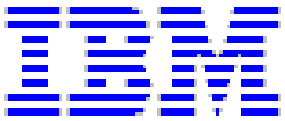


Whitepaper

Enabling and Configuring BladeCenter Chassis Internal Network (CIN)

Document owner: Binh Nguyen
Revision Level: 7.1
Last Revised: 4 August 2008

Table of Contents

1 Introduction

This white paper explains how to enable and configure the BladeCenter Advanced Management Module (AMM), various I/O modules, and blade device operating systems (OS) that are required to enable the Chassis Internal Network (CIN).

There are a number of steps that must be taken to enable and to configure CIN to work properly:

- The AMM firmware must be updated to level BPET35x or higher and configured.
- The I/O modules (IOMs) must have their Virtual Local Area Network (VLAN) configuration set up correctly.
- The blade device OS must be manually configured.

This white paper provides details on hardware and software requirements, as well as, step-by-step instructions to configure each component. It is imperative that all steps outlined in this document are followed closely and completely to ensure CIN functionality.

The following components were used during the development of this white paper:

- AMM
- Cisco Systems Intelligent GB Ethernet Switching Module (ESM, also known as an IOM).
- Nortel Layer 2/3 GbE Ethernet Switching Module (ESM, also known as an IOM)
- Type 8832 HS20 blade server running SUSE Linux Enterprise Server 9 for x86
- Type 8843 HS20 blade server running Red Hat Enterprise Linux 2.6.9-5.Elsmp
- Type 8832 HS20 blade server running Microsoft Windows Server 2003

Instructions for setting up other IOMs and blade device OSs are also provided.

Note:

1. **The CIN feature is also supported on the BladeCenter Telco Chassis Management Module 2 (CMM2). All the instructions that are written for the AMM can also be used to set up the CMM2.**
2. **All user input from a Telnet session to the AMM, IOM, or X Windows is underlined.**

2 Overview

The CIN feature creates an internal communication path between the blade devices and the AMM or CMM2. When CIN is enabled and configured properly, the AMM and CMM2 can fully utilize all the resources such as LDAP, SMTP, Director, SNMP, DNS, or NTP services installed on the blade devices. Conversely, the blade devices can directly connect to the AMM via the CIN path.

As the name implies, the communication path is internal to the BladeCenter unit and is on a private user-defined VLAN. This means that the communication path cannot be hacked or "snooped" and is therefore is very secure.

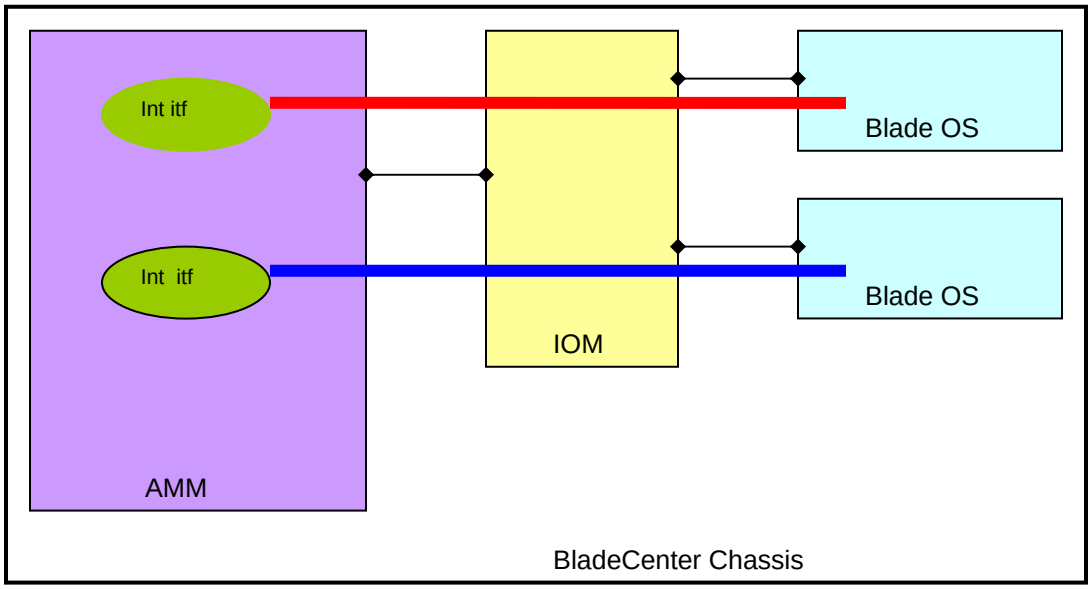


Figure 1: Diagram of Chassis Internal Network from blade device OS to AMM

The CIN feature is not bay dependent. The AMM can be in either bay 1 or 2, provided that the AMM is active. An IOM can be in any IOM bay as long as it has network connectivity to the AMM and blade devices. A blade device can be in any blade bay as long as it has network connectivity to at least one of the IOMs that supports CIN.

3 Hardware and software requirements

The AMM firmware must be at level BPET35x or higher. The CIN feature is not supported by the original BladeCenter Management Module (MM).

The IOMs must support custom VLAN configuration. The following IOMs provide this support:

- Cisco Systems Intelligent GB Ethernet Switch Module (part numbers 13N2281 and 32R1892 for copper and part numbers 26K6547 and 32R1888 for fibre).
- Nortel Layer 2/3 GbE ESMs (part numbers 32R1860 and 26K6530 for copper and part numbers 32R1861 and 26K6531 for fibre) with firmware level 1.4.2 or later

Any blade device that runs any version of any OS (Windows, Linux, etc.) that supports VLAN Configuration should work. The following OSs were used to write this document:

- Red Hat Enterprise Linux 4 with kernel version 2.6.9-5.Elsmp
- SUSE Linux Enterprise Server 9 for x86
- Microsoft Windows Server 2003

4 AMM configuration

Assumptions:

- You already know how to update the AMM firmware.
- You already know how to configure the AMM External Network Interface (Ethernet port).
- You already know how to establish a Telnet session from a client or workstation to the AMM.

4.1 AMM external network interface

The IP address for the external network interface on the AMM can be configured either statically or obtained from DHCP. During the development of this document, the IP address was statically configured.

Below is the configuration that was used during the development of this document. This information will be used as reference and in examples.

IP address:	192.168.70.125
Subnet mask:	255.255.255.0
Gateway:	0.0.0.0

4.2 CIN configuration

Configuration of the CIN feature has the following characteristics:

- The CIN feature can be globally enabled or disabled. When CIN is enabled, the communication path between blade devices and the AMM is open. When CIN is disabled, this communication path is shut down. CIN is globally disabled by default.

- There are a maximum of 14 CIN pairs, each pair consisting of a valid IP address and VLAN ID that can be configured. An IP address of 0.0.0.0 is valid and designates that dynamic host learning is enabled on this VLAN interface. Dynamic host learning is the ability for the AMM to communicate back to blade device OS without having to configure a specific CIN address pair; thus, static configuration of a CIN pair for a specific IP address is not required.

- Each CIN pair can be added, deleted, changed, enabled, or disabled individually. This change will take effect immediately without rebooting the AMM.

- The CIN VLAN ID must be between 3 and 4094 and cannot be the same as the SOL, concurrent KVM (cKVM), or other standard IDs being used by the IOMs.

- In addition to the 14 configured entries, dynamic host learning can learn up to 34 entries.

4.2.1 CIN-pair entry for a specific host IP address

A CIN-pair entry for a specific host consists of a valid VLAN ID and an IP address. For example,. a VLAN ID of 4000 and an IP address of 9.9.9.1. When this entry is configured, the AMM will create a host route to this host on the VLAN 4000 interface.

Below is the configuration that was used during the development of this document and will be used as reference and in examples. The IP address for the CIN pair does not have to be in the same subnet as the IP address of the AMM.

VLAN ID:	4000
IP address:	9.9.9.1

You can use either the management module Web interface, Command-Line Interface (CLI), or SNMP to configure the CIN feature. The following sections contain procedures for the management module Web interface and CLI.

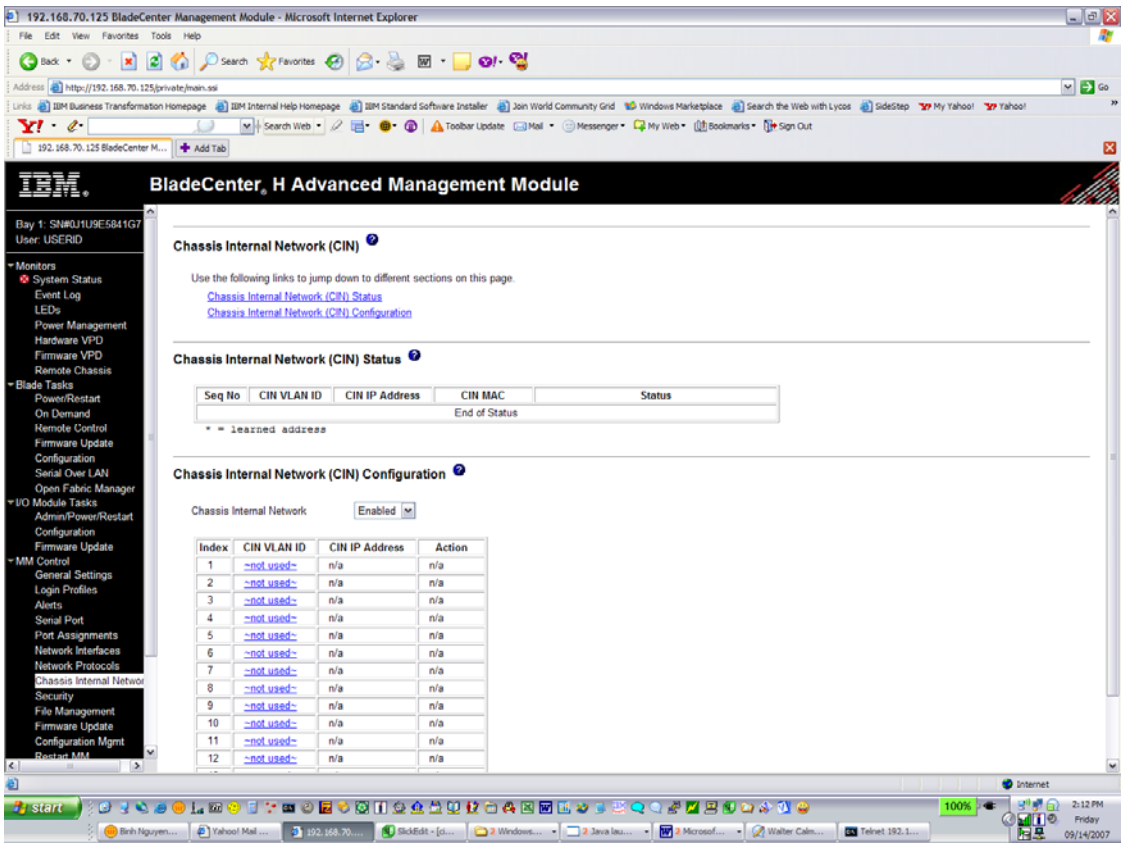
4.2.2 Configuring CIN using the Web interface

