  [-host <FTP/SFTP/TFTP Server address>]
  [-file_name <name of the config file to upload>]
  [-user <FTP username>]
  [-password <FTP password>]
  [-port {data|mgt|ext}]
  [-timeout <value>]
```

Uploads the given config file from the specified FTP/SFTP/TFTP server to the given switch.

Notes:

If not supplied in the command input, the system prompts you to specify the following:

- (i) FTP/SFTP/TFTP host address
- (ii) The name of the config file to upload
- (iii) User Name and Password in case of FTP server (user can choose to press Enter without a value to indicate TFTP server).
- (iv) Timeout value (if not specified, the default value is used).
- (v) Port to use on the switch (this is an optional and is prompted only if the given switch supports it).

SNSC UI Equivalent: Group Operations > Deployment > Configuration Upgrade

Command Syntax and Usage

```
firmware conf_upload -domain <name>  
  [-host <FTP/SFTP/TFTP Server address>]  
  [-file_name <name of the config file to upload>]  
  [-user <FTP username>]  
  [-password <FTP password>]  
  [-port {data|mgt|ext}]  
  [-timeout <value>]
```

Uploads the given config file from the specified FTP/SFTP/TFTP server to the switches listed in the domain. The domain refers to the groups/domains created in System Networking Switch Center UI.

Notes:

If not supplied in the command input, the system prompts you to specify the following:

- (i) FTP/SFTP/TFTP host address
- (ii) The name of the config file to upload
- (iii) User Name and Password in case of FTP server (user can choose to press Enter without a value to indicate TFTP server).
- (iv) Timeout value (if not specified, the default value is used).
- (v) Port to use on the switch (this is an optional and is prompted only if the given switch supports it).

SNSC UI Equivalent: Group Operations > Deployment > Configuration Upgrade

Command Syntax and Usage

firmware conf_upload -list *<IP addresses as comma separate values>*

[**-host** *<FTP/SFTP/TFTP Server address>*]
 [**-file_name** *<name of the config file to upload>*]
 [**-user** *<FTP username>*]
 [**-password** *<FTP password>*]
 [**-port** {**data**|**mgt**|**ext**}]
 [**-timeout** *<value>*]

Uploads the given config file from the specified FTP/SFTP/TFTP server to the listed switches.

Notes:

If not supplied in the command input, the system prompts you to specify the following:

- (i) FTP/SFTP/TFTP host address
- (ii) The name of the config file to upload
- (iii) User Name and Password in case of FTP server (user can choose to press Enter without a value to indicate TFTP server).
- (iv) Timeout value (if not specified, the default value is used).
- (v) Port to use on the switch (this is an optional and is prompted only if the given switch supports it).

SNSC UI Equivalent: Group Operations > Deployment > Configuration Upgrade

firmware config_dump

Command Syntax and Usage

firmware config_dump

Displays the usage information.

firmware config_dump -ip *<IP address>*

Dumps the current configuration of the given switch on to the screen.

SNSC UI Equivalent: Device > Actions > Config Dump

firmware diff_config

Command Syntax and Usage

firmware diff_config

Displays the usage information.

firmware diff_config -ip *<IP address>*

Displays the pending configuration information on the given switch.

SNSC UI Equivalent: Device > Actions > Diff Config

firmware diff_flash

Command Syntax and Usage

firmware diff_flash

Displays the usage information.

firmware diff_flash -ip *<IP address>*

Displays the unsaved configuration information on the given switch.

SNSC UI Equivalent: Device > Actions > Diff Flash

firmware panicdump

Command Syntax and Usage

firmware panic_dump

Displays the usage information.

```
firmware panic_dump -ip <IP address>
  [-host <FTP/SFTP/TFTP Server address>]
  [-user <FTP username>]
  [-password <FTP password>]
  [-port {data|mgt|ext}]
  [-timeout <value>]
```

Downloads the panic dump, if any, from the given switch and saves it on the specified FTP/SFTP/TFTP server.

The panic dump for the selected switch or switches is stored on the selected FTP, TFTP, or SFTP server. The default filename convention is `panicdump_<IPAddress>_ddMMMyyyy_HHmms`. For example, the panic dump downloaded from the switch at 192.168.1.1 on 7th March 2008 at 23:59:01 hours is stored as `panicdump_192.168.1.1_07Mar2008_235901`.

Notes:

If not supplied in the command input, the system prompts you to specify the following:

- (i) FTP/SFTP/TFTP host address
- (ii) User Name and Password in case of FTP server (user can choose to press Enter without a value to indicate TFTP server).
- (iii) Timeout value (if not specified, the default value is used).
- (iv) Port to use on the switch (this is an optional and is prompted only if the given switch supports it).

SNSC UI Equivalent: Group Operations > Deployment > Panic Dump

Command Syntax and Usage

```
firmware panic_dump -domain <name>
  [-host <FTP/SFTP/TFTP Server address>]
  [-user <FTP username>]
  [-password <FTP password>]
  [-port {data|mgt|ext}]
  [-timeout <value>]
```

Downloads the panic dump, if any, from all the switches listed in the domain and saves them on the specified FTP/SFTP/TFTP server. The domain refers to the groups/domains created in System Networking Switch Center UI.

The panic dump for the selected switch or switches is stored on the selected FTP, TFTP, or SFTP server. The default filename convention is `panicdump_<IP Address>_ddMMMyyy_HHmmss`. For example, the panic dump downloaded from the switch at 192.168.1.1 on 7th March 2008 at 23:59:01 hours is stored as `panicdump_192.168.1.1_07Mar2008_235901`.

Notes:

If not supplied in the command input, the system prompts you to specify the following:

- (i) FTP/SFTP/TFTP host address
- (ii) User Name and Password in case of FTP server (user can choose to press Enter without a value to indicate TFTP server).
- (iii) Timeout value (if not specified, the default value is used).
- (iv) Port to use on the switch (this is an optional and is prompted only if the given switch supports it).

SNSC UI Equivalent: Group Operations > Deployment > Panic Dump

Command Syntax and Usage

```
firmware panic_dump -list <IP addresses as comma separate values>
  [-host <FTP/SFTP/TFTP Server address>]
  [-user <FTP username>]
  [-password <FTP password>]
  [-port {data|mgt|ext}]
  [-timeout <value>]
```

Downloads the panic dump, if any, from given list of switches and saves them on the specified FTP/SFTP/TFTP server.

The panic dump for the selected switch or switches is stored on the selected FTP, TFTP, or SFTP server. The default filename convention is `panicdump_<IP Address>_ddMMMyyy_HHmms`. For example, the panic dump downloaded from the switch at 192.168.1.1 on 7th March 2008 at 23:59:01 hours is stored as `panicdump_192.168.1.1_07Mar2008_235901`.

Notes:

If not supplied in the command input, the system prompts you to specify the following:

- (i) FTP/SFTP/TFTP host address
- (ii) User Name and Password in case of FTP server (user can choose to press Enter without a value to indicate TFTP server).
- (iii) Timeout value (if not specified, the default value is used).
- (iv) Port to use on the switch (this is an optional and is prompted only if the given switch supports it).

SNSC UI Equivalent: Group Operations > Deployment > Panic Dump

firmware reset

Command Syntax and Usage

firmware reset

Displays the usage information.

firmware reset -ip *<IP address>* [**-timeout** *<value>*]

Resets (reboots) the specified switch.

Note: If timeout is not specified, the CLI prompts you to specify the timeout or use the default.

SNSC UI Equivalent: Device > Actions > Reboot Switch

firmware reset -domain *<name>* [**-timeout** *<value>*]

Resets (reboots) all the switches that are listed in the domain. The domain refers to the groups/domains created in System Networking Switch Center UI.

Note: If timeout is not specified, the CLI prompts you to specify the timeout or use the default.

SNSC UI Equivalent: Group Operations > Group Actions > Reboot Switch

firmware reset -list *<IP addresses as comma separate values>* [**-timeout** *<value>*]

Resets (reboots) the given list of switches.

Note: If timeout is not specified, the CLI prompts you to specify the timeout or use the default.

SNSC UI Equivalent: Group Operations > Group Actions > Reboot Switch

firmware save

Command Syntax and Usage

firmware save

Displays the usage information.

firmware save -ip *<IP address>*

Saves the current configuration changes to the Flash memory on the given switch.

SNSC UI Equivalent: Device > Actions > Save

firmware save -domain *<name>*

Saves the current configuration changes to the Flash memory on all the switches listed in the specified domain. The domain refers to the groups/domains created in System Networking Switch Center UI.

SNSC UI Equivalent: Group Operations > Group Actions > Save

firmware save -list *<IP addresses as comma separate values>*

Saves the current configuration changes to the Flash memory on the given list of switches.

SNSC UI Equivalent: Group Operations > Group Actions > Save

firmware tsdump

Command Syntax and Usage

firmware tsdump

Displays the usage information.

firmware tsdump -ip <IP address>

[-host <FTP/SFTP/TFTP Server address>]

[-user <FTP username>]

[-password <FTP password>]

[-port {data|mgt|ext}]

[-timeout <value>]

Generates the tech support dump on the given switch and saves it on the specified FTP/SFTP/TFTP server.

The tech support dump for the selected switch or switches is stored on the selected FTP, TFTP, or SFTP server. The default filename convention is `tsdump_<IPAddress>_ddMMMyyyy_HHmms`. For example, the tech support dump downloaded from the switch at 192.168.1.1 on 7th March 2008 at 23:59:01 hours is stored as `tsdump_192.168.1.1_07Mar2008_235901`.

Notes:

If not supplied in the command input, the system prompts you to specify the following:

(i) FTP/SFTP/TFTP host address

(ii) User Name and Password in case of FTP server (user can choose to press Enter without a value to indicate TFTP server).

(iii) Timeout value (if not specified, the default value is used).

(iv) Port to use on the switch (this is an optional and is prompted only if the given switch supports it).

SNSC UI Equivalent: Group Operations > Deployment > Tech Support Dump

Command Syntax and Usage

```
firmware tsdump -domain <name>
  [-host <FTP/SFTP/TFTP Server address>]
  [-user <FTP username>]
  [-password <FTP password>]
  [-port {data|mgt|ext}]
  [-timeout <value>]
```

Generates the tech support dump on all the switches listed in the domain and saves them on the specified FTP/SFTP/TFTP server. The domain refers to the groups/domains created in System Networking Switch Center UI.

The tech support dump for the selected switch or switches is stored on the selected FTP, TFTP, or SFTP server. The default filename convention is `tsdump_<IP Address>_ddMMMyyy_HHmmss`. For example, the tech support dump downloaded from the switch at 192.168.1.1 on 7th March 2008 at 23:59:01 hours is stored as `tsdump_192.168.1.1_07Mar2008_235901`.

Notes:

If not supplied in the command input, the system prompts you to specify the following:

- (i) FTP/SFTP/TFTP host address
- (ii) User Name and Password in case of FTP server (user can choose to press Enter without a value to indicate TFTP server).
- (iii) Timeout value (if not specified, the default value is used).
- (iv) Port to use on the switch (this is an optional and is prompted only if the given switch supports it).

SNSC UI Equivalent: Group Operations > Deployment > Tech Support Dump

Command Syntax and Usage

```
firmware tsdump -list <IP addresses as comma separate values>  
    [-host <FTP/SFTP/TFTP Server address>]  
    [-user <FTP username>]  
    [-password <FTP password>]  
    [-port {data|mgt|ext}]  
    [-timeout <value>]
```

Generates the tech support dump on the listed switches and saves them on the specified FTP/SFTP/TFTP server.

The tech support dump for the selected switch or switches is stored on the selected FTP, TFTP, or SFTP server. The default filename convention is `tsdump_<IP Address>_ddMMMyyyy_HHmmss`. For example, the tech support dump downloaded from the switch at 192.168.1.1 on 7th March 2008 at 23:59:01 hours is stored as `tsdump_192.168.1.1_07Mar2008_235901`.

Notes:

If not supplied in the command input, the system prompts you to specify the following:

- (i) FTP/SFTP/TFTP host address
- (ii) User Name and Password in case of FTP server (user can choose to press Enter without a value to indicate TFTP server).
- (iii) Timeout value (if not specified, the default value is used).
- (iv) Port to use on the switch (this is an optional and is prompted only if the given switch supports it).

SNSC UI Equivalent: Group Operations > Deployment > Tech Support Dump

firmware upload

Command Syntax and Usage

firmware upload

Displays the usage information.

```
firmware upload -ip <IP address>
  [-host <FTP/SFTP/TFTP Server address>]
  [-file_name <firmware file to upload>]
  [-user <FTP username>]
  [-password <FTP password>]
  [-port {data|mgt|ext}]
  [-timeout <value>]
```

Uploads the firmware from the specified FTP/SFTP/TFTP server to the given switch.

Notes:

If not supplied in the command input, the system prompts you to specify the following:

- (i) Switch software image slot to use (image1, image2 or boot)
- (ii) FTP/SFTP/TFTP host address
- (iii) The firmware file to upload
- (iv) User Name and Password in case of FTP server (user can choose to press Enter without a value to indicate TFTP server).
- (v) Timeout value (if not specified, the default value is used).
- (vi) Port to use on the switch (this is an optional and is prompted only if the given switch supports it).

SNSC UI Equivalent: Group Operations > Deployment > Image Upgrade

Command Syntax and Usage

```
firmware upload -domain <name>  
    [-host <FTP/SFTP/TFTP Server address>]  
    [-file_name <firmware file to upload>]  
    [-user <FTP username>]  
    [-password <FTP password>]  
    [-port {data|mgt|ext}]  
    [-timeout <value>]
```

Uploads the firmware from the specified FTP/SFTP/TFTP server to the switches listed in the domain. The domain refers to the groups/domains created in System Networking Switch Center UI.

Notes:

If not supplied in the command input, the system prompts you to specify the following:

- (i) Switch software image slot to use (image1, image2 or boot)
- (ii) FTP/SFTP/TFTP host address
- (iii) The firmware file to upload
- (iv) User Name and Password in case of FTP server (user can choose to press Enter without a value to indicate TFTP server).
- (v) Timeout value (if not specified, the default value is used).
- (vi) Port to use on the switch (this is an optional and is prompted only if the given switch supports it).

SNSC UI Equivalent: Group Operations > Deployment > Image Upgrade

Command Syntax and Usage

firmware upload -list *<IP addresses as comma separate values>*

[-host *<FTP/SFTP/TFTP Server address>*]

[-file_name *<firmware file to upload>*]

[-user *<FTP username>*]

[-password *<FTP password>*]

[-port {**data**|**mgt**|**ext**}]

[-timeout *<value>*]

Uploads the firmware from the specified FTP/SFTP/TFTP server to the listed switches.

Notes:

If not supplied in the command input, the system prompts you to specify the following:

(i) Switch software image slot to use (image1, image2 or boot)

(ii) FTP/SFTP/TFTP host address

(iii) The firmware file to upload

(iv) User Name and Password in case of FTP server (user can choose to press Enter without a value to indicate TFTP server).

(v) Timeout value (if not specified, the default value is used).

(vi) Port to use on the switch (this is an optional and is prompted only if the given switch supports it).

SNSC UI Equivalent: Group Operations > Deployment > Image Upgrade

data backup

Command Syntax and Usage

maint databackup -path <directory>

Backs up System Networking Switch Center's critical data in the given directory.

System Networking Switch Center uses the standard ZIP format to compress the contents in backup file. The backup file is named as follows:

`SNSC_<version>_<date>_<time>.zip`

Where:

`<version>` is the System Networking Switch Center version in a.b.c.d format,

`<date>` is the date on the System Networking Switch Center server system in **yyyymmdd** format, on which the backup operation was initiated

`<time>` is the time on the System Networking Switch Center server system in **HHMMSS** format, at which the backup operation was initiated.

For example, if the backup operation is initiated in System Networking Switch Center 5.2.1.0 on 23rd July 2010 at 14:01:43 hrs, the backup file is named as follows: `SNSC_5.2.1.0_20100723_140143.zip`

SNSC UI Equivalent: Maintenance > Data Backup > Take Data Backup

support dump

Command Syntax and Usage

```
maint supportdump [-include_db] -path <directory>
```

Saves the System Networking Switch Center's support dump in the given repository. If - include_db is specified, the database will also get included in the support dump.

The support dump file is named as follows:

```
SNSC_SupportDump_<version>_<date>_<time>.zip
```

Where:

<version> is the System Networking Switch Center version in a.b.c.d format,

<date> is the date on the System Networking Switch Center server system in **yyyymmdd** format, on which the backup operation was initiated.

<time> is the time on the System Networking Switch Center server system in **HHMMSS** format, at which the backup operation was initiated.

For example, if the support dump is initiated in System Networking Switch Center 5.2.1.0 on 23rd July 2010 at 14:01:43 hrs, the support dump file is named as follows: SNSC_SupportDump_5.2.1.0_20100723_140143.zip

SNSC UI Equivalent: Maintenance > Data Backup > SNSC Support Dump

Appendix A: Externally Launching IBM System Networking Switch Center

System Networking Switch Center (SNSC) can be launched from an external application using a specialized URL, which allows you to specify additional parameters such as device IP address and a specific page of System Networking Switch Center.

The specialized URL is in the following form:

- **HTTP**
`http://<SNSC system>:40080/snsc/jsp/Launch.jsp?ipaddress=<address>&sysname=<string>&pageid=<id>`
- **HTTPS**
`https://<SNSC system>:40443/snsc/jsp/Launch.jsp?ipaddress=<address>&sysname=<string>&pageid=<id>`

where

ipaddress	The IP address of the switch that is discovered in SNSC, and for which you want to launch the Device Console page.
sysname	The sysName of the device. This parameter enables SNSC to search for the discovered device matching the sysName, if for example, a search based on the IP address fails.
pageid	Enables you to specify which page SNSC should open when it launches for the specified device.

Note: The additional parameters namely `ipaddress`, `sysname`, and `pageid` are optional. If not specified, System Networking Switch Center opens the Summary Page.

List of Page IDs

The following table lists the pageid used for various Monitoring and Configuration pages of System Networking Switch Center:

Tab Reference	Page ID
Monitor > Summary > Health Status	mon_sum_hs
Monitor > Summary > Information	mon_sum_inf
Monitor > Summary > Port Status	mon_sum_pstat
Monitor > Summary > Port Summary	mon_sum_psum
Monitor > Summary > Events	mon_sum_ev
Monitor > Summary > Syslog	mon_sum_syslog
Monitor > Switch > Information	mon_sw_inf
Monitor > Switch > SNMP Statistics	mon_sw_snmp
Monitor > Switch > Packet Statistics	mon_sw_pkt
Monitor > Switch > STP Statistics	mon_sw_stpstat
Monitor > Switch > MP CPU Statistics	mon_sw_mpcpustat
Monitor > Switch > UFD Statistics	mon_sw_ufdstat
Monitor > Switch > UFD information	mon_sw_ufdinfo
Monitor > Switch > NTP Statistics	mon_sw_ntpstat
Monitor > Switch > Trunk Groups	mon_sw_trnkgrps
Monitor > Switch > Trunk Group Ports	mon_sw_trnkgrppts
Monitor > Switch > TACACS Authentication Statistics	mon_sw_tac_auth_stat
Monitor > Ports > Summary	mon_prt_sum
Monitor > Ports > Interface Statistics	mon_prt_ifstat
Monitor > Ports > 802.1x Statistics	mon_prt_8021x
Monitor > Ports > LACP Statistics	mon_prt_lacpstat
Monitor > Ports > LACP Aggregator	mon_prt_lacpagrtor
Monitor > Ports > LACP Port Aggregator	mon_prt_lacpprtagrtor
Monitor > Ports > Bridge Statistics	mon_prt_brdgstat
Monitor > Ports > Ethernet Error Statistics	mon_prt_etherstat
Monitor > Ports > Transceiver Info	mon_prt_transinfo
Monitor > Ports > IP Statistics	mon_prt_ipstat
Monitor > Ports > Authenticator Diagnostics Statistics	mon_prt_authdiagstat

Monitor > Layer 2 > Bridge > Forwarding Statistics	mon_brdg_fwdstat
Monitor > Layer 2 > Bridge > Forwarding Database Information	mon_brdg_fwddbinfo
Monitor > Layer 2 > Bridge > Base Port Information	mon_brdg_bpinfo
Monitor > Layer 2 > Bridge > CIST Bridge Information	mon_brdg_cistbrdginfo
Monitor > Layer 2 > Bridge > CIST Port Information	mon_brdg_cistprtinfo
Monitor > Layer 2 > Bridge > STP	mon_brdg_stp
Monitor > Layer 2 > LLDP > LLDP Port Info	mon_lldp_portinfo
Monitor > Layer 2 > Failover > General	mon_failovr_gen
Monitor > Layer 2 > Failover > Trigger Information	mon_failovr_trgrinfo
Monitor > Layer 2 > Failover > Monitor Port Status	mon_failovr_monprtstat
Monitor > Layer 2 > Failover > Control Port Status	mon_failovr_ctrlprt
Monitor > Layer 2 > Hot Links > Summary	mon_hotlnk_sum
Monitor > Layer 2 > Hot Links > Statistics	mon_hotlnk_stat
Monitor > Layer 2 > Hot Links > Info	mon_hotlnk_info
Monitor > Layer 2 > 802.1x/p > 802.1x/p General	mon_802_gen
Monitor > Layer 2 > 802.1x/p > 802.1x/p Priority COSq	mon_802_pricosq
Monitor > Layer 2 > 802.1x/p > Port Priority	mon_802_pprior
Monitor > Layer 3 > IP > IP Interface Statistics	mon_ip_ipifstat
Monitor > Layer 3 > IP > Interface Information	mon_ip_ifinfo
Monitor > Layer 3 > IP > TCP Statistics	mon_ip_tcpstat
Monitor > Layer 3 > IP > TCP Connections	mon_ip_tcpcon
Monitor > Layer 3 > IP > UDP Statistics	mon_ip_udpstat
Monitor > Layer 3 > IP > UDP Information	mon_ip_udpinfo
Monitor > Layer 3 > IP > IP Statistics	mon_ip_ipstat
Monitor > Layer 3 > IP > ICMP In Statistics	mon_ip_icmpinstat
Monitor > Layer 3 > IP > ICMP Out Statistics	mon_ip_icmpoutstat
Monitor > Layer 3 > IP > DNS Statistics	mon_ip_dnsstat
Monitor > Layer 3 > IP > Routes	mon_ip_routes
Monitor > Layer 3 > IP > Routes Standard	mon_ip_routesstd
Monitor > Layer 3 > IP > Route Statistics	mon_ip_routesstat
Monitor > Layer 3 > IP > ARP	mon_ip_arp
Monitor > Layer 3 > IP > ARP Statistics	mon_ip_arpstat
Monitor > Layer 3 > IP > Gateway Information	mon_ip_gtwinfo

Monitor > Layer 3 > IP > IP Address Information	mon_ip_ipaddinfo
Monitor > Layer 3 > BGP > Peers Summary	mon_bgp_peersum
Monitor > Layer 3 > BGP > Routing Table	mon_bgp_routtable
Monitor > Layer 3 > RIP > RIP V2 Statistics	mon_rip_ripstat
Monitor > Layer 3 > RIP > RIP Route Information	mon_rip_riprouinfo
Monitor > Layer 3 > OSPF > General OSPF Statistics	mon_ospf_genospfstat
Monitor > Layer 3 > OSPF > OSPF Area Statistics	mon_ospf_areatstat
Monitor > Layer 3 > OSPF > OSPF Area Neighbor Statistics	mon_ospf_areaneighstat
Monitor > Layer 3 > OSPF > OSPF Area Interface Statistics	mon_ospf_areaifstat
Monitor > Layer 3 > OSPF > OSPF Area Receive Error Statistics	mon_ospf_arearecverrstat
Monitor > Layer 3 > OSPF > OSPF Area Interface Receive Error Statistics	mon_ospf_areaifrecverrstat
Monitor > Layer 3 > OSPF > OSPF Interface Change Statistics	mon_ospf_ifchngstat
Monitor > Layer 3 > OSPF > OSPF Interface Transmission Statistics	mon_ospf_iftransstat
Monitor > Layer 3 > OSPF > OSPF Interface Neighbor Statistics	mon_ospf_ifneighstat
Monitor > Layer 3 > OSPF > OSPF Area Information	mon_ospf_areainfo
Monitor > Layer 3 > OSPF > OSPF Interface Information	mon_ospf_ifinfo
Monitor > Layer 3 > OSPF > OSPF Neighbor Interface Information	mon_ospf_neighifinfo
Monitor > Layer 3 > OSPF > OSPF Virtual Interface Information	mon_ospf_virtifinfo
Monitor > Layer 3 > OSPF > OSPF Stats2 Information	mon_ospf_stat2finfo
Monitor > Layer 3 > OSPF > OSPF Link-State DB Information	mon_ospf_lnkdbinfo
Monitor > Layer 3 > OSPF > OSPF External Link-State DB Information	mon_ospf_extlnkdbinfo
Monitor > Layer 3 > OSPF > OSPF Summary Range Information	mon_ospf_sumrnginfo
Monitor > Layer 3 > OSPF > OSPF Routes Information	mon_ospf_routesinfo
Monitor > Layer 3 > IGMP > IGMP Information	mon_igmp_info
Monitor > Layer 3 > IGMP > Multicast Router Information	mon_igmp_multirouteinfo
Monitor > Layer 3 > IGMP > IGMP Snooping Statistics	mon_igmp_snoopstat

Monitor > Layer 3 > Virtual Routing > Virtual Routing	mon_vr_virtrouting
Monitor > Layer 3 > Virtual Routing > Virtual Routing State	mon_vr_virtroutingstate
Monitor > Access Control List > ACL Statistics	mon_acl_aclstat
Monitor > Access Control List > MAC ACL Statistics	mon_acl_macaclstat
Monitor > Access Control List > IP ACL Statistics	mon_acl_ipaclstat
Monitor > FCoE > FIP Snooping Information	mon_fcoe_fipsnoopinfo
Monitor > FCoE > FIP Snooping Statistics	mon_fcoe_fipsnoopstat
Monitor > Virtualization > VMReady Port Info	mon_virt_vmreadyportinfo
Monitor > Virtualization > VMReady VM Info	mon_virt_vmreadyvminfo
Monitor > EVB > VDP TLV Info	mon_evb_vdptlvinfo
Monitor > EVB > VSI Information	mon_evb_vsiinfo
Monitor > EVB > ECP Channel Info	mon_evb_ecbchannelinfo
Monitor > EVB > EVB Local Info	mon_evb_evblocalinfo
Monitor > EVB > EVB Remote Info	mon_evb_evbremoteinfo
Monitor > EVB > VM Info	mon_evb_vminfo
Monitor > EVB > VSI DB Info	mon_evb_vsidbinfo
Monitor > EVB > VSI DB ACL Info	mon_evb_vsidbaclinfo
Monitor > iSwitch > Port Information	mon_iswitch_portinfo
Monitor > iSwitch > Host Uplink Information	mon_iswitch_hostuplink_info
Configure > Switch > General	cfg_sw_gen
Configure > Switch > Firmware	cfg_sw_fw
Configure > Switch > Syslog Hosts	cfg_sw_syshost
Configure > Switch > Trap Settings	cfg_sw_trapsettings
Configure > Switch > RADIUS Server	cfg_sw_radserv
Configure > Switch > RADIUS General	cfg_sw_radgen
Configure > Switch > TACACS Server	cfg_sw_tacacserv
Configure > Switch > TACACS - User Map	cfg_sw_tacacusmap
Configure > Switch > TACACS General	cfg_sw_tacacsgen
Configure > Switch > TACACS Command Auth	cfg_sw_tacacscmdauth
Configure > Switch > NTP Service	cfg_sw_ntpservc
Configure > Switch > Management Network	cfg_sw_mgmtntwrk
Configure > Switch > Port Mirroring	cfg_sw_portmirr
Configure > Switch > System Trap Settings	cfg_sw_systrapsettings

Configure > Config/Image/Dump Control > Config/Image/ Dump Control	cfg_cfgimgdumpctrl
Configure > Access User > Access User	cfg_accessuser
Configure > Layer 2 > General > General	cfg_l2_general
Configure > Layer 2 > Trunk > Trunk Hash	cfg_l2_trnk_hash
Configure > Layer 2 > Trunk > Trunk Groups	cfg_l2_trnk_grps
Configure > Layer 2 > LACP > LACP General	cfg_l2_lacp_gen
Configure > Layer 2 > LACP > LACP Ports	cfg_l2_lacp_ports
Configure > Layer 2 > 802.1x > General	cfg_l2_8021x_gen
Configure > Layer 2 > 802.1x > Global	cfg_l2_8021x_global
Configure > Layer 2 > 802.1x > Guest VLAN	cfg_l2_8021x_guestvlan
Configure > Layer 2 > 802.1x > Ports	cfg_l2_8021x_ports
Configure > Layer 2 > MSTP/RSTP > MSTP	cfg_l2_mstprstp_mstp
Configure > Layer 2 > CIST > CIST Bridge	cfg_l2_cist_bridge
Configure > Layer 2 > CIST > CIST Port	cfg_l2_cist_ports
Configure > Layer 2 > Spanning Tree Protocol > STP Groups	cfg_l2_stp_grps
Configure > Layer 2 > Spanning Tree Protocol > STP Port	cfg_l2_stp_ports
Configure > Layer 2 > Spanning Tree Protocol > Spanning Tree	cfg_l2_stp_tree
Configure > Layer 2 > Forwarding Database > FDB General	cfg_l2_fdb_gen
Configure > Layer 2 > Forwarding Database > FDB Static	cfg_l2_fdb_static
Configure > Layer 2 > Forwarding Database > Static Multicast	cfg_l2_fdb_mcast
Configure > Layer 2 > VLAG > General	cfg_l2_vlag_gen
Configure > Layer 2 > VLAG > Trunk	cfg_l2_vlag_trunk
Configure > Layer 2 > VLAG > LACP	cfg_l2_vlag_lacp
Configure > Layer 2 > VLAG > ISL	cfg_l2_vlag_isl
Configure > Layer 2 > Hot Links > General Configuration	cfg_l2_hl_gencfg
Configure > Layer 2 > Hot Links > Triggers	cfg_l2_hl_triggers
Configure > Layer 2 > Virtual LANs > VLAN Memberships	cfg_l2_virtlans_vlanmem
Configure > Layer 2 > Virtual LANs > VMAP for Non Server Ports	cfg_l2_virtlans_vmap_nonsrv ports