Complete the following steps to configure the CIN feature using the management module Web interface:

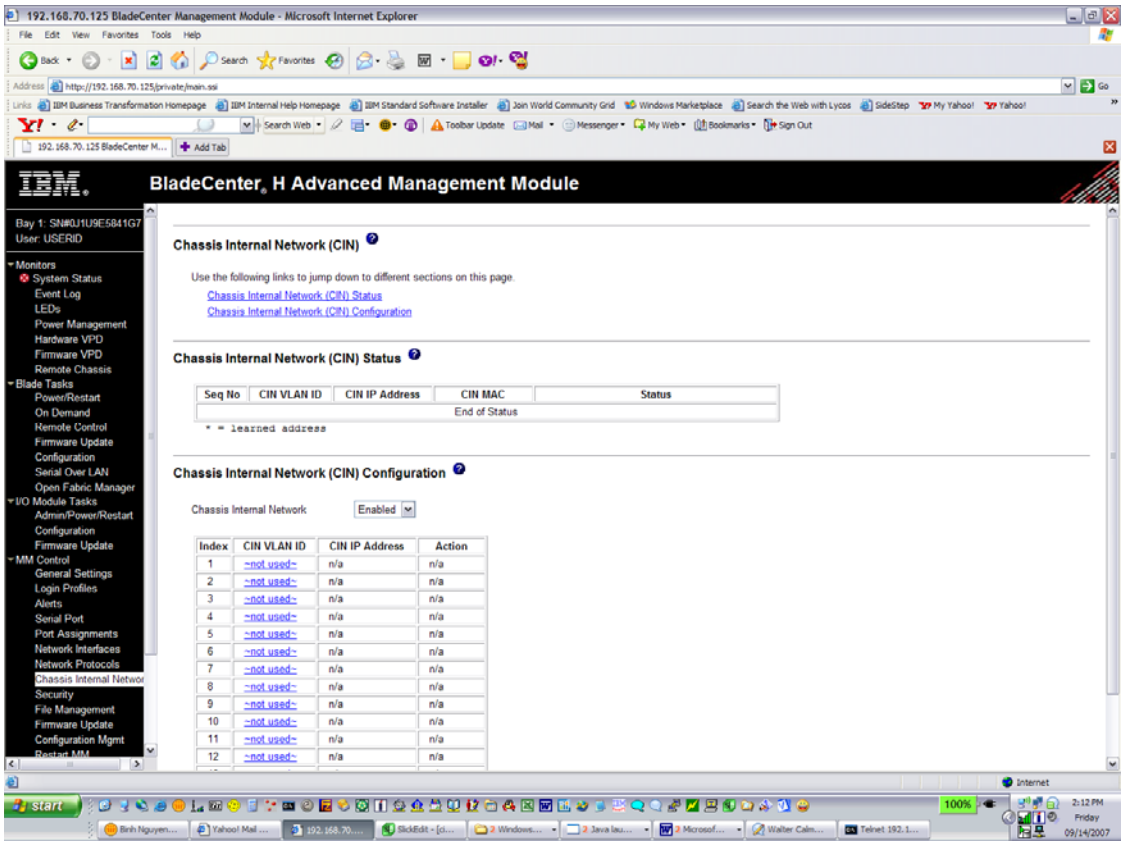
1. Open an http or https session to the AMM. The factory-defined static IP address of the management module is 192.168.70.125.

2. When prompted, enter the appropriate user ID and password.

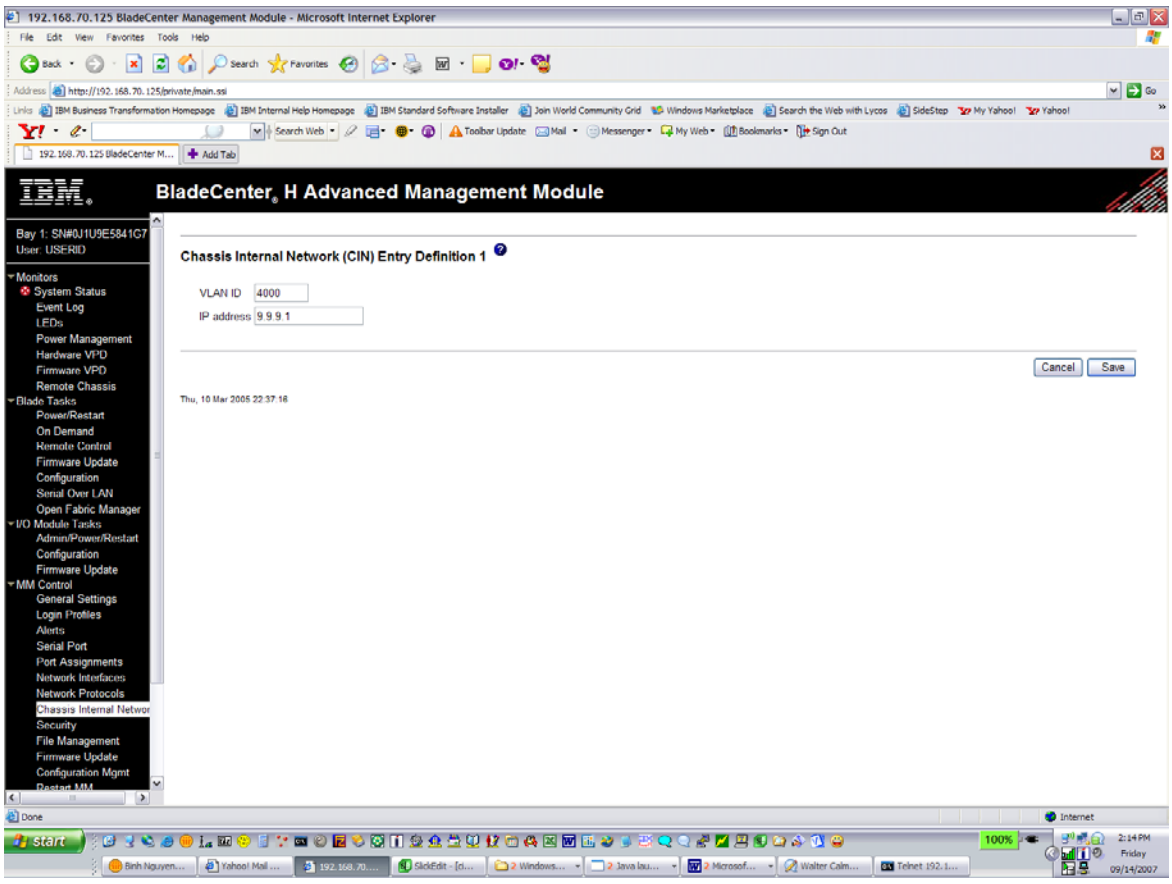
3. To display the current CIN configuration, click on **Chassis Internal Network**. The following page is displayed, indicating that the Chassis Internal Network is disabled.



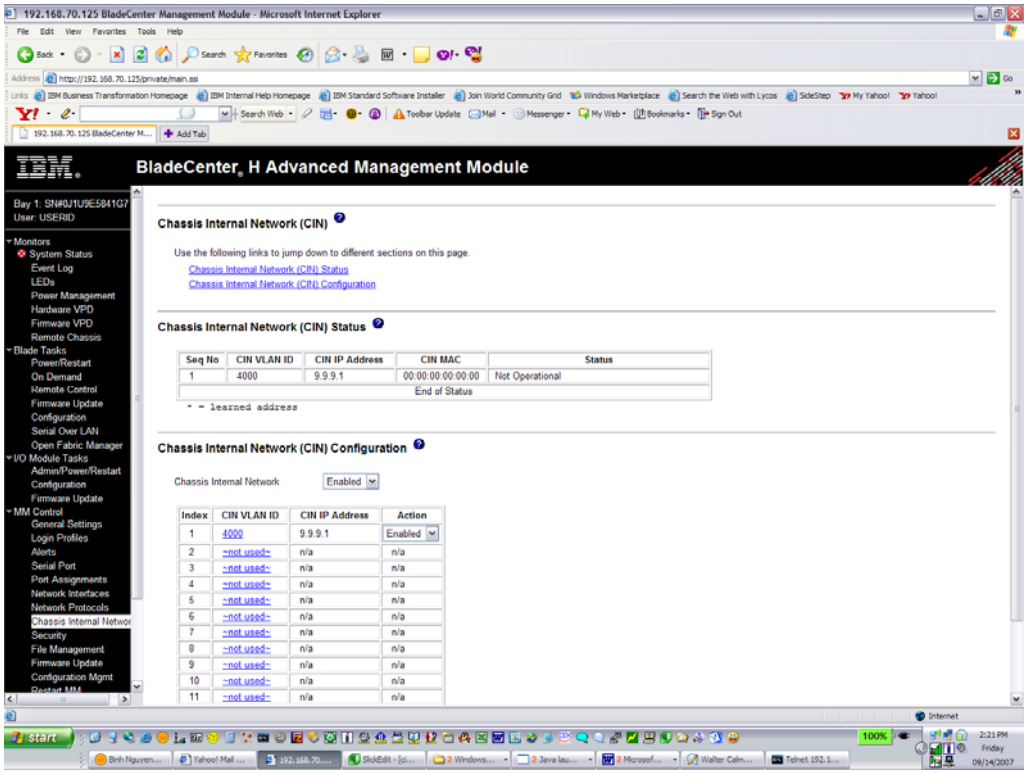
4. To globally enabled CIN, choose **Enabled** in the **Chassis Internal Network** select box. The following page is displayed, indicating that the Chassis Internal Network is now enabled.