Configure > Layer 2 > Virtual LANs > VMAP for Server Ports	cfg_l2_virtlans_vmap_srvpor ts

Configure > Layer 2 > Virtual LANs > VMAP for All Ports	cfg_l2_virtlans_vmapallports
Configure > Layer 2 > Virtual LANs > Private Vlan	cfg_l2_virtlans_privlan
Configure > Layer 2 > Virtual LANs > Protocol Vlan	cfg_l2_virtlans_protovlan
Configure > Layer 2 > LLDP > General	cfg_l2_lldp_gen
Configure > Layer 2 > LLDP > LLDP Port	cfg_l2_lldp_ports
Configure > Layer 2 > AMP > General	cfg_l2_amp_gen
Configure > Layer 2 > AMP > Group	cfg_l2_amp_group
Configure > Layer 3 > IP > Interfaces	cfg_l3_if
Configure > Layer 3 > IP > Forwarding	cfg_l3_ip_fwd
Configure > Layer 3 > IP > Network Filters	cfg_l3_ip_nwf
Configure > Layer 3 > IP > Loopback Interfaces	cfg_l3_ip_loopbackif
Configure > Layer 3 > IP > Static ARP	cfg_l3_ip_statarp
Configure > Layer 3 > Gateways > Gateways	cfg_l3_gw
Configure > Layer 3 > ARP > ARP	cfg_l3_arp
Configure > Layer 3 > OSPF > General	cfg_l3_ospf_gen
Configure > Layer 3 > OSPF > Areas	cfg_l3_ospf_area
Configure > Layer 3 > OSPF > Interfaces	cfg_l3_ospf_if
Configure > Layer 3 > OSPF > Summary Ranges	cfg_l3_ospf_sumrange
Configure > Layer 3 > OSPF > Virtual Interfaces	cfg_l3_ospf_virtif
Configure > Layer 3 > OSPF > Host Table	cfg_l3_ospf_hosttab
Configure > Layer 3 > OSPF > MD5 Key	cfg_l3_ospf_md5key
Configure > Layer 3 > OSPF > Loopback Interface	cfg_l3_ospf_loopbackif
Configure > Layer 3 > OSPF > Static Routes	cfg_l3_ospf_staticroute
Configure > Layer 3 > OSPF > Fixed Routes	cfg_l3_ospf_fixedroute
Configure > Layer 3 > OSPF > RIP	cfg_l3_ospf_rip
Configure > Layer 3 > OSPF > BGP External Route Redistribute	cfg_l3_ospf_bgpext
Configure > Layer 3 > OSPF > BGP Internal Route Redistribute	cfg_l3_ospf_bgpint
Configure > Layer 3 > VRRP > General	cfg_l3_vrrp_gen
Configure > Layer 3 > VRRP > Virtual Router	cfg_l3_vrrp_virtrouter
Configure > Layer 3 > VRRP > Virtual Interface	cfg_l3_vrrp_virtif
Configure > Layer 3 > VRRP > Virtual Router Group	cfg_l3_vrrp_virtroutegrp

Configure > Layer 3 > DHCP > Snooping	cfg_l3_dhcp_snooping
Configure > Layer 3 > DHCP > Snooping VLAN	cfg_l3_dhcp_snoopingvlan
Configure > Layer 3 > Flooding > Flooding	cfg_l3_flooding
Configure > Ports > Ports	cfg_ports
Configure > Ports > Ports General	cfg_ports_gen
Configure > Ports > Threshold Rate	cfg_ports_threshold
Configure > Ports > Gigabit Link	cfg_ports_gigabitlink
Configure > Ports > UDLD	cfg_ports_udld
Configure > Ports > OAM	cfg_ports_oam
Configure > Ports > ACL/QOS	cfg_ports_aclqos
Configure > Ports > STP	cfg_ports_stp
Configure > Ports > Port Priority	cfg_ports_priority
Configure > Ports > DHCP Snooping	cfg_ports_dhcpsnooping
Configure > Access Control List > ACL	cfg_acl
Configure > Access Control List > ACL Groups	cfg_acl_aclgrps
Configure > Access Control List > VMAP	cfg_acl_vmap
Configure > Access Control List > Log	cfg_acl_log
Configure > Access Control List > MAC ACL	cfg_acl_mac
Configure > Access Control List > IP ACL	cfg_acl_ip
Configure > CEE > General	cfg_cee_gen
Configure > CEE > Priority Allocation	cfg_cee_prioalloc
Configure > CEE > Bandwidth Allocation	cfg_cee_bwalloc
Configure > CEE > PFC	cfg_cee_pfc
Configure > CEE > PFC Status	cfg_cee_pfcstatus
Configure > CEE > Port PFC	cfg_cee_portpfc
Configure > CEE > Port PFC Status	cfg_cee_portpfcstatus
Configure > CEE > DCBX	cfg_cee_dcbx
Configure > FCoE > FIP Snooping	cfg_fcoe_fipsnoop
Configure > FCoE > FIP Snooping Port	cfg_fcoe_fipsnoopport
Configure > Virtualization > VMready > General	cfg_virt_vmready_gen
Configure > Virtualization > VMready > VMware vCenter Access	cfg_virt_vmready_vmvctraccess
Configure > Virtualization > VMready > Profiles	cfg_virt_vmready_profiles
Configure > Virtualization > VMready > Groups	cfg_virt_vmready_grps

Configure > Virtualization > VMready > Bandwidth	cfg_virt_vmready_bw
Configure > Virtualization > VMready > Ports	cfg_virt_vmready_ports
Configure > Virtualization > VMready > Virtual Machines	cfg_virt_vmready_virtmachine
Configure > Virtualization > VMready > Advanced Pre-Provisioning	cfg_virt_vmready_advpreprovision
Configure > vNIC > General	cfg_vnic_gen
Configure > vNIC > vNICs	cfg_vnic_vnics
Configure > vNIC > vNICs Groups	cfg_vnic_vnicsgrps
Configure > EVB > General	cfg_evb_gen
Configure > EVB > Profiles	cfg_evb_prof
Configure > EVB > VSI DB Host	cfg_evb_vsldbhost
Configure > iSwitch > vCenter	cfg_iswitch_vcenter
Configure > iSwitch > Virtual Data Station	cfg_iswitch_vds
Virtualization Tools > VSI DB Console	vsi_manager

Appendix B: Integrating SNSC with IBM Tivoli Network Manager

System Networking Switch Center (SNSC) can be integrated with IBM Tivoli Network Manager (ITNM) IP Edition 3.9 and above so that it can be launched from Tivoli Integrated Portal (TIP) GUI. System Networking Switch Center supports Launch-In-Context (LIC) and Single Sign-On (SSO) based launch from Tivoli Network Manager. This section describes various steps involved in configuring both System Networking Switch Center and Tivoli Network Manager for enabling LIC and SSO of System Networking Switch Center from Tivoli Network Manager.

Requirements

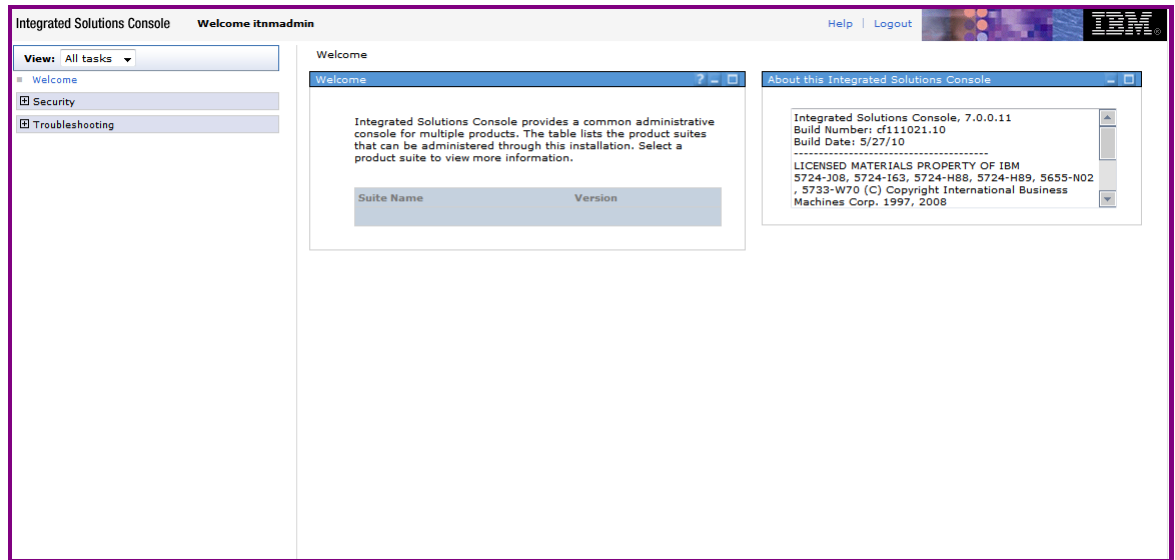
- Tivoli Network Manager 3.9 or above installed
- System Networking Switch Center 6.1
- Tivoli Network Manager has discovered at least one IBM BLADE switch.

Step 1: Generate Signer Certificate

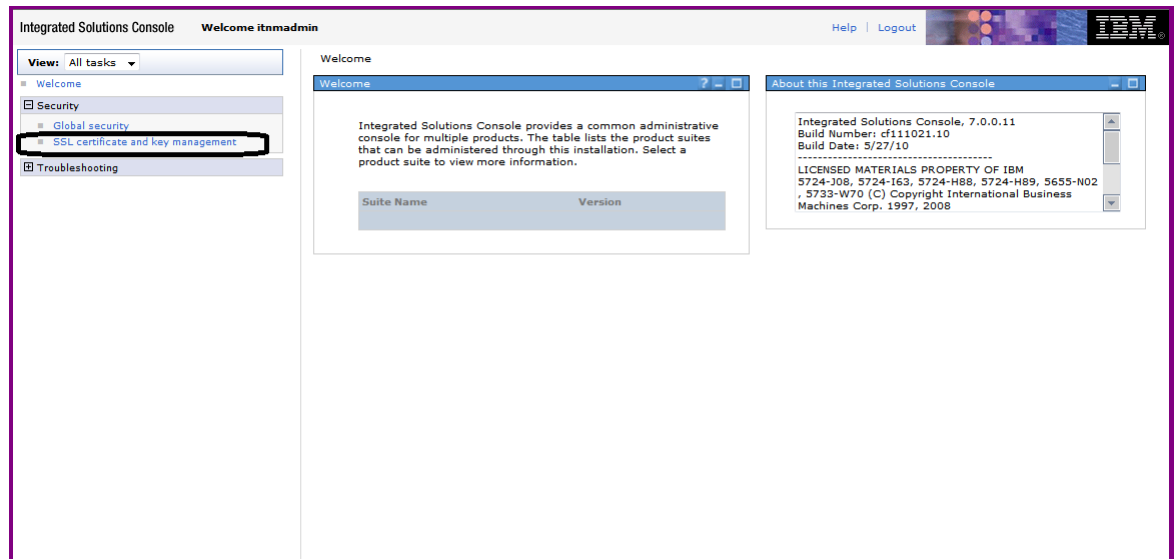
System Networking Switch Center needs Tivoli Network Manager Signer Certificate for creating the key store. This key store is required for single sign-on. The following steps describe signer certificate generation:

- 1 Launch Tivoli Network Manager's WebSphere console:
 - a You can directly launch WebSphere Console (Integrated Solutions Console) using the following URL:
`https://<Tivoli Network Manager IP Address>: 16316/ibm/console/login.jsp`

- b Alternatively, launch Tivoli Network Manager TIP (<https://<Tivoli Network Manager IP Address>:16311/ibm/console>) and then select **Settings > WebSphere Administrative Console**.



- 2 On the left pane, select **Security > SSL certificate and key management**.



3 Under Related Items, click **Key stores and certificates**.

Integrated Solutions Console Welcome itnadmin

Cell=TIPCell, Profile=TIPProfile

SSL certificate and key management

SSL certificate and key management

SSL configurations

The Secure Sockets Layer (SSL) protocol provides secure communications between remote server processes or endpoints. SSL security can be used for establishing communications inbound to and outbound from an endpoint. To establish secure communications, a certificate and an SSL configuration must be specified for the endpoint.

In previous versions of this product, it was necessary to manually configure each endpoint for Secure Sockets Layer (SSL). In this version, you can define a single configuration for the entire application-serving environment. This capability enables you to centrally manage secure communications. In addition, trust zones can be established in multiple node environments by overriding the default, cell-level SSL configuration.

If you have migrated a secured environment to this version using the migration utilities, the old Secure Sockets Layer (SSL) configurations are restored for the various endpoints. However, it is necessary for you to re-configure SSL to take advantage of the centralized management capability.

Configuration settings

[Manage endpoint security configurations](#)

[Manage certificate expiration](#)

☐ Use the United States Federal Information Processing Standard (FIPS) algorithms. Note: This option requires the TLS handshake protocol, which some browsers do not enable by default.

☒ Dynamically update the run time when SSL configuration changes occur

Related Items

- SSL configurations
- Dynamic outbound endpoint SSL configurations
- Key stores and certificates**
- Key sets
- Key set groups
- Key managers
- Trust managers
- Certificate Authority (CA) client configurations

Field help
For field help information, select a field label or list marker when the help cursor is displayed.

Page help
[More information about this page](#)

4 Click **NodeDefaultTrustStore**.

Integrated Solutions Console Welcome itnadmin

Cell=TIPCell, Profile=TIPProfile

SSL certificate and key management

SSL certificate and key management > Key stores and certificates

Defines keystore types, including cryptography, RACF(R), CMS, Java(TM), and all truststore types.

Keystore usages

SSL keystores

Preferences

New Delete Change password... Exchange signers...

Select	Name	Description	Management Scope	Path
<input type="checkbox"/>	NodeDefaultKeyStore	Default key store for TIPNode	(cell):TIPCell; (node):TIPNode	\$(CONFIG_ROOT)/cells/TIPCell/nodes/TIPNode/key.p12
<input checked="" type="checkbox"/>	NodeDefaultTrustStore	Default trust store for TIPNode	(cell):TIPCell; (node):TIPNode	\$(CONFIG_ROOT)/cells/TIPCell/nodes/TIPNode/trust.p12

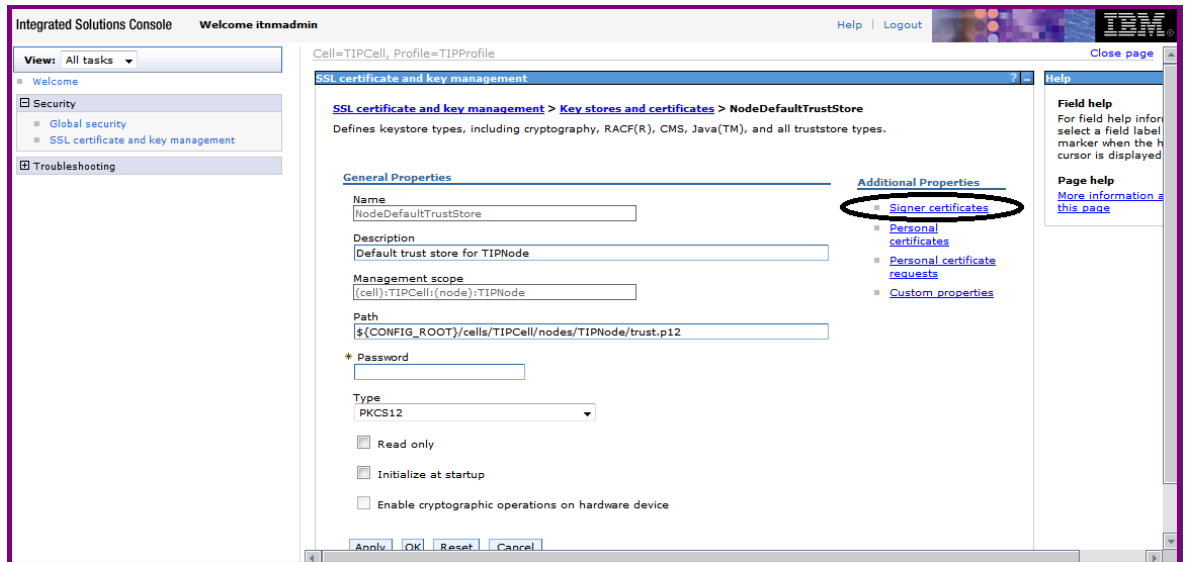
Total 2

Field help
For field help information, select a field label or list marker when the help cursor is displayed.

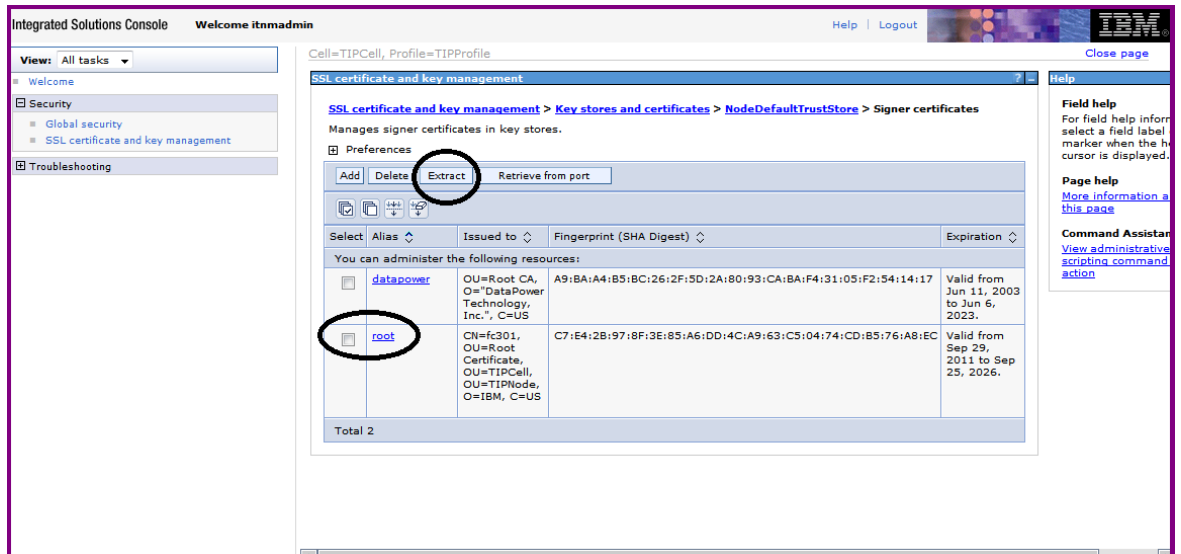
Page help
[More information about this page](#)

Command
[View and execute command](#)

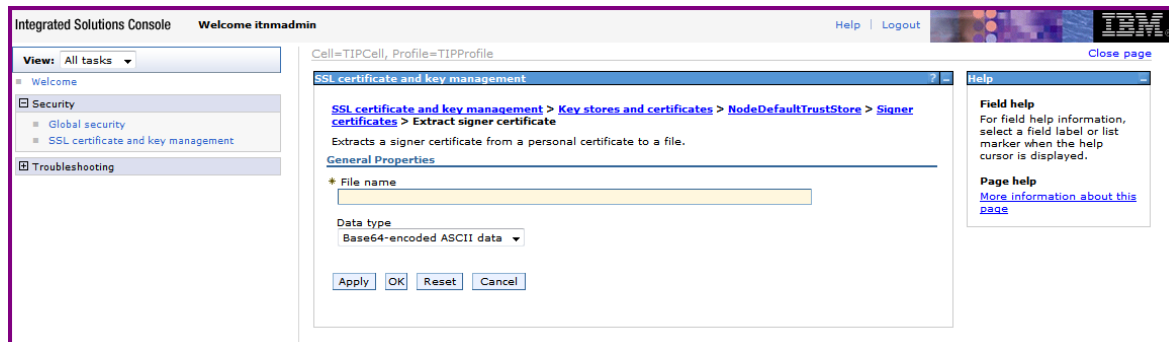
5 Under Additional Properties, click **Signer certificates**.



6 Select the **default** or **root** certificate box, then click **Extract**.



- 7 In the dialog box, enter a file name for the signer certificate and select the following data type: Base64-encoded ASCII data. Click **OK**.



Note: The contents are extracted onto the system where Tivoli Network Manager is running, so the file name should be specific to that system, including the path.

Step 2: Create Key Store

- 1 Login to the system where System Networking Switch Center is installed.
- 2 Download or copy the Signer certificate file created in “[Step 1: Generate Signer Certificate](#)” on page 799 to a directory (for Linux, use /tmp). If System Networking Switch Center is installed on the same system where Tivoli Network Manager is also installed, then you just have to copy the file.
- 3 Change the directory to `<installation directory>/conf/auth`. For example:
`cd /opt/ibm/snsc/conf/auth`
- 4 Create key store using the JRE keytool bundled in System Networking Switch Center. Use the following command:
`<installation directory>/j2re/bin/keytool -import -keystore ess_ts.jks -storepass <password> -file <signer certificate file> -alias <alias>`

Where:

<code><password></code>	The password required for protecting the integrity of the keystore.
<code><signer certificate file></code>	The file path of the signer certificate file.
<code><alias></code>	An alias for the keystore. This should be unique within the trust store. If it is a new file, you may use any name, for example, default.

For example, issue the command below to create the keystore with the following parameters:

- signer certificate is `/tmp/signer_cert`
- password is `pass123`
- alias is `default`

```
# /opt/ibm/snsc/j2re/bin/keytool -import -keystore ess_ts.jks -
storepass pass123 -file /tmp/signer_cert -alias default
```

Step 3: Configure System Networking Switch Center for LIC & SSO

- 1 Login as root to Linux system where System Networking Switch Center is running.
- 2 Stop SNSC:
`/opt/ibm/snsc/bin/shutdown.sh`
- 3 Update the following file: `/opt/ibm/snsc/conf/auth/ess_auth.properties`
Edit the following fields:

<code>itnm.server.address</code>	The IP Address of the system where Tivoli Network Manager is installed (example: <code>itnm.server.address=snsc.foo.net</code>).
<code>itnm.server.port</code>	The port number where Tivoli Network Manager can be accessed (example: <code>itnm.server.port=16311</code>).
<code>snsc.keystore.password</code>	The password that was used to generate the keystore (example: <code>snsc.keystore.password=pass123</code>).
<code>itnm.ess.username</code>	The username for accessing the ESS Server. This can be an Tivoli Network Manager login user name (example: <code>itnm.ess.username=tipadmin</code>)
<code>itnm.ess.password</code>	The password for <code>itnm.ess.username</code> (example: <code>itnm.ess.password=xxxxx</code>).

- 4 Start SNSC:
`/opt/ibm/snsc/bin/startup.sh`

Note: Though the passwords are entered in clear text, when System Networking Switch Center is restarted, the clear text passwords in the `ess_auth.properties` file are replaced with encrypted passwords.

Step 4: Create System Networking Switch Center User Groups in IBM Tivoli Network Manager

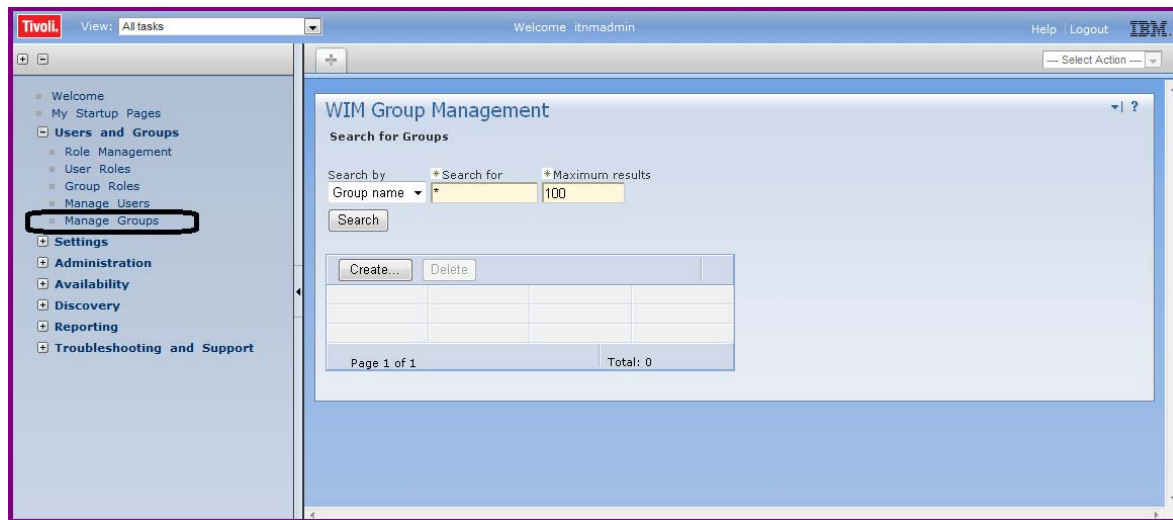
System Networking Switch Center uses User Groups information for determining the role (admin, oper, user) associated with a user when the user tries to launch System Networking Switch Center from Tivoli Network Manager TIP.

The following list shows the mapping of System Networking Switch Center roles with System Networking Switch Center User Groups in Tivoli Network Manager:

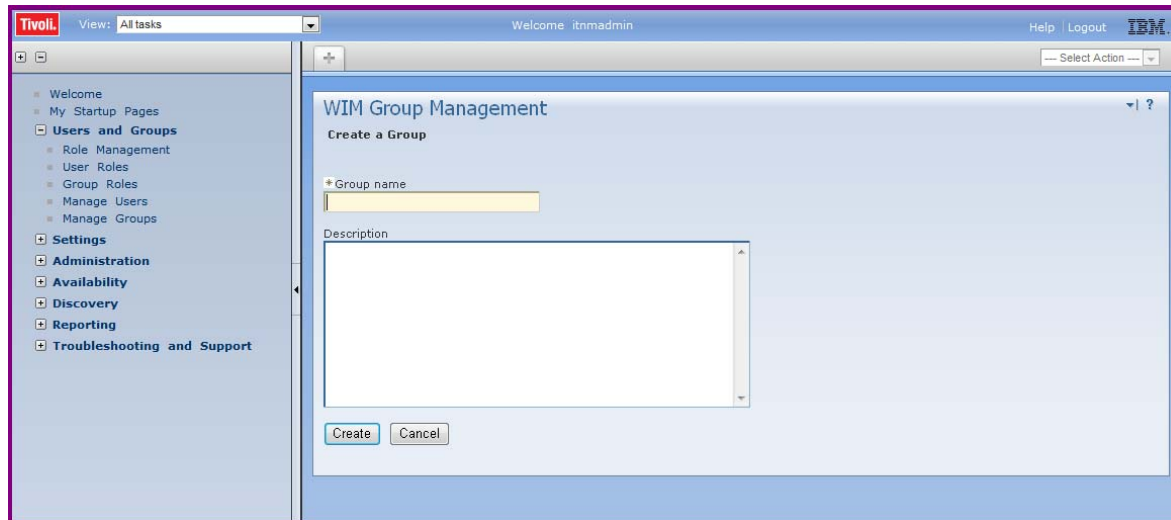
User Groups in Tivoli Network Manager	SNSC Role
snsadmin	admin
snscooper	oper
snsuser	user

Use the following steps to create System Networking Switch Center User Groups in Tivoli Network Manager:

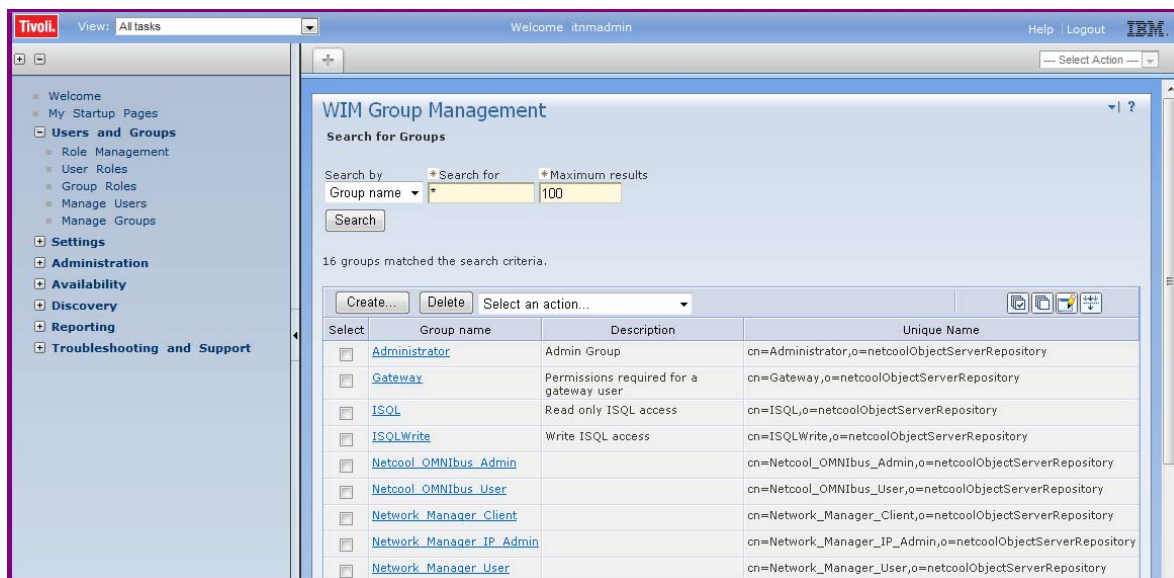
- 1 Login to Tivoli Network Manager using an administrative privileged user (for example, itnadmin).
- 2 Select **Users and Groups > Manage Groups** to open the WIM Group Management window.



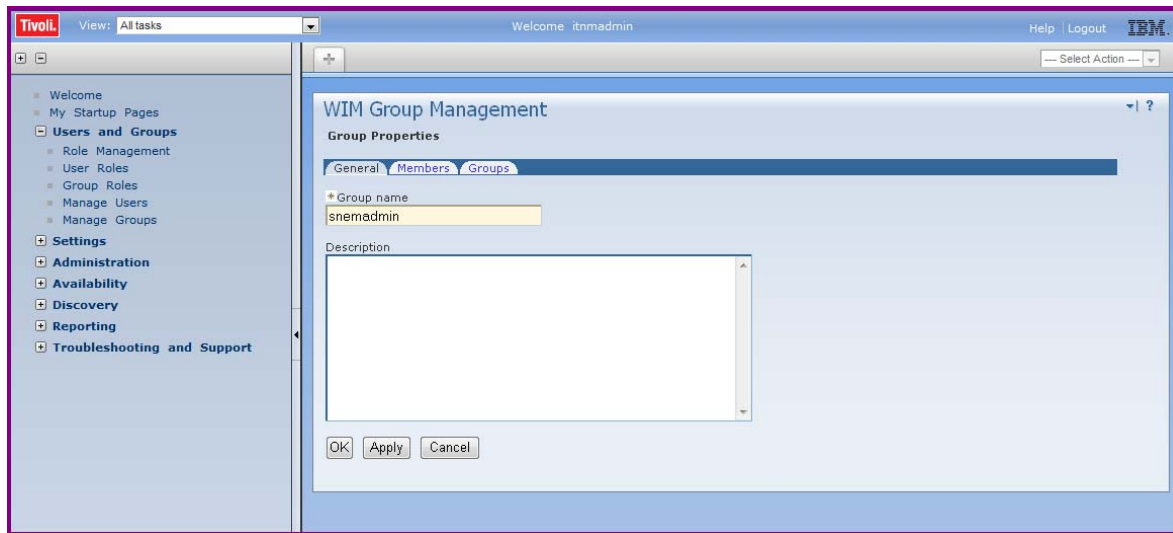
- Click **Create...** in WIM Group Management panel to open the Group creation dialog.



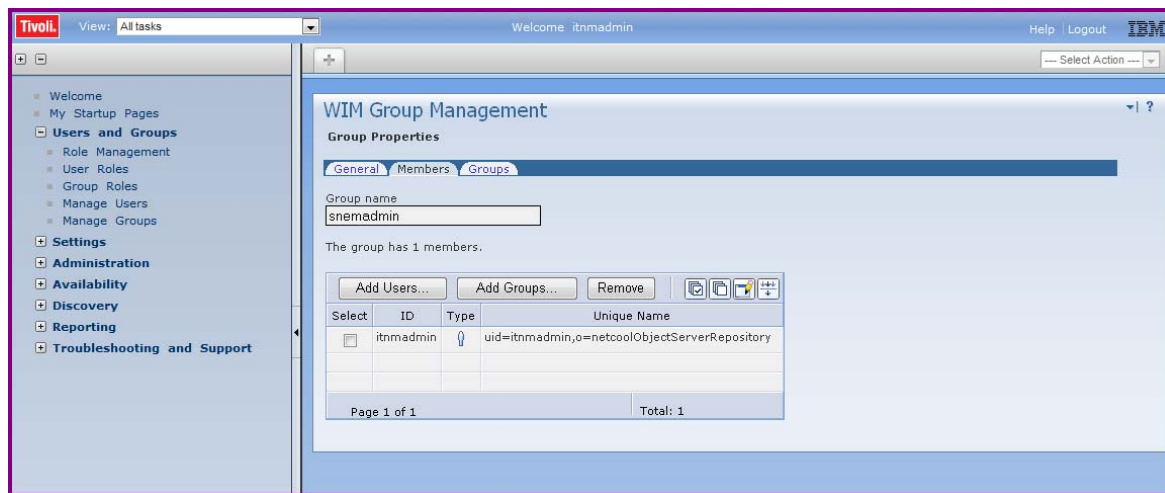
- Enter the text `snsadmin` in Group name field and click **Create** to create `snsadmin` User Group.
- Repeat the above step for the `snscooper` and `snsuser` User Groups.
- Select **Users and Groups > Manage Groups** and click **Search** to list all the configured User Groups.



- 7 Select the snscadmin Group name hyperlink for which you want to add users. The Group Properties dialog opens.



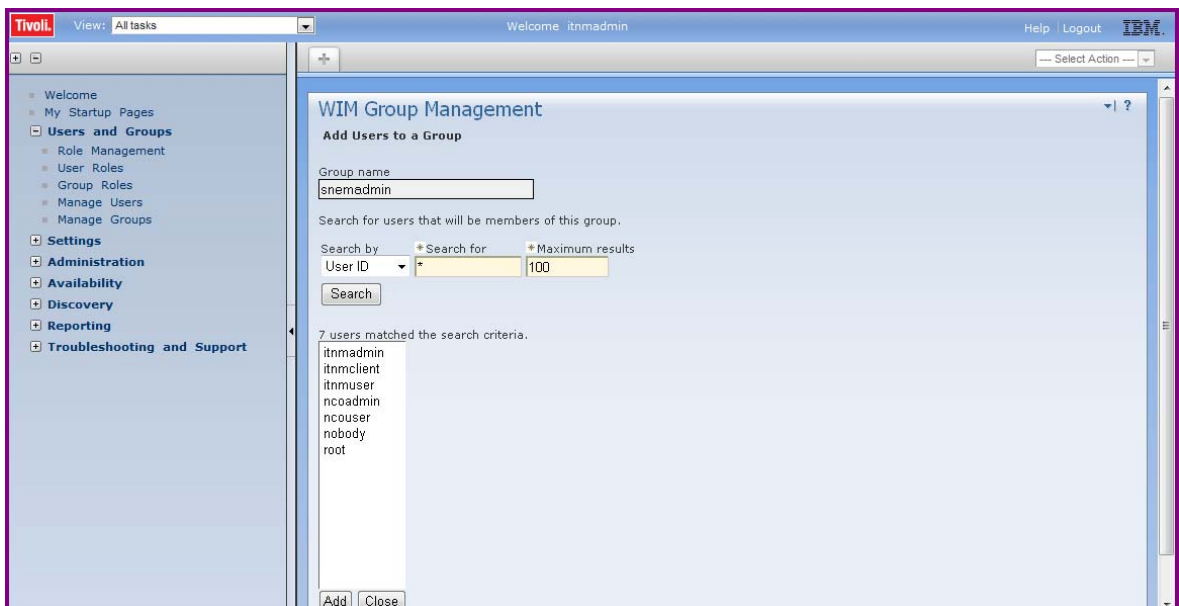
- 8 Select the Members tab to add users.



9 Click **Add Users...** to open the Add Users to a Group dialog.



10 Click **Search** to list all of the configured users.



To list only those users matching the search pattern, type the user name in the * **Search for** field and click **Search**.

11 Select the user you want to add to the System Networking Switch Center User Group and click **Add**.

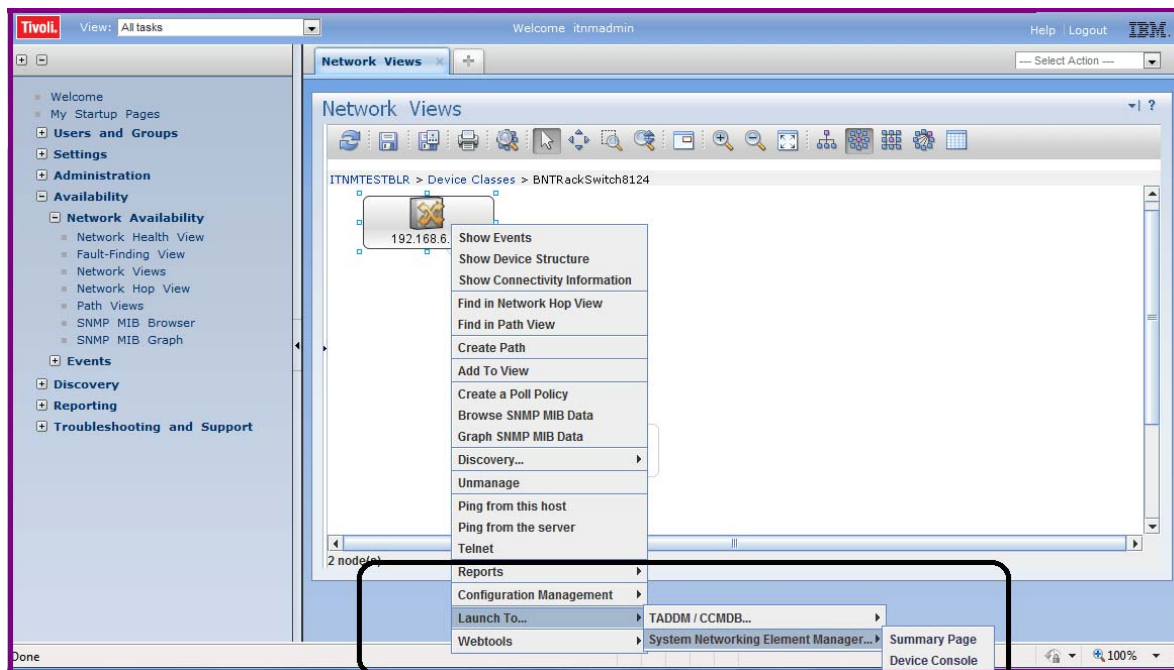
12 Repeat steps 7-11 to add other users to other System Networking Switch Center User Groups.

Note: You can add multiple System Networking Switch Center User Groups for a user. However, System Networking Switch Center selects the highest User Group privilege while launching the screens (for example, if a user is assigned with `snsadmin` and `snscooper` Groups, then System Networking Switch Center picks `snsadmin`, the highest privileged User Group, for operations).

Step 5: Edit IBM Tivoli Network Manager tools and menu configuration files

The following steps describe the configuration changes required for creating the following System Networking Switch Center launch menus (see [Figure 97](#)).

- 1 To launch System Networking Switch Center's Device Console > Monitor > Summary > Health Status page:
Right-click an IBM BLADE switch icon, and choose menu **Launch To... > System Networking Switch Center... > System Networking Switch Center > Device Console**.
- 2 To launch System Networking Switch Center's Summary page (Main page):
Right-click an IBM BLADE switch icon, and choose menu **Launch To... > System Networking Switch Center... > System Networking Switch Center > Summary Page**.

Figure 97 TIP GUI showing System Networking Switch Center launch menus

Step 5.1: IBM Tivoli Network Manager – TNM Properties

Edit Tivoli Network Manager's `tnm.properties` file to add System Networking Switch Center host information.

- 1 Login to Tivoli Network Manager system as an Administrator or root.
- 2 Open `$ITNMHOME/profiles/TIPProfile/etc/tnm/tnm.properties`.
On Linux system, the path is as follows:
`/opt/IBM/tivoli/netcool/precision/profiles/TIPProfile/etc/tnm/tnm.properties`
- 3 Add the following two properties:
`tnm.snc.serverName=<Host Name/IP address of SNSC System>`
`tnm.snc.serverPort=<HTTPs port on which SNSC is listening>`

For example, if System Networking Switch Center is running on 192.168.1.1 on HTTPs port 40443, then the following lines should be added in the `tnm.properties` file:

```
tnm.snc.serverName=192.168.1.1
tnm.snc.serverPort=40443
```

Step 5.2: IBM Tivoli Network Manager – Create System Networking Switch Center Launch-In-Context Tools Files

- 1 Create Device Specific System Networking Switch Center Launch Tools File.

Note: In this example menu, the rules are configured to launch System Networking Switch Center's **Device Console > Monitor > Health Status** tab.

Create the tools file, for example `ncp_snsc_device.xml`, under the following directory: `$ITNMHOME/profiles/TIPProfile/etc/tnm/tools`

On Linux system, the path is as follows:

```
/opt/IBM/tivoli/netcool/precision/profiles/TIPProfile/etc/tnm/tools/ncp_snsc_device.xml
```

- 2 Add the following details and save the contents of the file:

```
<ncp_tool id="ncp_snsc_device" label="Device Console" type="url">
<url value="https://{%prop:tnm.snsc.serverName}:{%prop:tnm.snsc.serverPort}/snsc/jsp/Launch.jsp"
  target="_blank" method="GET">
<parameter name="ipaddress" valueType="ncim" table="chassis" column="accessIPAddress"
  runOnMainNode="true"/>
<parameter name="sysname" valueType="ncim" table="chassis" column="sysName"
  runOnMainNode="true"/>
<parameter name="pageid" valueType="text" text="mon_sum_hs"/>
</url>
<context>
<attribute id="sysName" valueType="ncim" table="chassis" column="accessIPAddress">
<notequals value=""/>
</attribute>
</context>
</ncp_tool>
```

Refer to [“Appendix A: Externally Launching IBM System Networking Switch Center” on page 789](#) for details about `ipaddress`, `sysname` and `pageid` parameters.

Create System Networking Switch Center Summary Page (Main Page) Launch Tools File

- 1 Create the tools file, for example `ncp_snsc_main.xml`, under the following directory: `$ITNMHOME/profiles/TIPProfile/etc/tnm/tools`

On Linux system, the path is as follows:

```
/opt/IBM/tivoli/netcool/precision/profiles/TIPProfile/etc/tnm/tools/ncp_snsc_main.xml
```

2 Add the following details and save the contents of the file:

```
<ncp_tool id="ncp_snsc_main" label="Summary Page" type="url">
<url value="https://{%prop:tnm.snsc.serverName}:{%prop:tnm.snsc.serverPort}/snsc/jsp/
Launch.jsp"
target="_blank" method="GET" omitDefaultParameters="true">
</url>
</ncp_tool>
```

Step 5.3: IBM Tivoli Network Manager – Create System Networking Switch Center Launch-In-Context Menu File

Create SNSC specific LIC Menu files by providing references to System Networking Switch Center Launch Tools File created in [“Step 5.2: IBM Tivoli Network Manager – Create System Networking Switch Center Launch-In-Context Tools Files”](#) on [page 811](#).

- 1** Create the menu file, for example `ncp_snsc_lic.xml`, under the following directory: `$ITNMHOME/profiles/TIPProfile/etc/tnm/menus`

On Linux system, the path is:

```
/opt/IBM/tivoli/netcool/precision/profiles/TIPProfile/etc/
tnm/menus/ncp_snsc_lic.xml
```

- 2** Add the following details and save the contents of the file:

```
<ncp_menu id="ncp_snsc_lic" label="SNSC...">
<definition>
<tool id="ncp_snsc_device"/>
<tool id="ncp_snsc_main"/>
</definition>
</ncp_menu>
```

Step 5.4: IBM Tivoli Network Manager – Update Global Launch-In-Context Menu File

Edit Tivoli Network Manager's Global Launch-In-Context file (`ncp_wt_lic.xml`) to add the System Networking Switch Center launch-in-context menu created in [“Step 5.3: IBM Tivoli Network Manager – Create System Networking Switch Center Launch-In-Context Menu File”](#) on page 812:

- 1 Open `$ITNMHOME/profiles/TIPProfile/etc/tnm/menus/ncp_wt_lic.xml`

On Linux system, the path is:

```
/opt/IBM/tivoli/netcool/precision/profiles/TIPProfile/etc/tnm/menus/ncp_wt_lic.xml
```

- 2 Add the following line inside the `<definition>` tag:

```
<menu id="ncp_snscl_lic"/>
```

After adding the above line, the contents of the file should look somewhat similar to the below listing:

```
<ncp_menu id="ncp_wt_lic" label="Launch To...">
<context>
<attribute id="licURL" valueType="launchInContext">
<exists/>
</attribute>
</context>
<definition>
<menu id="ncp_wt_lic_sdnc"/>
<menu id="ncp_wt_lic_taddm"/>
<menu id="ncp_wt_lic_tpc"/>
<menu id="ncp_snscl_lic"/>
</definition>
</ncp_menu>
```

Step 6: Re-login to IBM Tivoli Network Manager TIP GUI

Tivoli Network Manager TIP takes couple of minutes to load the newly created System Networking Switch Center Launch-In-Context menus.

- 1 [Optional] If you are logged in to TIP GUI, logout.
- 2 Wait approximately two minutes.

- 3 Login to Tivoli Network Manager TIP GUI as a Tivoli Network Manager user belonging to an System Networking Switch Center User Group (see [“Step 4: Create System Networking Switch Center User Groups in IBM Tivoli Network Manager”](#) on page 805).
- 4 Click **Availability > Network Availability > Network Views** to open the network view showing the discovered IBM BLADE Switch (see [“Requirements”](#) on page 799).
- 5 Right-click the discovered IBM BLADE Switch and select one of the following:
 - **Launch To.. > System Networking Switch Center... > System Networking Switch Center** to launch the Device Console's Monitor > Summary > Health Status page.
 - **Launch To..> System Networking Switch Center... > System Networking Switch Center Summary Page** to launch System Networking Switch Center Summary page (Main page).

Appendix C: Integrating System Networking Switch Center with IBM Systems Director

System Networking Switch Center (SNSC) can be integrated with IBM Systems Director 6.3 and above so that System Networking Switch Center can be launched from IBM Systems Director GUI. System Networking Switch Center supports Launch-In-Context (LIC) and Single Sign-On (SSO) based launch from IBM Systems Director. This section describes various steps involved in configuring IBM Systems Director required for integrating System Networking Switch Center.

Note: Before you start working on different steps, make sure to discover the host, where System Networking Switch Center is installed, in IBM Systems Director.

Step 1: Create External App Launch Template File

The template file provides the information necessary to register an external application. A template file defines one or more external launch points for a single external application. The template file is written using JavaScript Object Notation (JSON) format.

Note: Though the template file lets you to define one or more external launch points, but it is preferable to define only one launch point per template file since IBM Systems Director uses `applicationID` and `browserWindowID` for identifying the browser window in which the application is launched. So if you define multiple launch points in a single template file, the newly launched external application replaces the previously launched external application contents in the window.

The following sample template file defines the rules for launching System Networking Switch Center's **Device Console > Monitor > Summary > Health Status, Summary Page** and **Virtualization Tools > VSI DB Console** pages:

- 1 Login as an Administrator (in case of Windows) or as root (in case of Linux/AIX) to the system where IBM Systems Director is installed.
- 2 Create the following template file in any directory. For example, you can create a file named `snsnsc.json`

```

{
  "version": "6.2.0.0",
  "type": "URI",
  "applicationID": "IBMSNSC",
  "browserWindowID": "SNSC001",
  "resolveURI": false,
  "uriBase": "https://<IBM System_Networking_Element_Manager Server
Address>:40443/snsc/jsp",
  "binding": {
    "objectType" : "Switch"
  },
  "security": {
    "ssoEnabled" : true,
    "ssoType" : "UserCredential",
    "authRegType": "LocalOS",
    "credPassing": "POST_ENCODED_TEXT",
    "userNameKey": "login-user-name",
    "passwordKey": "login-password"
  },
  "launchpoints" : [
    {
      "launchPointID" : "SNSC01",
      "displayName": [
        { "lang": "default", "text": "IBM SNSC Device Console" }
      ],
      "description": [
        { "lang": "default", "text": "IBM SNSC Device Console launch po
int" }
      ],
      "uriExtension": "/Launch.jsp",
      "uriParameters": {
        "encoding": "base64",
        "pageid": "mon_sum_hs",
        "ipaddress": "{Switch.DeviceName}"
      }
    },
    {
      "launchPointID" : "SNSC02",
      "displayName": [
        { "lang": "default", "text": "IBM SNSC Summary" }
      ],

```



```

    "description": [
      { "lang": "default", "text": "IBM SNSC Summary launch point" }
    ],
    "uriExtension": "/Launch.jsp",
    "uriParameters": {
      "encoding": "base64",
    }
  },
  {
    "launchPointID" : "SNSC03",
    "displayName": [
      { "lang": "default", "text": "IBM SNSC VSI Manager" }
    ],
    "description": [
      { "lang": "default", "text": "IBM SNSC VSI Manager launch point"
    " }
    ],
    "uriExtension": "/Launch.jsp",
    "uriParameters": {
      "encoding": "base64",
      "pageid": "vsi_manager"
    }
  },
],
}

```

Table 362 Template File field descriptions

Field	Type	Required	Description
version	String	Yes	Value representing the version of the template schema used to define the launch points. This value coincides with the version of the SDK where the template schema is defined.
type	String	Yes	Value representing the type of launch points defined. Valid values are: URI

applicationID	String	Optional	<p>Application identifier for the grouping of launch points defined in the template file. This unique value is used as a reference for IBM® Systems Director when performing internal operations. The applicationID/launchPointID combination must be unique among all registered launch points. Specifying this value is optional; if it is not specified, a unique applicationID will be generated dynamically. If a specified applicationID already exists, registration will fail and an error will be returned.</p> <p>Note: Application ID string cannot contain a blank (white) space character.</p>
browserWindowID	String	Optional	<p>An ID to associate the browser window to use for the launch point. Launch points with the same browserWindowID will be launched into the same browser window. If this value is not defined, it will be automatically generated such that all launch points for given application will share the same browser window. In addition, if resolveURI is true, then unless specified, all launch points for a given targeted managed resource will share the same browser window.</p>
resolveURI	Boolean	Optional	<p>Indicates if the launch point URI value should be resolved before launching. Resolving the URI involves replacing the variable {hostname} with the targeted resource hostname value. This value can only be true if the launch point URI has the variable {hostname} included in it, and the launch point has binding information specified (making it targeted). If this value is false, the launch point URI is launched as is.</p>
uriBase	String	Yes	<p>The base URL to the external Web-based application associated with this launch point. This value cannot include the "?" character. This value can have the following special substring included as part of its value: {hostname}. If the {hostname} substring is included, the launch point must be targeted (by specifying a binding). The uriBase value will be concatenated with the uriExtension to form the final URI value. NOTE: This value is overridden if a fully qualified uriExtension value is defined for a launch point. See uriExtension information for more details.</p> <p>Note: If security is enabled, the endpoint represented by the hostname included in the uriBase value must be discovered and managed by IBM Systems Director.</p>
binding	Object	Yes	<p>Launch points defined in template can be associated with resources in IBM® Systems Director environment using binding criteria.</p>

objectType	String	Yes, if binding is present	Part of the binding specification, this value identifies the objectType value within IBM Systems Director this launch point is bound to. Example: OperatingSystem. This value must be a valid ObjectType as defined by the IBM Systems Director Data Model. By specifying this value, the launch point(s) associated with this objectType binding become targeted. The binding specification can be specified at the application level (in effect for ALL launch points defined) or at the individual launch point level. If this binding value is specified at the launch point level, it overrides the value defined at the application level.
security	Object	Yes	Defines the security credentials for the application launch.
ssoEnabled	Boolean	Yes, if SSO is enabled	Indicates whether SSO is enabled for all launch points.
ssoType	String	Yes	The SSO credential type. Valid values are: UserCredential
authRegType	String	Optional	The type of authentication registry to use for authentication. Valid values are as follows: <ul style="list-style-type: none"> LocalOS - Local OperatingSystem registry LDAP - Lightweight Directory Access Protocol registry DOMAIN - Windows Active Directory (DOMAIN) registry
credPassing	String	Optional	The technique used to pass credentials (username and password). The username is always passed URLEncoded using UTF-8 encoding. The password is encoded using base64 encoding whenever POST_ENCODED_TEXT is specified. The password is sent URLEncoded using UTF-8 encoding whenever POST_PLAIN_TEXT is specified. Allowed values are as follows: <ul style="list-style-type: none"> POST_PLAIN_TEXT - Indicates username and password be sent as part of the HTTP request header when launching the external application. POST_ENCODED_TEXT - Indicates username and password (base64 encoded) be sent as part of the HTTP request header when launching the external application.
userNameKey	String	Optional	The key to associate with the username value when passing information to the launch point application. The username key and value are passed either as part of the query string or as a variable in the HTTP POST message.
passwordKey	String	Optional	The key to associate with the password value when passing information to the launch point application. The password key and value are passed either as part of the query string or as a variable in the HTTP POST message.
launchpoints	Object	Yes	An array of launch points to the application.

launchPointID	String	Yes	Unique name/ID for a specific launch point entry. This value is used as a reference for IBM Systems Director when performing internal operations. The applicationID/launchPointID combination must be unique among all registered launch points. If a specified launchpointID already exists under a given applicationID, registration will fail and an error will be returned.
displayName	String	Yes	An array of localized text representing the display name for the launch point. The default text value must be specified; all other supported languages are optional.
description	String	Optional	An array of localized text representing the description for the launch point. The primary intent of this field is to enable an administrator to understand the purpose of the launch point, as the display name may not fully describe the intent of the entry. The default text value must be specified; all other supported languages are optional.
uriExtension	String	Optional	The string to concatenate to the base URL defined by uriBase to form the fully qualified URI value. This value cannot include the ? (question mark) character. If the value is a fully qualified URL (example: <code>http://<address></code>), then the uriBase value is disregarded and the uriExtension becomes the fully qualified URI for the launch point.
uriParameters	String	Optional	<p>A list of parameters values to be passed to the launch point application. The parameters themselves are specified in the format "key" : "value", where key is the parameter name and value is the parameter value. Parameter values are passed URLEncoded using UTF-8. Options for the parameter value are as follows:</p> <ul style="list-style-type: none"> • Static: A static parameter value is passed as-is to the launch point application. This parameter has the same value regardless of targeted resource. • Dynamic: A dynamic parameter value is resolved at runtime using data from IBM Systems Director. The parameter value is based on the context of the targeted resource.

encoding	String	Yes	<p>Determines whether the credentials are encoded or not. Possible values are as follows:</p> <ul style="list-style-type: none"> • plain: If 'credPassing' in security object is defined as POST_PLAIN_TEXT • base64: If 'credPassing' in security object is defined as POST_ENCODED_TEXT <p>Note: The encoding field should be set by the user, depending on the type of credPassing setting. Make sure you assign the correct value. For example, if credPassing is set to POST_PLAIN_TEXT, but encoding is set to base64, the authentication will fail.</p>
pageid	String	Yes	<p>Indicates the page/tab in SNSC's UI to be launched. For various pageid mappings, refer to “Appendix A: Externally Launching IBM System Networking Switch Center” on page 789.</p>
ipaddress	String	Yes, if device-specific page is the launch point	<p>If the external application launch should be associated with the IP address/device address, this field should be set to {Switch.DeviceName}, which enables IBM Systems Director to pass either the IP address or the sysName assigned to the selected device.</p>

Step 2: Register External App Launch Template File

The template file created in [“Step 1: Create External App Launch Template File” on page 815](#) should be registered with IBM Systems Director. You can register the template file using IBM Systems Director's `smcli` command utility.

To register the template file:

- 1 Login as an Administrator (in case of Windows) or as root (in case of Linux/AIX) to the system where IBM Systems Director is installed and the template file was created.
- 2 Register the template file:

```
smcli importextlps -f <template file path>
```

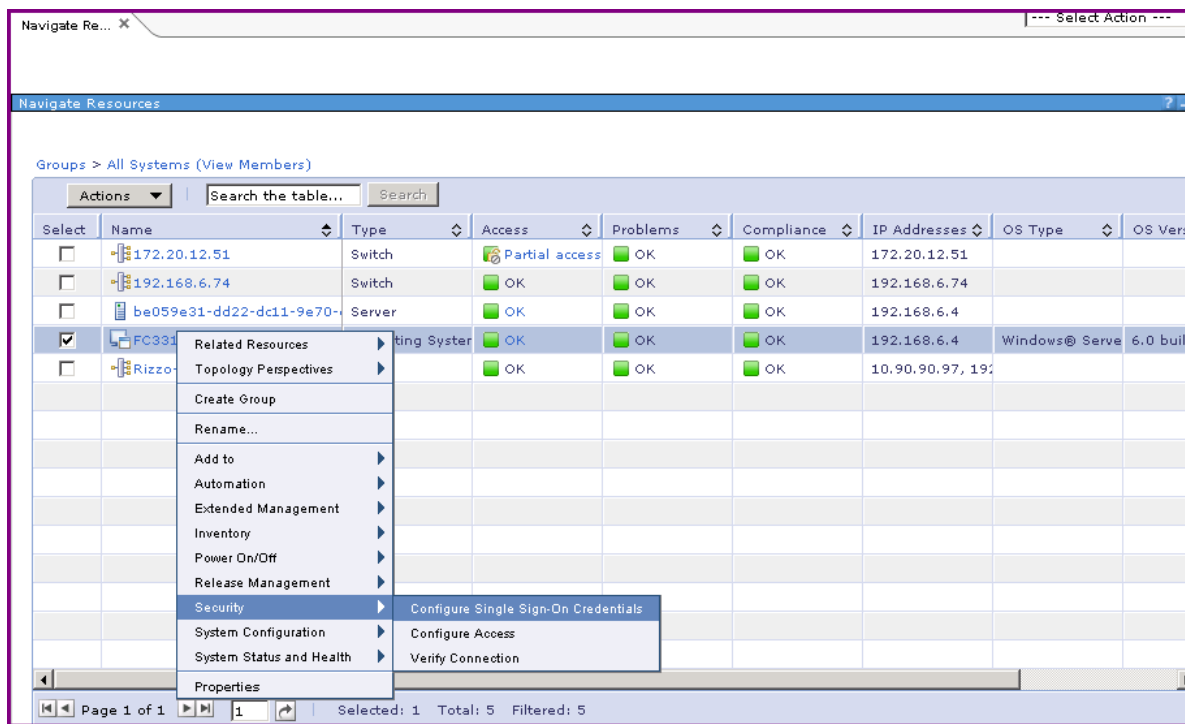
Note: You can view the registered launch points by executing the following command: `smcli listextlps`

Note: You can remove (unregister) an external launch point by executing the following command: `smcli removeextlps -A <applicationID>`

Where *<applicationID>* is the ID used in the template JSON file.

Step 3: Configure Single Sign-On Credentials

- 1 Login to IBM Systems Director.
- 2 From the task list in the left pane, select **Navigate Resources**.
- 3 From the Groups table on the Navigate Resources tab, select **All Systems**.
- 4 In the **Group > All Systems** table, right-click the IBM System Networking Switch Center server entry.
- 5 Choose menu **Security > Configure Single Sign-On Credentials**.



- 6 Right-click the entry that contains the Access Information:
<http://<IBM System Networking Switch Center IP>:<Port>/snsc/jsp>

7 Choose menu **Credential**.

To perform advanced systems management function on the selected system, a single sign-on credentials must exist for the Systems Director Web Interface user to the remote service access point for the system. The single sign-on credential is a mapping that must exist between the web interface user, and a user profile on the target system. These credential mappings allow access to the additional function on that remote service access point for the system.

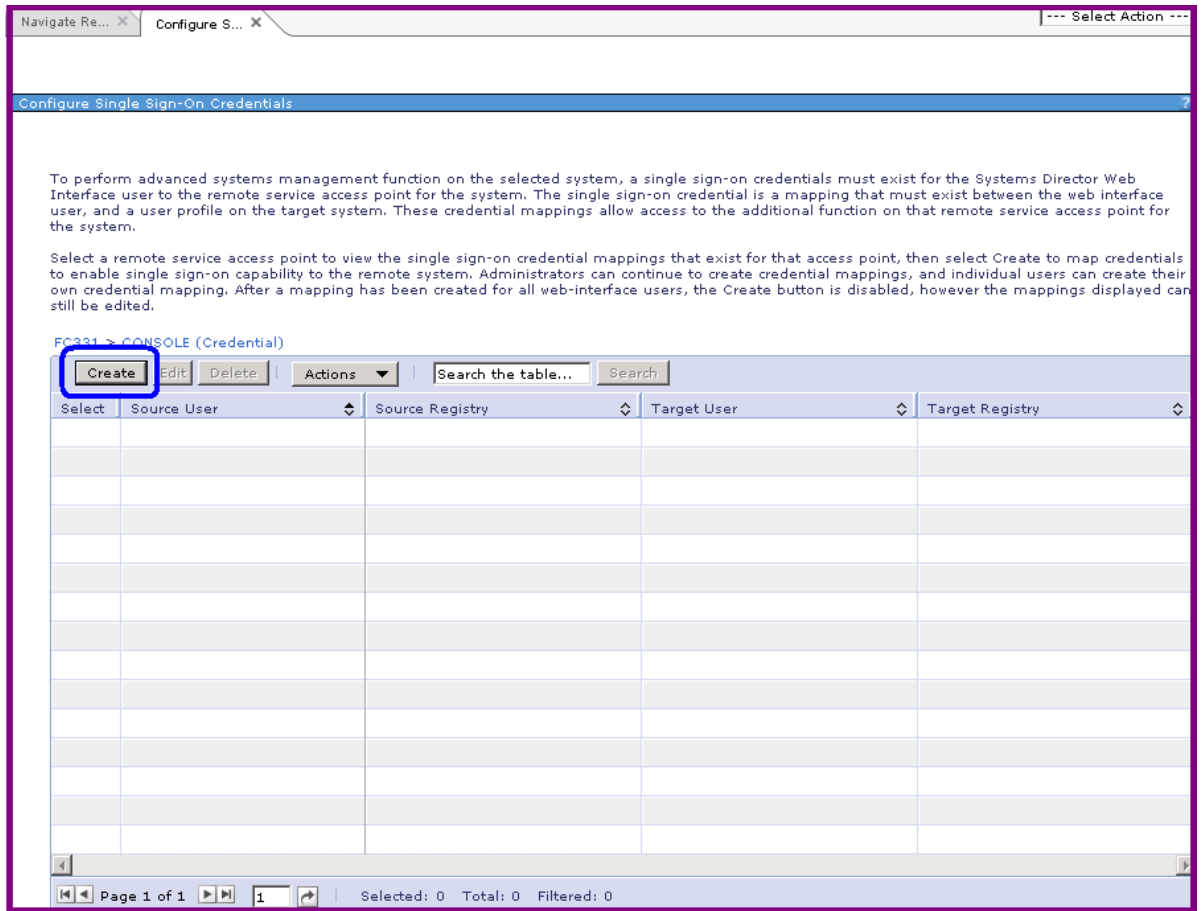
Select a remote service access point to view the single sign-on credential mappings that exist for that access point, then select Create to map credentials to enable single sign-on capability to the remote system. Administrators can continue to create credential mappings, and individual users can create their own credential mapping. After a mapping has been created for all web-interface users, the Create button is disabled, however the mappings displayed can still be edited.

FC331 (Remote Service Access Point)

Configure Authentication Registry					
		Actions ▼	Search the table...		Search
Select	Name	Access Information	Port		
<input checked="" type="radio"/>	CONSOLE	Credential	http://192.168.6.47:40080/bhm/jsp	40,080	
<input type="radio"/>	CONSOLE	Create Group	http://192.168.6.4/java/console	80	
<input type="radio"/>	CONSOLE	Remove...	http://192.168.6.47/java/console	80	
<div>Add to ▶</div>					

Page 1 of 1 | Selected: 1 Total: 3 Filtered: 3

8 Click Create.



9 Click Next.

- 10 Type the user ID and password with the values of the Login ID and Password fields of the user account configured in System Networking Switch Center.

11 Click Next.

Navigation: Navigate Re... | Configure S... | Create and ... | --- Select Action ---

Create and Edit Single Sign-on Credentials

✓ Welcome
 ➔ Create Single Sign-on Credential
 Assign to IBM Systems Director User
 Summary

Create Single Sign-on Credential

Enter a valid user ID and password for system FC331

Authentication registry type: Local OS

*User ID: admin

*Password: *****

*Verify password: *****

< Back Next > Finish Cancel

12 Do not modify the default Use current user option.**13 Click Next.****14 On the Summary page, click Finish.**

Navigation: Navigate Re... | Configure S... | Create and ... | --- Select Action ---

Create and Edit Single Sign-on Credentials

✓ Welcome
 ✓ Create Single Sign-on Credential
 ➔ Assign to IBM Systems Director User
 Summary

Assign to IBM Systems Director User

Assign the previously created credentials to a known IBM Systems Director user.

☒ Use current user - FC331\Administrator
☐ Choose a different user

Select	Name	Registry Type : Name	Type
<input type="radio"/>	admin	Local OS : FC331	User ID and Password
<input type="radio"/>	FC331\Administrator	Local OS : FC331	User ID and Password
<input type="radio"/>	oper	Local OS : FC331	User ID and Password
<input type="radio"/>	oper	Local OS : FC331	User ID and Password

Page 1 of 1 1 Selected: 0 Total: 12 Disabled

< Back Next > Finish Cancel

Appendix D: Using Third-Party JDBC/ODBC Tools for Querying SNSC Database

System Networking Switch Center component uses IBM Derby database for data storage and IBM Derby is configured to run in Network Server mode, which enables accessing SNSC DB through multiple connections. This section describes the steps that can be used for retrieving the data from SNSC Database using third-party JDBC/ODBC tool such as EasySoft ODBC-JDBC Gateway.

Note: The steps given in this section pertains to 3rd party tools installed on Microsoft Windows XP/7 OS.

Requirements

- Java Runtime Environment (JRE) 1.5 or above installed.
- EasySoft ODBC-JDBC Gateway v 2.3 for Microsoft Windows platform (http://www.easysoft.com/products/data_access/odbc_jdbc_gateway/index.html) installed.
- ODBC Test Utility (<http://media.datadirect.com/download/files/Tools/odbctest.zip>) is installed. Note that ODBC Test Utility is packaged as a Windows Zip file. Extract the contents of the zip file to install ODBC Test Utility.
- IBM Derby client JAR file copied to a directory on the system where you have installed EasySoft ODBC-JDBC Gateway. You can find IBM Derby client (`derbyclient.jar`) under the following directory:
<SNSC Installation Directory>/derby/lib/

Task 1: EasySoft ODBC-JDBC Gateway – Configuring JVM

- 1 Click **Start > Programs > EasySoft > ODBC-JDBC Gateway > Configure Java Interface** to open the Setup Java Interface window.
- 2 Set the JVM Library path.

- a Click the elipsis button (...) next to JVM Library path text field to open the Select JVM window.
- b By default, Select JVM window lists the known JVM libs (<Java Install Path>\bin\client\jvm.dll). You can also click the **Browse** or **Search** buttons to find other JVM library paths.
- c Select the appropriate JVM library by double-clicking the listed library path.
- d (Optional) Click **Test** and **Save if OK** button to test the selected JVM library and save only if the test was successful.
- e Click **OK** to save the changes.

Task 2: EasySoft ODBC-JDBC Gateway – Configuring Data Source (DSN)

- 1 Select **Start > Control Panel > Administrative Tools** and click **Data Source (ODBC)** to open the ODBC Data Source Administrator window.
- 2 Select System DSN tab and click **Add...** to open the Create New Data Source window.
- 3 Select **EasySoft ODBC-JDBC Gateway** option and click **Finish** to open the EasySoft ODBC-JDBC Gateway DSN Setup window.
- 4 In EasySoft ODBC-JDBC Gateway DSN Setup window, complete the fields as follows and then click **OK**.
 - a DSN
Enter the DSN name for this entry. For example, SNSC DB.
 - b Description
(Optional) Enter any descriptive text.
 - c Driver Class
Specify the IBM Derby network driver class
(`org.apache.derby.jdbc.ClientDriver`)
 - d Class Path
Specify the patch where you have copied IBM Derby client JAR file (see ["Requirements" on page 827](#)).

For example, if IBM Derby client JAR (`derbyclient.jar`) is located under `c:\tools\derby\` directory, then type `c:\tools\derby\derbyclient.jar`

- e URL
Specify the SNSC DB URL as follows:

```
jdbc:derby://<SNSC Host IP Address>:41527/<SNSC Install
Path>/database/snsc;create=false
```

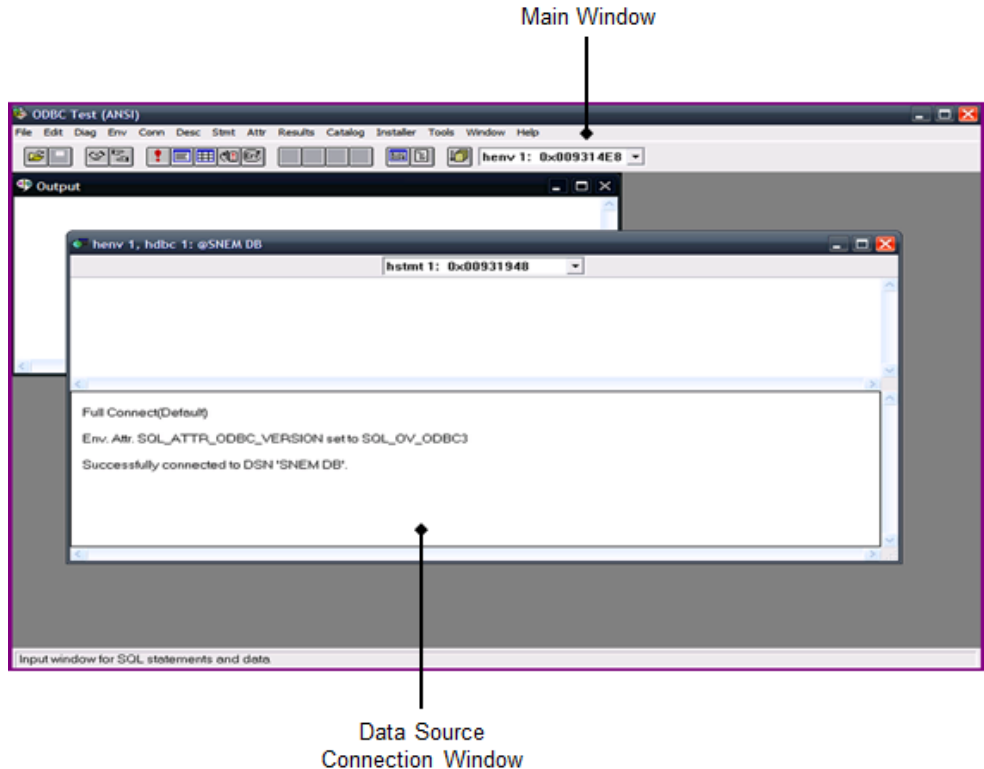
For example, if SNSC is installed on RHEL 5.0 system 192.168.1.1, enter:

```
jdbc:derby://192.168.1.1:41527//opt/ibm/snsc/database/
snsc;create=false
```

- 5 Once the Data Source is created and listed, click **OK** to complete.

Task 3: ODBC Test Utility – Connecting to Data Source

- 1 Navigate to the directory in which you have extracted ODBC Test Utility contents.
- 2 Double-click `OdbcTE32.exe` to bring ODBC Test Utility window.
- 3 Select **Conn > Full Connect...** to bring up Full Connect window.
- 4 In Full Connect window, select the ODBC datasource (for example, SNSC DB) that you created (see [“Task 2: EasySoft ODBC-JDBC Gateway – Configuring Data Source \(DSN\)” on page 828](#)).
- 5 Click **OK** to establish the connection with the database. A successful connection to Data Source brings up another window (see [Figure 98](#)) enabling you to execute database queries.

Figure 98 ODBC Test Utility window

Task 4: ODBC Test Utility – Retrieving the Data from the Database and Viewing

After successfully establishing the connection with the Data Source, you can retrieve and view the data using the following steps:

- 1 In Data Source Connection Window's upper panel (see Figure 98), enter the SQL query associated with the DB table you want to query.

For example, to retrieve and view all the data from the Device table, type `select * from Device`.

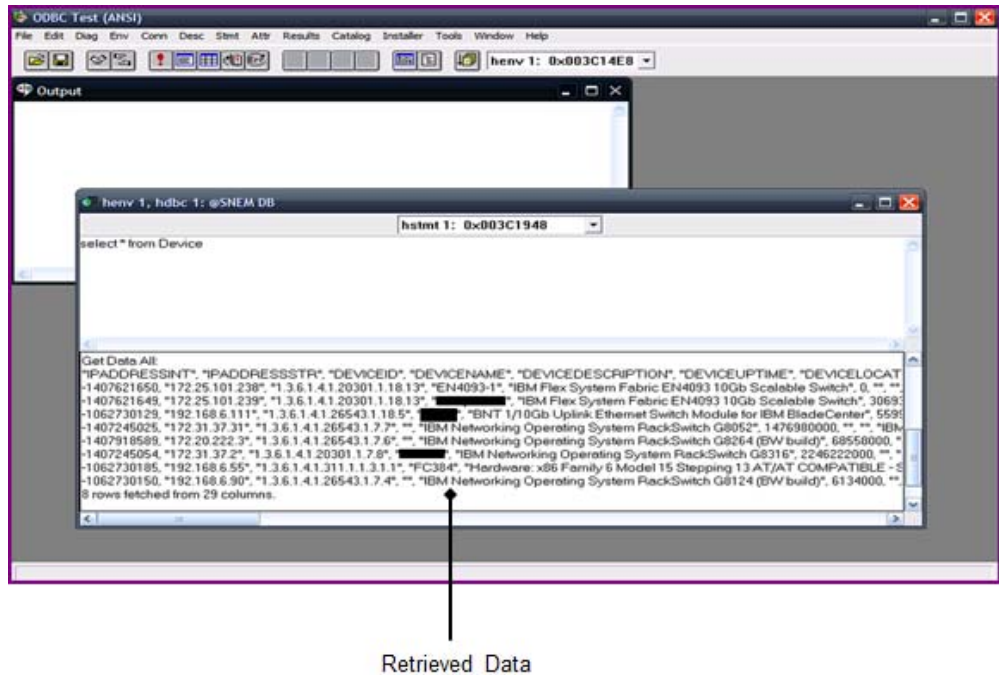
Note: Refer to the following file for complete list of database tables used by SNSC for storing the data: `<SNSC Install Path>/database/snsedb.sql`

- 2 In the Main Window (see Figure 98), select **Stmt>SQLExecDirect...** to execute the SQL statement.

- 3 In the Main Window, choose menu **Results > Get Data All** for listing the retrieved data (see Figure 99).

Note: You can also view the data in tabular format. For details, you can refer ODBC Test Utility documents.

Figure 99 ODBC Test Utility window with retrieved data



Index

A

- ACL Groups 570
- ACL VMAPs 574
- ACLs 567
- Actions (device-specific) 689
- admin, oper and user passwords 38
- Administrator 42
- Alerts report 162
- Apply 694
- apply configuration 197
- applying configuration changes 377
- authentication 108
- Auto Discovery 47
- auto discovery configuration tasks 48
- Auto Discovery Log 52

B

- backup firmware 184
- Bandwidth configuration (VMs) 602
- BBI 697
- Browser-Based Interface 697

C

- CEE (Converged Enhanced Ethernet) 580
- Chart 204
- chart statistics 366
- CIST Bridge 425
- CIST Port 426

- Clear Counter 204
- Clear Statistics 204
- CLI commands 191
- collect data 193
- concurrent limit setting 179
- Config Dump 694
- configuration
 - ACL Groups 570
 - ACLs 567
 - applying changes 377
 - Auto Discovery 47
 - CIST Bridge 425
 - CIST Port 426
 - FDB 434
 - FDB Static 435
 - firmware 382
 - general 380
 - LACP 415
 - LACP Ports 416
 - LACP trunk groups 413
 - Management Network 401
 - MSTP 423
 - NTP service 399
 - Port Mirroring 402
 - Ports 550
 - RADIUS General 390
 - RADIUS Server 391
 - RSTP 423
 - saving 377
 - STP 428
 - STP Groups 431
 - STP Port 432
 - submitting changes 377
 - synchronizing 690

- Syslog Hosts 384
- TACACS General 393
- TACACS+ Server 394
- TACACS+ User Map 396
- Trunk groups 412
- Trunk hash 411
- Virtualization 598
- VLAN Memberships 447
- VM Bandwidth 602
- VM Groups 601
- VM Ports 605
- VM Pre-Provisioning 607
- VM profiles 600
- VMAPs 451, 452
- VMs 606
- VMware vCenter 599
- configuring the switch 371
- Converged Enhanced Ethernet (CEE) 580
- CSV file
 - exporting 60
 - importing 56

D

- data collection 104, 193
- database purge 106
- Default Passwords 42
- Delete Switch 694
- Device Console page 87
- Device List
 - importing 57
- Device List page 71
- Device List pane 74
- Device-Specific Actions 689
- Diff Config 694
- Diff Flash 694
- disk space 1
- Domains pane 72
- download configuration file 185
- Downloads window 369

E

- Enabling JavaScript 3
- Exclude Address Range 50
- Export 204
- export statistical data 368

F

- FCoE (Fiber Channel over Ethernet) 591
- FDB 434
- FDB Static 435
- Fiber Channel over Ethernet (FCoE) 591
- Filter Type 49
- Firmware configuration 382
- firmware download 180
- Form pane 374
- Forwarding Database 434
- FTP configuration 114

G

- General configuration 380
- group operations 179

H

- Help 204
- home page 63
- HTTP 4
- HTTPs 4

I

- image download 180
- information
 - general 132
- IP address 3

J

JavaScript 2

L

LACP 415

LACP Ports 416

LACP trunk groups 413

Launching the BBI 697

Levels of Severity 386

Link Layer Discovery Protocol 453

LLDP 453

log archive 134

log viewer 134

M

maint_critical_data_backup_dir_setup 701

maint_critical_data_backup_init 702

Management Network 401

Manual Discovery 54

menu bar

Device Console page 92

Device List page 76

Microsoft Internet Explorer 2

monitored port 402

Mozilla Firefox 2

MSTP 423

multi-homed system configuration 36

N

NTP Service 399

O

Operator 42

P

panic dump 187

Port 204

Port Bridge

monitoring 242

Port configuration 550

Port Ethernet Statistics

monitoring 243

Port Group (VMready) 651

Port Mirroring 402

port monitor 402

Port Synchronization 692

Port Trunk Groups 412, 413

Pre-provisioning 607

Print 204

print statistical summary 370

properties

general 101

R

RADIUS general 390

RADIUS Server 391

RAM 1

Read Community 49

Reboot Switch 694

Refresh 204

refresh configuration 103

reports

viewing 161

RESTful API 661

Retries 49

Revert 694

Revert Apply 694

RMI Service 4

RSTP 423

S

Save 694

save configuration 197

- [saving the configuration](#) 377
- [scheduled jobs](#) 189
- [Selection windows](#) 376
- [severity levels](#) 386
- [SNMP access](#) 3
- [SNMPv1](#) 3
- [software download](#) 180
- [Spanning Tree](#) 428
- [Spanning Tree Groups](#) 431
- [Spanning Tree Port](#) 432
- [static FDB](#) 435
- [statistical data export](#) 368
- [Statistical Summary](#) 368
- [statistics chart](#) 366
- [STP](#) 428
- [STP Groups](#) 431
- [STP Port](#) 432
- [submitting configuration changes](#) 377
- [Subnet](#) 50
- [Subnet Mask](#) 50
- [subnet mask range](#) 49
- [Summary Status window](#) 73
- [switch summary](#) 209
- [switch version report](#) 164
- [Sync Config](#) 690
- [synchronizing the configuration](#) 690
- [Syslog Dump](#) 694
- [Syslog Hosts](#) 384
- [Syslog severity levels](#) 386
- [System Networking Switch Center home page](#) 63
- [system requirements](#) 1

T

- [Tabular pane](#) 375
- [TACACS general](#) 393
- [TACACS+ Server](#) 394

- [TACACS+ User Map](#) 396
- [tech support dump](#) 188
- [TFTP configuration](#) 114
- [Timeout](#) 48
- [transceiver information report](#) 166
- [Trunk groups](#) 412
- [Trunk hash](#) 411

U

- [upgrade configuration file](#) 185
- [upgrade firmware](#) 182
- [Use SNMPv3](#) 54
- [User](#) 42
- [User Map \(TACACS+\)](#) 396

V

- [vCenter](#) 628
- [vCenter Access](#) 599
- [Virtual Machines](#) 635
- [Virtual Machines configuration](#) 606
- [Virtual Machines discovered](#) 349
- [Virtual Switch Instance \(VSI\)](#) 661
- [virtualization](#) 598
- [VLAN Maps \(VMAPs\)](#) 640
- [VLAN Memberships](#) 447
- [VLAN Synchronization](#) 692
- [VM](#) 606
- [VM Bandwidth](#) 602
- [VM configuration](#) 598
- [VM Data Center Report](#) 168
- [VM Groups](#) 601, 633
- [VM management server](#) 628
- [VM Ports](#) 605
- [VM pre-provisioning](#) 607
- [VM profiles](#) 600
- [VMAP](#) 451, 452, 574

- VMAPs (VLAN Maps) 640
- VMready VM Reports 170
- VMready Wizard 621
- VMs (virtual machines) 635
- VMs discovered 349
- VMware 599
- vNIC configuration 608
- vNIC groups 610
- VSI Database 661

W

- web session 697
- Wizard
 - VMready 621
- Write Community 49