5. Configure CIN Index entry 1 by clicking **~not_used~**. Enter a **VLAN ID** of 4000 and an **IP address** of 9.9.9.1 as shown in the following page.



6. Click **Save**. The following page shows that Index 1 was configured and saved.

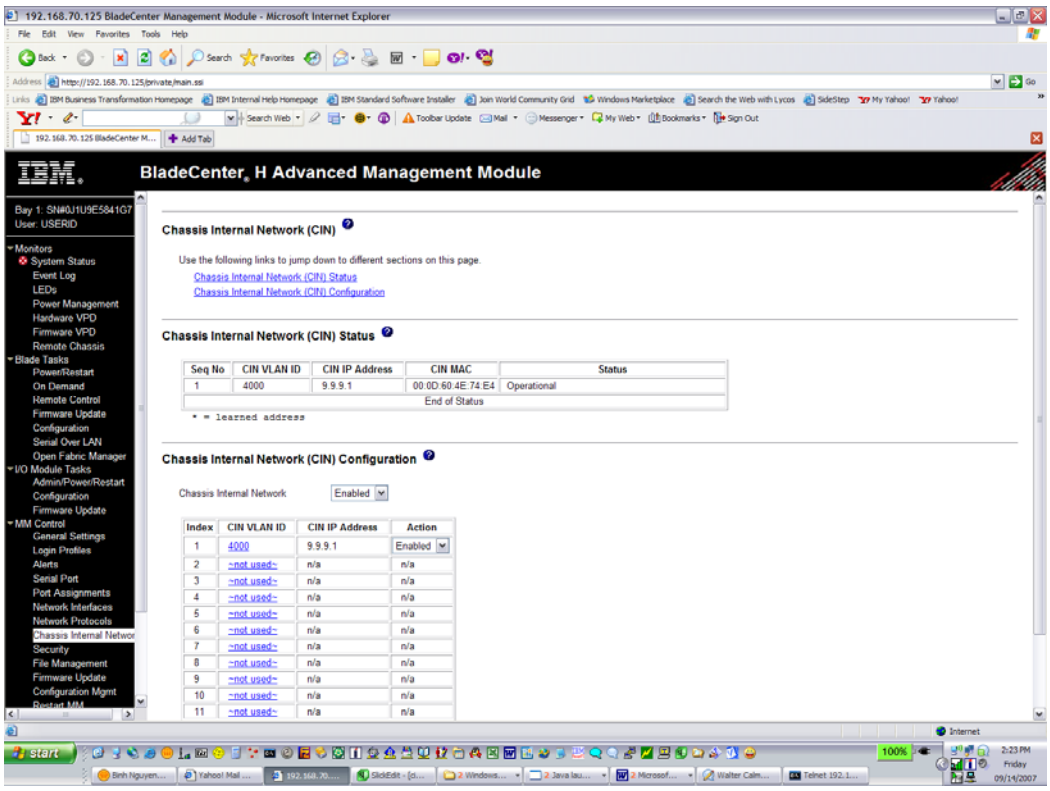


7. Verify that the AMM is able to communicate with the blade device OS. The following three states are possible:
   - **Operational**: The AMM was able to successfully ping the host.
   - **Not operational**: The AMM was not able to ping the host.
   - **Disabled**: The CIN-pair entry is disabled.

   Note 1: For the AMM to ping the host successfully, both the IOM and blade device OS must be configured correctly. Since you have not yet configured the blade device OS, "Not operational" is shown in the **Status** column.

   Note 2: All entries that have a valid VLAN ID and an IP address of 0.0.0.0 will have their state set to "Operational**.**" This indicates that Dynamic Host Learning is active for these VLAN interfaces.

8. After you configure the IOM and blade device OS, the AMM should be able to successfully ping the host and updates the **Status** to “Operational”.



4.2.3 Configuring CIN using the CLI

Complete the following steps to configure the CIN feature using the management module CLI:

1. Open a Telnet session with the AMM. The factory-defined static IP address of the management module is 192.168.70.125.

2. When prompted, enter the appropriate user ID and password. When you successfully log in, you should see information similar to the following:

```
Hostname:                       MM001125C308E6
Static IP address:              192.168.70.125
Burned-in MAC address:  00:11:25:C3:08:E6
DHCP:                           Disabled - Use static IP
configuration.
Last login: Tuesday February 1 2005 1:00 from 192.168.70.201
(Telnet)
system>
```

3. To display the current CIN configuration, type `cin` at the AMM Telnet (`system>`) prompt and press enter. If CIN is not enabled or configured, you will see the following output:

```
system> cin
 -global -en off
 -index  1 -en off  <not configured>
 -index  2 -en off  <not configured>
 -index  3 -en off  <not configured>
 -index  4 -en off  <not configured>
 -index  5 -en off  <not configured>
 -index  6 -en off  <not configured>
 -index  7 -en off  <not configured>
 -index  8 -en off  <not configured>
 -index  9 -en off  <not configured>
 -index 10 -en off  <not configured>
 -index 11 -en off  <not configured>
 -index 12 -en off  <not configured>
 -index 13 -en off  <not configured>
 -index 14 -en off  <not configured>
```

4. Globally enabled CIN by typing the following command at the `system>` prompt:

```
cin –global –en on
```

   An OK indication displays if CIN was successfully enabled.

5. Configure CIN entry 1 using a VLAN of 4000 and an IP address of 9.9.9.1 by typing the following command at the `system>` prompt:

```
system> cin –1 –id 4000 –ip  9.9.9.1
```

   An OK indication displays if the VLAN and IP address were successfully set.

6. Verify that CIN has been globally enabled by typing `cin` at the `system>` prompt. You should see that CIN is globally enabled and that a CIN pair with a VLAN ID of 4000 and an IP address of 9.9.9.1 has been added to the first entry.

```
system> cin
-global -en on
-index  1 -en on   -id 4000 -ip  9.9.9.1
-index  2 -en off  <not configured>
-index  3 -en off  <not configured>
-index  4 -en off  <not configured>
-index  5 -en off  <not configured>
-index  6 -en off  <not configured>
-index  7 -en off  <not configured>
-index  8 -en off  <not configured>
-index  9 -en off  <not configured>
-index 10 -en off  <not configured>
-index 11 -en off  <not configured>
-index 12 -en off  <not configured>
-index 13 -en off  <not configured>
-index 14 -en off  <not configured>
```

7. Verify that the AMM is able to communicate with the blade device OS. The following three states are possible:

   - **Operational**: The AMM was able to successfully ping the host.
   - **Not operational**: The AMM was not able to ping the host.
   - **Disabled**: The CIN-pair entry is disabled.

   Note 1: For the AMM to ping the host successfully, both the IOM and blade device OS must be configured correctly. Since you have not yet configured the blade device OS, if you run the `cinstatus –a` command, it will show a status of "Not operational." After you perform the OS configuration, you should run this command again: if the configuration is correct it will show a status of "Operational."

   Note 2: All entries that have a valid VLAN ID and an IP address of 0.0.0.0 will have their state set to "Operational." This indicates that Dynamic Host Learning is active for these VLAN interfaces.

   For example:

```
system> cinstatus –a
1. -ip  9.9.9.1 -id 4000 -mac 30:30:3A:30:44:3A -conn 0x4a -
text Operational

 Last entry reached
```

4.2.4 CIN-pair entry for Dynamic Host Learning

A CIN-pair entry for dynamic host learning consists of a valid VLAN ID and an IP address of 0.0.0.0. When this entry is configured, it will enable the AMM to accept communication from any host address secured in the specified VLAN. This ability will allow a blade device to communicate with the AMM without having to configure its IP address at the AMM. In addition, this allows the blade device OS to change its IP address without having to go back to the AMM configuration to change to a new IP address.

The configuration steps for this feature are the same as those in the previous section.

5 IOM VLAN configuration

The I/O modules in a BladeCenter unit are in between the AMM and the blade devices. Therefore, the IOMs are required to support user defined VLAN configuration on the management ports and blade device ports, for CIN to work. The following sections outline IOMs that support VLAN configuration and include instructions about how to configure them.

5.1 Cisco ESM configuration

Assumptions:

- You are already connected to the AMM Web interface
- You already know how to configure the IP address for the IOM
- You already know how to establish a Telnet connection to the IOM

The following I/O module configuration was used during the development of this document and will be used as reference and in examples:

CIN VLAN ID	4000
IP address:	192.168.70.127
Subnet mask:	255.255.255.0
Gateway:	0.0.0.0

Complete the following steps to configure and enable VLAN 4000 for the Cisco ESM:

1. Open a Telnet session with the Cisco ESM at IP address 192.168.70.127.

2. When prompted, enter the appropriate user ID and password. Once you successfully log in, you should see the `Switch#` prompt.

3. Enter the following commands to add and enable VLAN 4000 on **interface GigbitEthernet0/15** (mgmt1) and **interface GigbitEthernet0/16** (mgmt2).

   Note: mgmt1 and mgmt2 are the ports used for the IOM to connect to both of the AMM bays.

   - `Switch#config t`
   - `Switch(config)#vlan 4000`
   - `Switch(config-vlan)#state active`

     Note: You will receive the message “Can't modify state for extended VLAN 4000.” if the state on the VLAN is already active. This is expected and is OK.

   - `Switch(config-vlan)#exit`
   - `Switch(config)#int gi 0/15`
   - `Switch(config-if)#sw trunk allow vlan add 4000`

- Switch(config-if)#exit
- Switch(config)#int gi 0/16
- Switch(config-if)#sw trunk allow vlan add 4000
- Switch(config-if)#end
- Switch#wri

4. To make sure that VLAN 4000 was configured correctly, enter the following commands:

   - Switch#enable
   - Switch#show running

     Note: You should see output similar to the following. Pay close attention to **interface GigbitEthernet0/15** (mgmt1) and **interface GigbitEthernet0/16** (mgmt2) and make sure that VLAN 4000 is allowed for trunking. Those interfaces are shown in **bold** in the following output example.

```
Building configuration...

Current configuration : 4748 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch
!
!
username USERID privilege 15 secret 5
$1$AXj0$0QTwgcwApROQUVPhTxGP6.
ip subnet-zero
!
vtp mode transparent
!
!
spanning-tree mode rapid-pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
!
vlan 2
 name operational
!
vlan 4000
!
interface GigabitEthernet0/1
 description blade1
```

```
 switchport access vlan 2
 switchport trunk native vlan 2
 switchport trunk allowed vlan 2-4094
 switchport mode trunk
 spanning-tree portfast trunk
 spanning-tree bpdufilter enable
!
interface GigabitEthernet0/2
 description blade2
 switchport access vlan 2
 switchport trunk native vlan 2
 switchport trunk allowed vlan 2-4094
 switchport mode trunk
 spanning-tree portfast trunk
 spanning-tree bpdufilter enable
!
interface GigabitEthernet0/3
 description blade3
 switchport access vlan 2
 switchport trunk native vlan 2
 switchport trunk allowed vlan 2-4094
 switchport mode trunk
 spanning-tree portfast trunk
 spanning-tree bpdufilter enable
!
interface GigabitEthernet0/4
 description blade4
 switchport access vlan 2
 switchport trunk native vlan 2
 switchport trunk allowed vlan 2-4094
 switchport mode trunk
 spanning-tree portfast trunk
 spanning-tree bpdufilter enable
!
interface GigabitEthernet0/5
 description blade5
 switchport access vlan 2
 switchport trunk native vlan 2
 switchport trunk allowed vlan 2-4094
 switchport mode trunk
 spanning-tree portfast trunk
 spanning-tree bpdufilter enable
!
interface GigabitEthernet0/6
 description blade6
 switchport access vlan 2
 switchport trunk native vlan 2
 switchport trunk allowed vlan 2-4094
 switchport mode trunk
 spanning-tree portfast trunk
 spanning-tree bpdufilter enable
!
interface GigabitEthernet0/7
 description blade7
 switchport access vlan 2
 switchport trunk native vlan 2
 switchport trunk allowed vlan 2-4094
```

```
 switchport mode trunk
 spanning-tree portfast trunk
 spanning-tree bpdufilter enable
!
interface GigabitEthernet0/8
 description blade8
 switchport access vlan 2
 switchport trunk native vlan 2
 switchport trunk allowed vlan 2-4094
 switchport mode trunk
 spanning-tree portfast trunk
 spanning-tree bpdufilter enable
!
interface GigabitEthernet0/9
 description blade9
 switchport access vlan 2
 switchport trunk native vlan 2
 switchport trunk allowed vlan 2-4094
 switchport mode trunk
 spanning-tree portfast trunk
 spanning-tree bpdufilter enable
!
interface GigabitEthernet0/10
 description blade10
 switchport access vlan 2
 switchport trunk native vlan 2
 switchport trunk allowed vlan 2-4094
 switchport mode trunk
 spanning-tree portfast trunk
 spanning-tree bpdufilter enable
!
interface GigabitEthernet0/11
 description blade11
 switchport access vlan 2
 switchport trunk native vlan 2
 switchport trunk allowed vlan 2-4094
 switchport mode trunk
 spanning-tree portfast trunk
 spanning-tree bpdufilter enable
!
interface GigabitEthernet0/12
 description blade12
 switchport access vlan 2
 switchport trunk native vlan 2
 switchport trunk allowed vlan 2-4094
 switchport mode trunk
 spanning-tree portfast trunk
 spanning-tree bpdufilter enable
!
interface GigabitEthernet0/13
 description blade13
 switchport access vlan 2
 switchport trunk native vlan 2
 switchport trunk allowed vlan 2-4094
 switchport mode trunk
 spanning-tree portfast trunk
 spanning-tree bpdufilter enable
```

```
!
interface GigabitEthernet0/14
 description blade14
 switchport access vlan 2
 switchport trunk native vlan 2
 switchport trunk allowed vlan 2-4094
 switchport mode trunk
 spanning-tree portfast trunk
 spanning-tree bpdufilter enable
!
interface GigabitEthernet0/15
 description mgmt1
 switchport trunk allowed vlan 1,4000
 switchport mode trunk
 switchport nonegotiate
 spanning-tree cost 100
!
interface GigabitEthernet0/16
 description mgmt2
 switchport trunk allowed vlan 1, 4000
 switchport mode trunk
 switchport nonegotiate
 spanning-tree cost 100
!
interface GigabitEthernet0/17
 description extern1
 switchport access vlan 2
 switchport trunk native vlan 2
 shutdown
!
interface GigabitEthernet0/18
 description extern2
 switchport access vlan 2
 switchport trunk native vlan 2
 shutdown
!
interface GigabitEthernet0/19
 description extern3
 switchport access vlan 2
 switchport trunk native vlan 2
 shutdown
!
interface GigabitEthernet0/20
 description extern4
 switchport access vlan 2
 switchport trunk native vlan 2
 shutdown
!
interface Vlan1
 ip address 192.168.70.127 255.255.255.0
 no ip route-cache
!
ip http server
ip http authentication local
!
snmp-server community public RO
snmp-server community private RW
!
```

```
line con 0
line vty 0 4
 login local
line vty 5 15
 login local
!
end
```

5.2 Nortel ESM configuration

Assumptions:

- You are already connected to the AMM Web interface
- You already know how to configure the IP address for the IOM
- You already know how to establish a Telnet connection to the IOM

The following I/O module configuration that was used during the development of this document and will be used as reference and in examples:

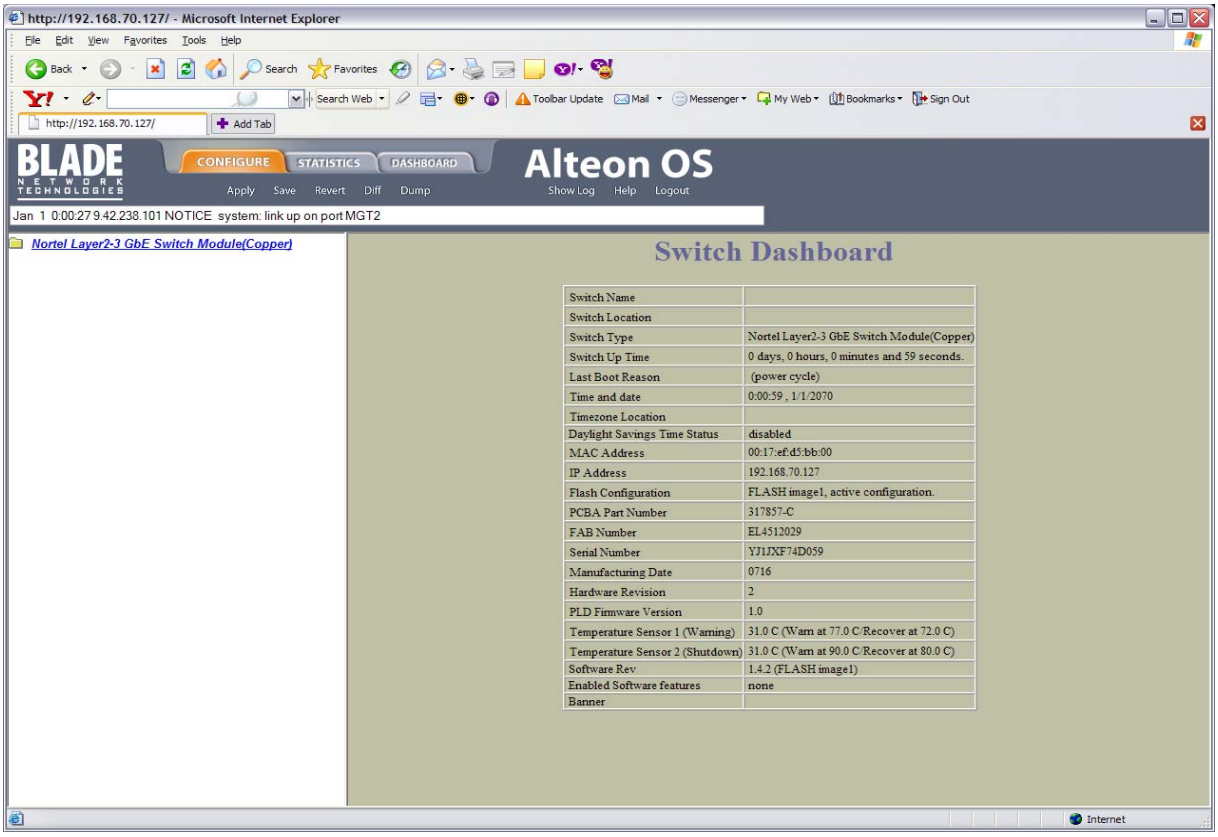
CIN VLAN ID	4000
IP address:	192.168.70.127
Subnet mask:	255.255.255.0
Gateway:	0.0.0.0

Complete the following steps to configure and enable VLAN 4000 for the Nortel 6-port ESM:

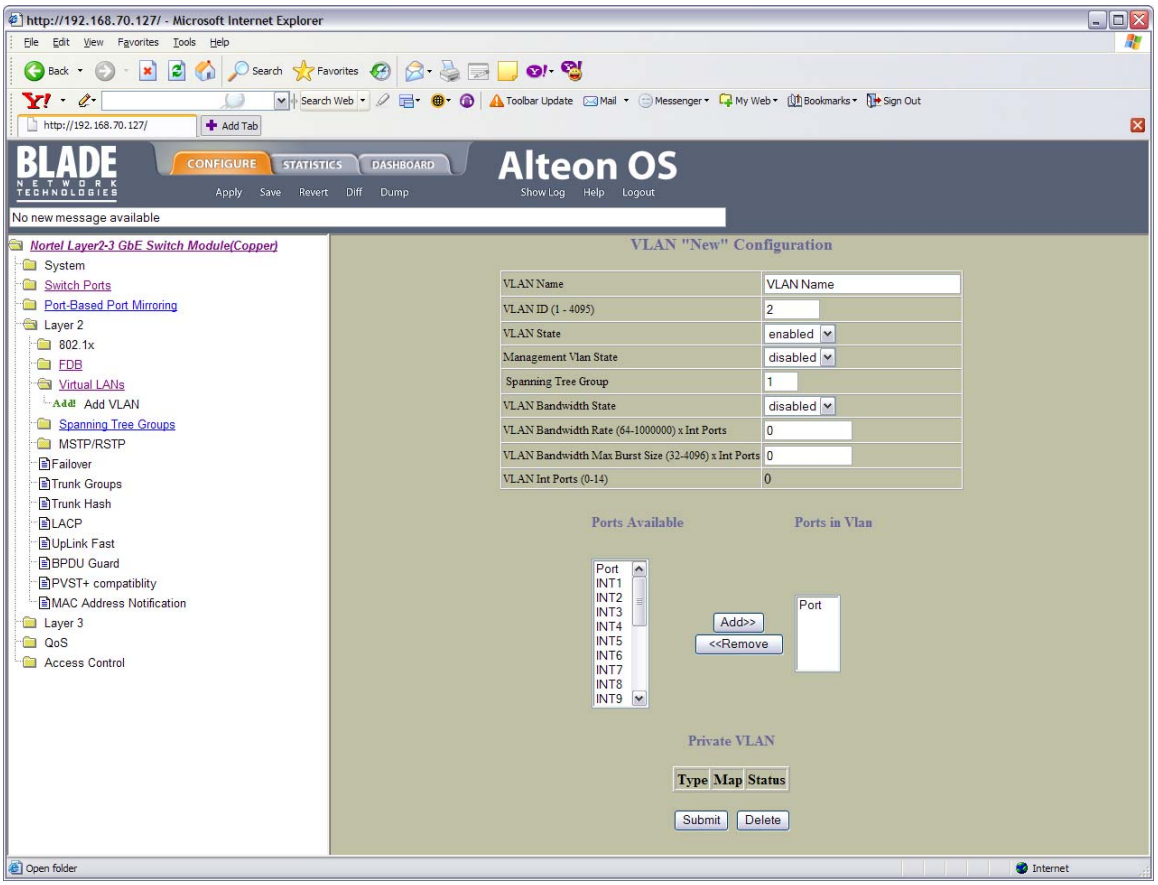
1. Open an http or https session with the Nortel 6-port ESM at IP address 192.168.70.127.

2. When prompted, enter the appropriate user ID and password

3. Click the **CONFIGURE** tab.



4. Click on the following items in the navigation pane to access the VLAN “New” Configuration screen:
   - **Nortel Layer2-3 GbE Switch Module (Copper)**
   - **Layer 2**
   - **Virtual VLAN**
   - **Add**



5. Set the following values:

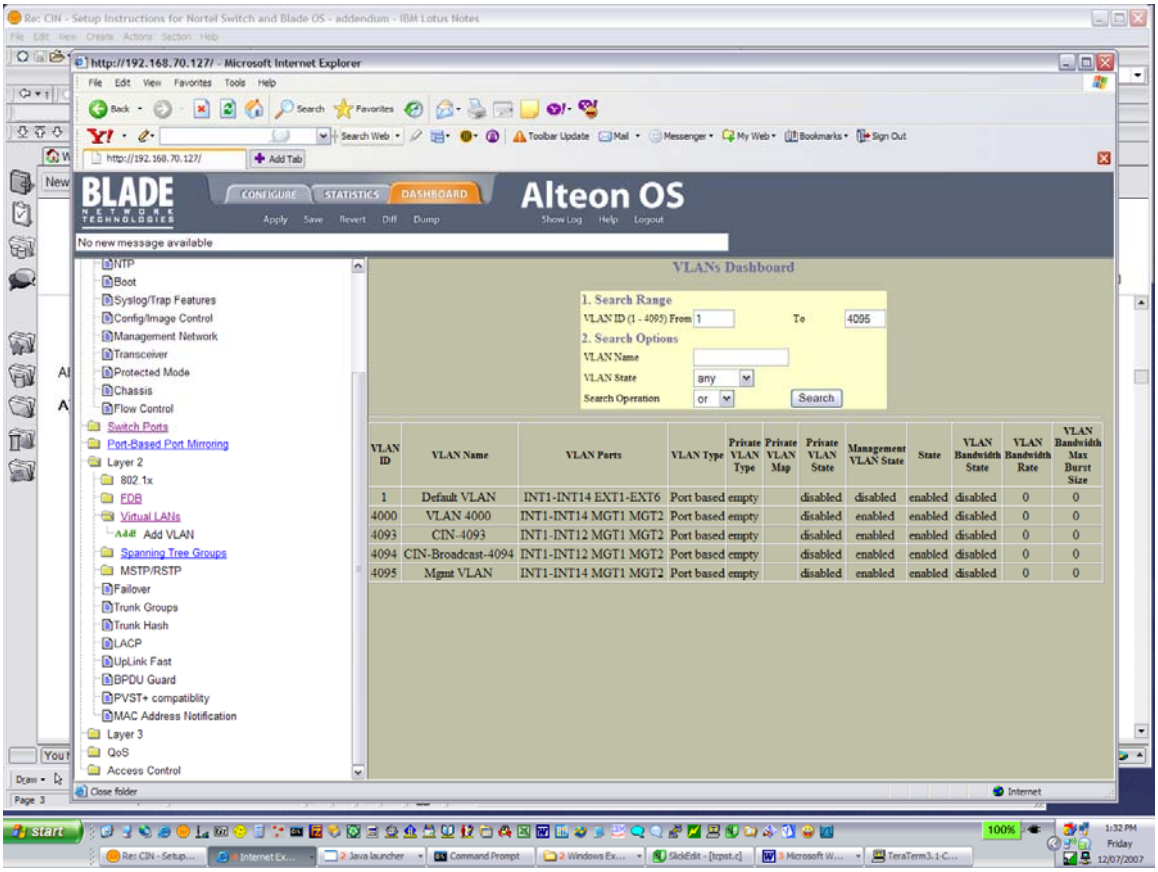
   a. **VLAN ID** to 4000.
   b. **Management Vlan State** to **enabled**
   c. Add the following ports to the **Ports in Vlan** list:
      - INT1 through INT14
      - MGT1
      - MGT2

6. Click **Submit**.

7. Click **Apply** for the new VLAN configuration to take effect.

8. Click **Save** to write the new VLAN configuration to the switch NVRAM.

9. Click the **DASHBOARD** tab and make sure that the new VLAN configuration is correct.



6 Blade device operating system configuration

All blade devices that run an OS that has VLAN configuration support can be used to access the AMM through the CIN path. The following sections outline OSs' that support VLAN configuration.

Assumptions:

- You have already installed an OS on the blade device
- You have verified that you can run the AMM remote control applet and that the keyboard, monitor, and mouse are accessible to the blade device OS.

6.1 Red Hat Enterprise Linux 2.6.9-5.SLxmp and SUSE Linux Enterprise Server 9 for x86 configuration

Assumptions:

- The blade device OS uses eth0 to connect to the IOM in bay 1. If the blade device OS uses eth to connect to the IOM in bay 1, replace "eth0" with "eth1" in the following procedure.

NOTE: The instructions in this section are for the IOM installed in IOM bay 1. If the IOM is installed in a different IOM bay, adjustments to the instructions must be made accordingly.

The following configuration was used during the development of this document and will be used as reference and in examples.

CIN VLAN ID:

VLAN ID: 4000

eth0:

Note: This is the interface the blade device OS uses to connect to the production network.

IP address: 8.8.8.1
Subnet mask: 255.255.255.0
Gateway: 0.0.0.0

eth0.4000:

Note: This is the interface that the blade device OS will use to communicate with AMM using CIN.

The IP addresses of the blade device OS and AMM do not have to be in the same subnet.

IP address:	9.9.9.1
Subnet mask:	255.255.255.0
Gateway:	0.0.0.0

Complete the following steps to enable the VLAN configuration.

Note: The blade device OS prompt is `linux:~ #`.

1. Log in as the root user.
2. Open an x window.
3. Enter the following commands at the `linux:~ #` prompt:
   - `ifconfig eth0  8.8.8.1 netmask 255.255.255.0 broadcast 8.8.8.255 -allmulti`
   - `modprobe 8021q`
   - `vconfig add eth0 4000`

   You should see the following output:
   ```
   Added VLAN with VID == 4000 to IF -:eth0:-
   ```
4. Enter the following commands at the `linux:~ #` prompt:
   - `ifconfig eth0.4000  9.9.9.1 netmask 255.255.255.0 broadcast 9.9.9.255`
   - `ifconfig`

   You should see the following output that shows that interface **eth0.4000** has been successfully created:

```
      eth0      Link encap:Ethernet  HWaddr 00:0D:60:4E:74:E4
                  inet addr: 8.8.8.1  Bcast: 8.8.8.255
Mask:255.255.255.0
                  inet6 addr: fe80::20d:60ff:fe4e:74e4/64 Scope:Link
                  UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
                  RX packets:0 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:164 errors:0 dropped:0 overruns:0 carrier:0
                      collisions:0 txqueuelen:1000
                  RX bytes:0 (0.0 b)  TX bytes:10730 (10.4 Kb)
                  Interrupt:16

      eth0.4000 Link encap:Ethernet  HWaddr 00:0D:60:4E:74:E4
                  inet addr: 9.9.9.1  Bcast: 9.9.9.255
Mask:255.255.255.0
                  inet6 addr: fe80::20d:60ff:fe4e:74e4/64 Scope:Link
                  UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
                  RX packets:0 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
```

```
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:460 (460.0 b)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
           inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
           RX packets:89 errors:0 dropped:0 overruns:0 frame:0
          TX packets:89 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
                RX bytes:5741 (5.6 Kb)  TX bytes:5741 (5.6 Kb)
```

5. Enter the following commands at the `linux:~ #` prompt:
   - `route add -host 192.168.70.125 dev eth0.4000`
   - `route`

   You should see the following output that shows that a route to the AMM IP address 192.168.70.125 has been created successfully on the **eth0.4000** interface.

```
Kernel IP routing table
Destination       Gateway         Genmask             Flags
      Metric      Ref         Use Iface
192.168.70.125    *                       255.255.255.255 UH 0
      0           0     eth0.4000
8.8.8.0           *                       255.255.255.0   U
      0           0           0     eth0
9.9.9.0     *                         255.255.255.0   U        0
      0           0     eth0.4000
link-local        *                       255.255.0.0     U
      0           0           0     eth0
```

6. Enter the following commands at the `linux:~ #` prompt:
   - `route add -net 224.0.0.0 netmask 240.0.0.0  dev eth0.4000`
   - `ping 192.168.70.125`

   If CIN is configured correctly, you should see the following successful ping responses:

```
PING 192.168.70.125 (192.168.70.125) 56(84) bytes of data.
64 bytes from 192.168.70.125: icmp_seq=4 ttl=64 time=0.259 ms
64 bytes from 192.168.70.125: icmp_seq=5 ttl=64 time=0.240 ms
64 bytes from 192.168.70.125: icmp_seq=6 ttl=64 time=0.225 ms
64 bytes from 192.168.70.125: icmp_seq=7 ttl=64 time=0.224 ms
```

The CIN feature is now enabled and correctly configured for this blade device.

6.2 Microsoft Windows Server 2003 configuration

Assumptions:

- The blade device OS uses network interface card 1 (nic1) to connect to the IOM in bay 1. If the blade device OS uses nic2 to connect to the IOM in bay 1, replace nic1 with nic2 in the following procedure.

NOTE: The instructions in this section are for the IOM installed in IOM bay 1. If the IOM is installed in a different IOM bay, adjustments to the instructions must be made accordingly.

The following configuration was used during the development of this document and will be used as reference and in examples.

CIN VLAN ID:

VLAN ID	4000

VLAN untagged interface nic1:

Note: This is the interface the blade device OS uses to connect to the production network

IP address:	8.8.8.1
Subnet mask:	255.255.255.0
Gateway:	0.0.0.0

VLAN tagged interface nic1.4000:

Note: This is the interface that the blade device OS will use to communicate with the AMM using CIN.

The IP addresses of the blade device OS and AMM do not have to be in the same subnet

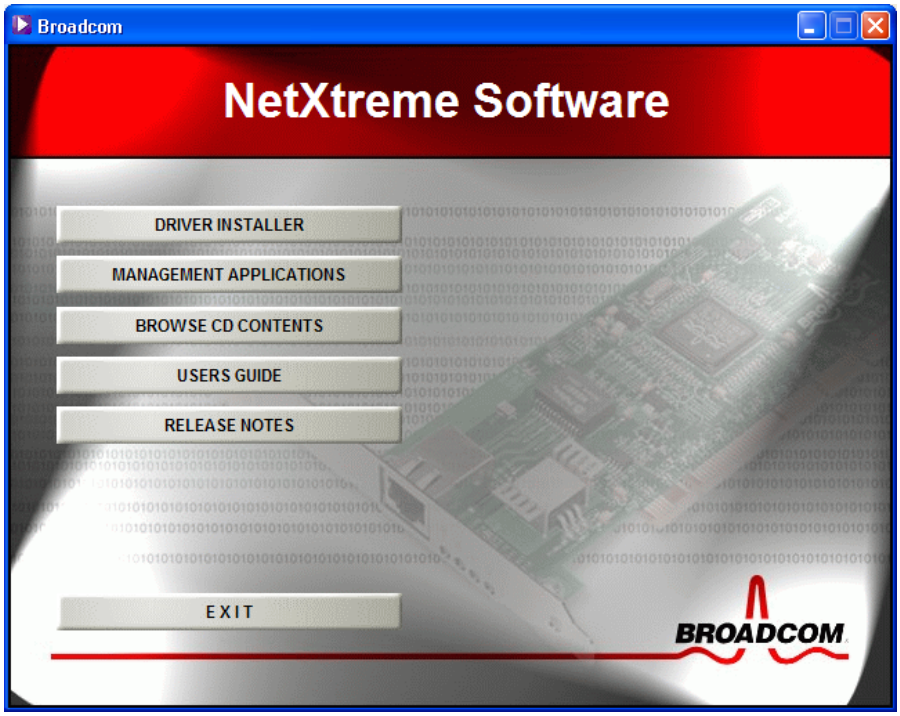
IP address:	9.9.9.1
Subnet mask:	255.255.255.0
Gateway:	0.0.0.0

Complete the following steps to enable the VLAN configuration:

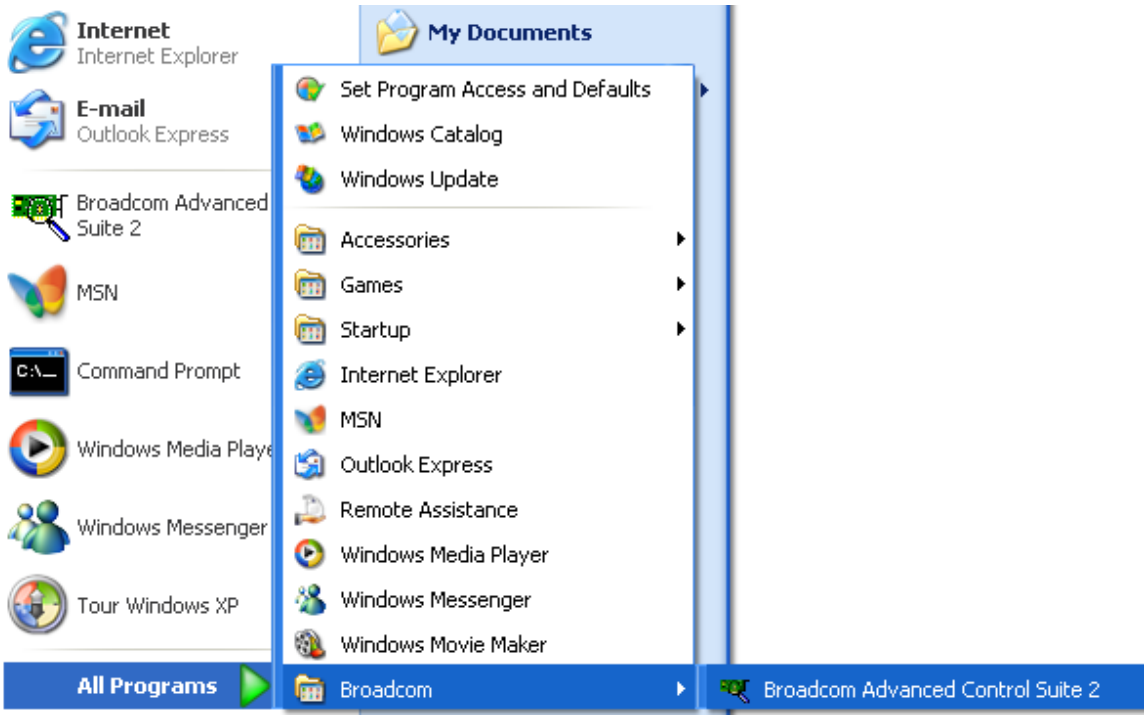
1. Obtain a Broadcom NetXtreme Software CD ISO image from http://www-304.ibm.com/jct01004c/systems/support/supportsite.wss/docdisplay?brandind=5000008&lndocid=MIGR-5070766

2. Following the instructions that come with the image, create a CD; then, use the CD to install the Broadcom NetXtreme Software.

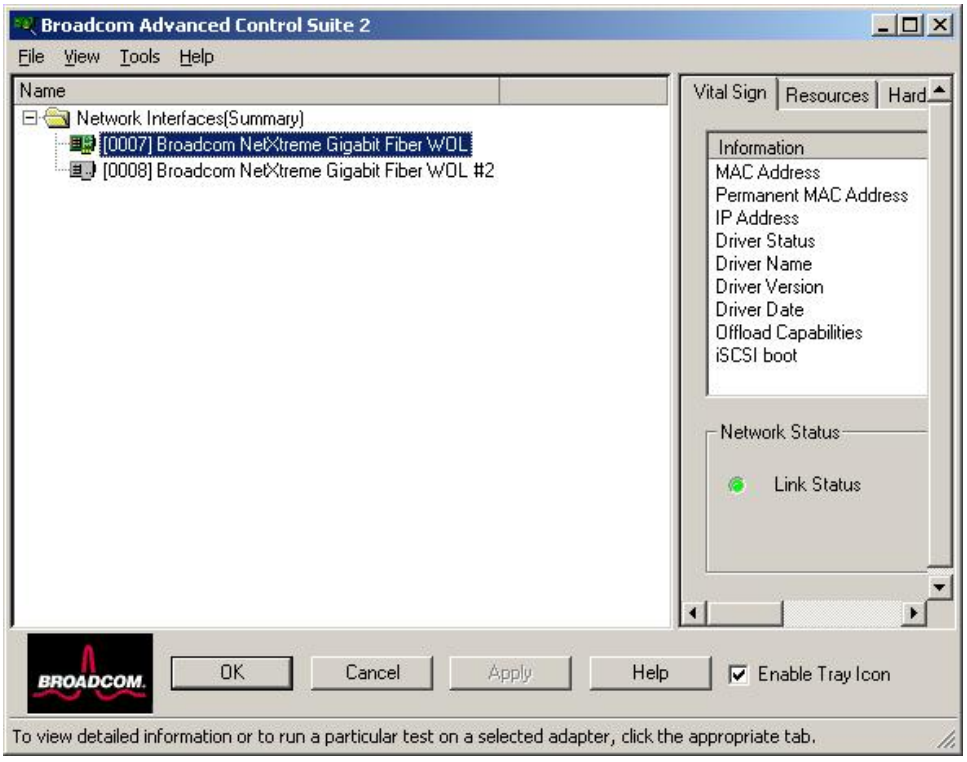
3. From the NetXtreme Software screen, select **MANAGEMENT APPLICATIONS**.



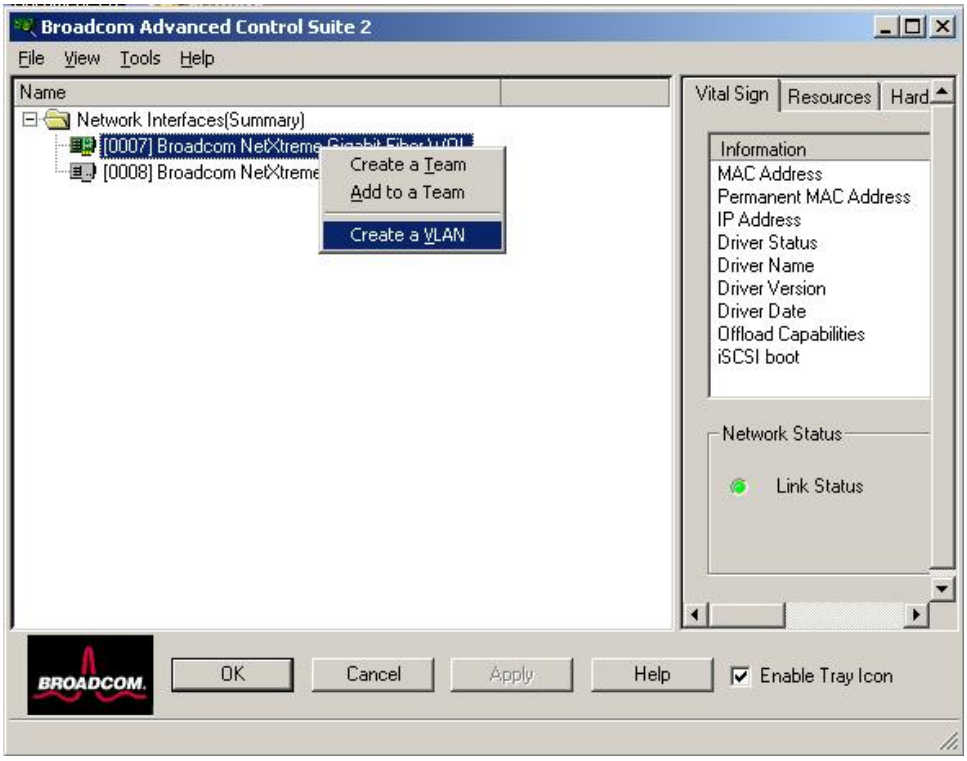
4. After installing the Management Application, from the Start menu select **Start > All Programs > Broadcom > Broadcom Advanced Control Suite 2**.



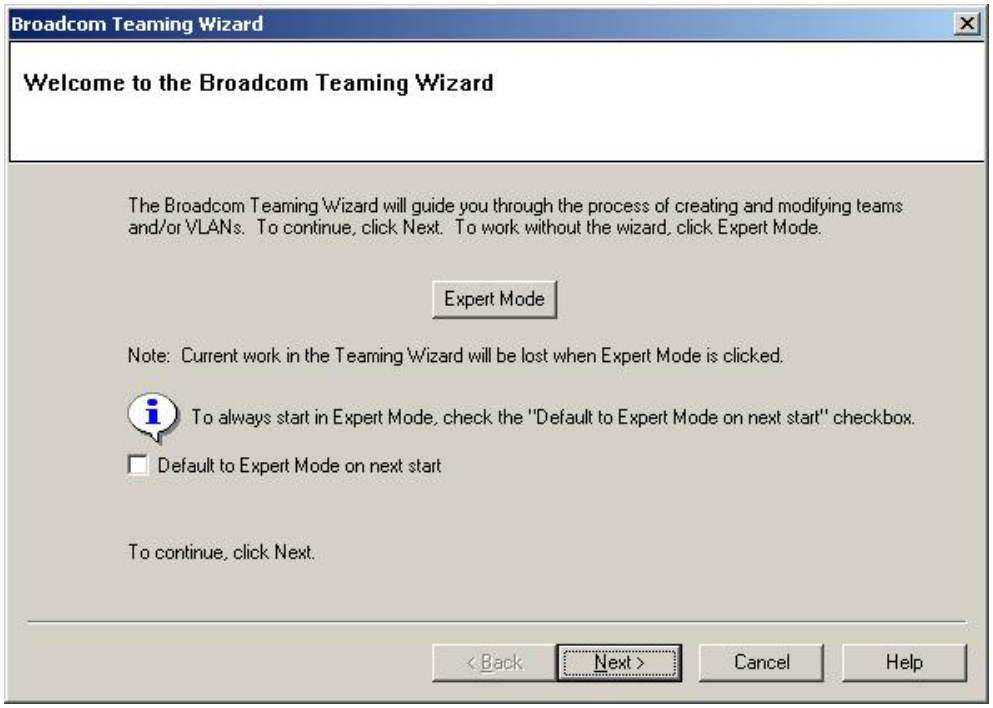
5. Select the network interface card that is connecting to the IOM in bay 1 from the **Network Interface (Summary)** list.



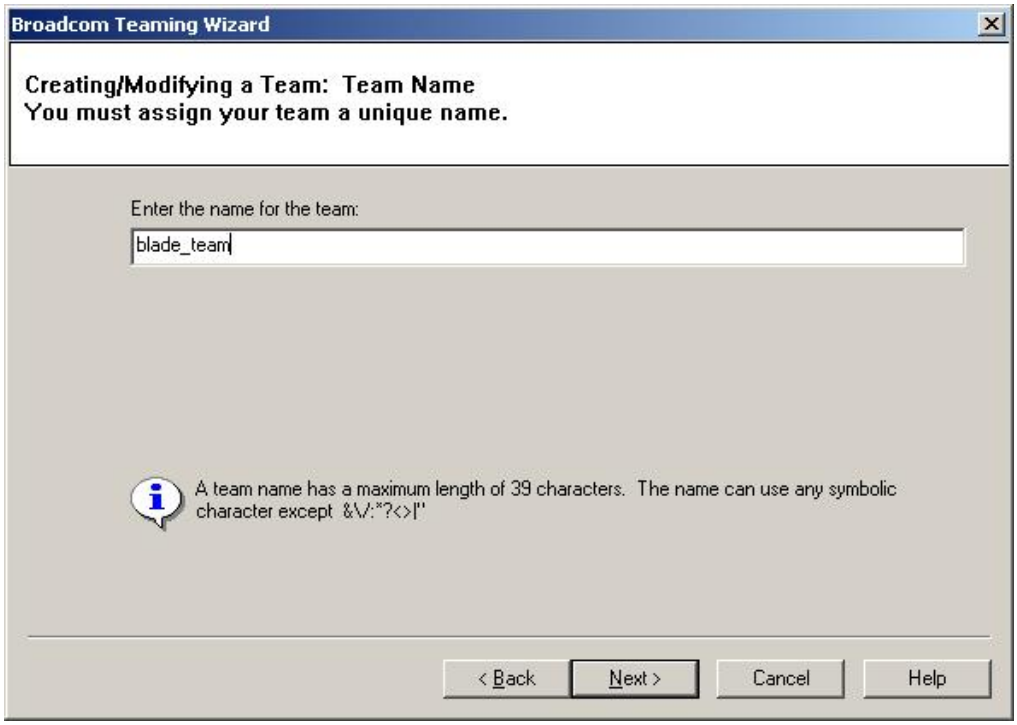
6. Right-click the selected network interface card; then, select **Create a VLAN**.



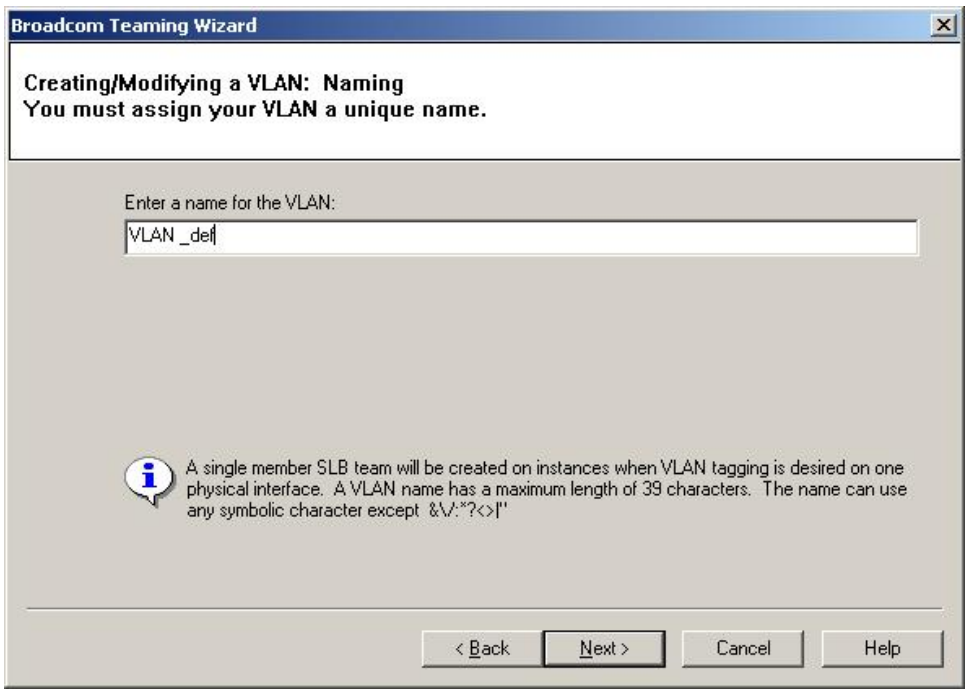
7. Click **Next** from the Welcome to the Broadcom Teaming Wizard window.



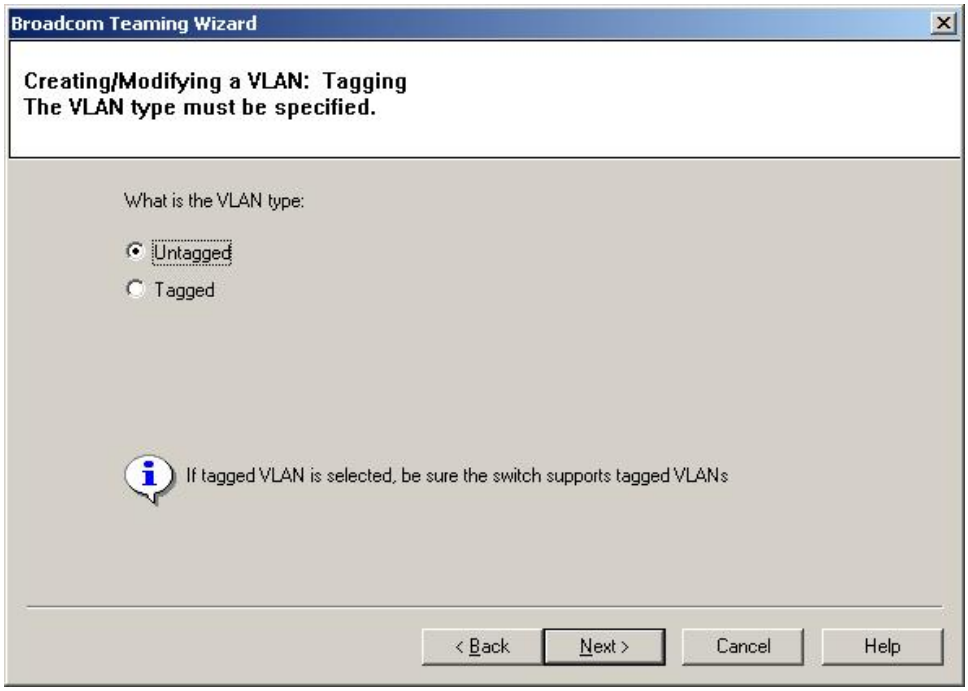
8. Enter a team name in the **Enter the name for the team:** field (for example, blade_name); then, click **Next**.



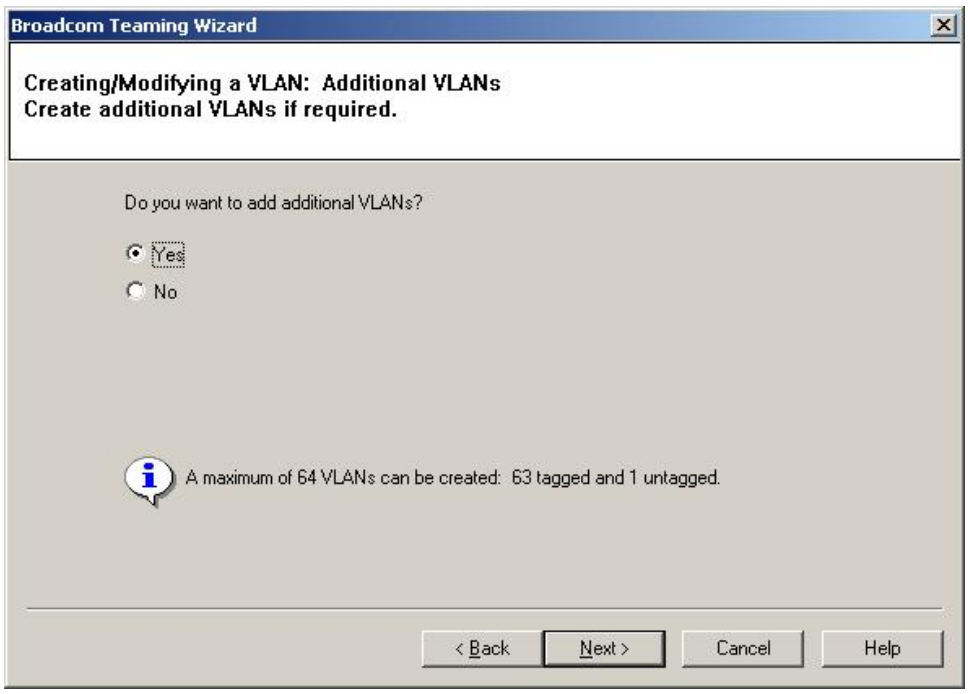
9. Enter a VLAN name in the **Enter a name for the VLAN:** field (for example, VLAN_def); then, click **Next**.



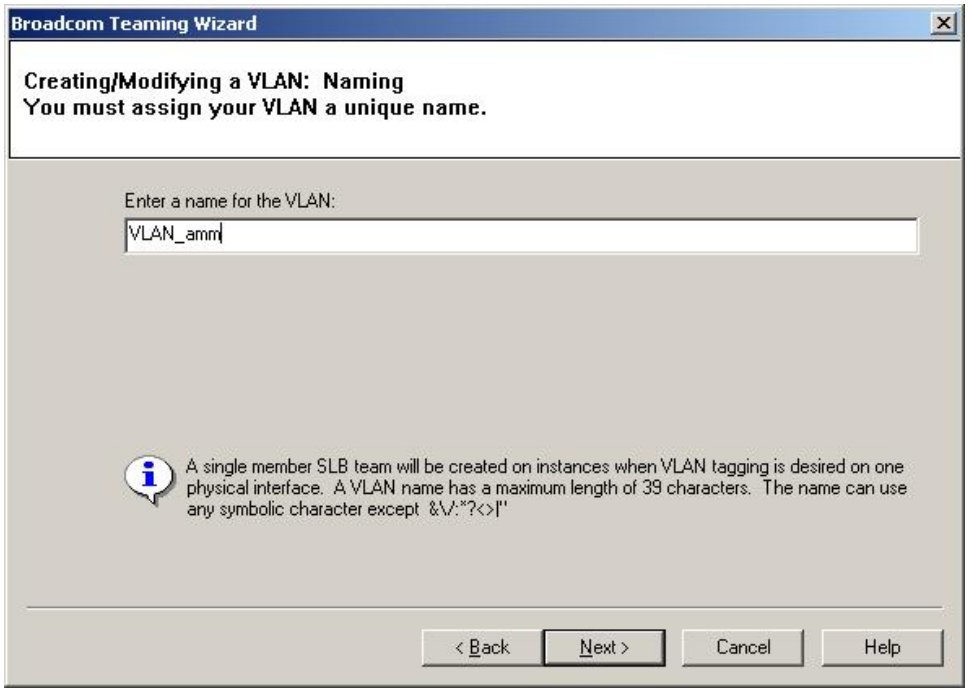
10. Select **Untagged** as the VLAN type; then, click **Next**.



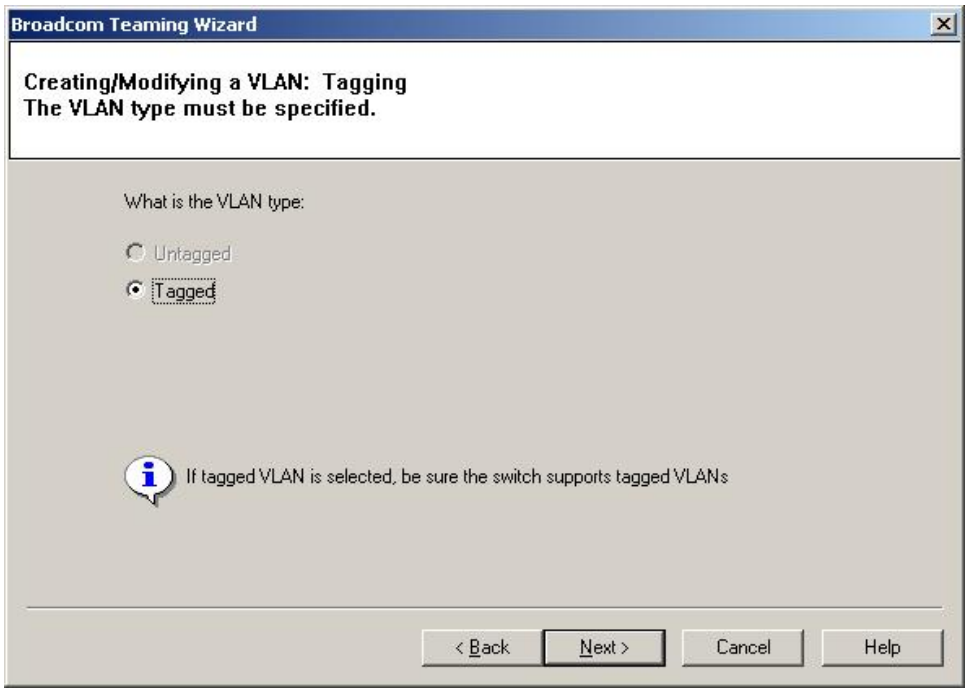
11. Select **Yes** for adding additional VLANs; then, click **Next**.



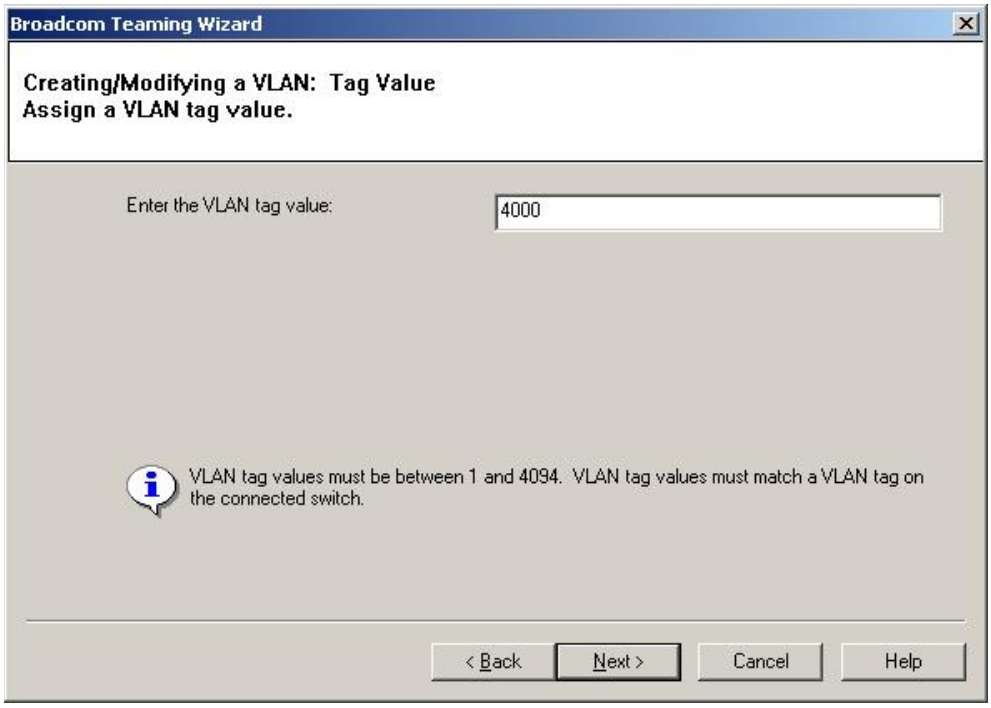
12. Enter a VLAN name in the **Enter a name for the VLAN:** field (for example, VLAN_amm); then, click **Next**.



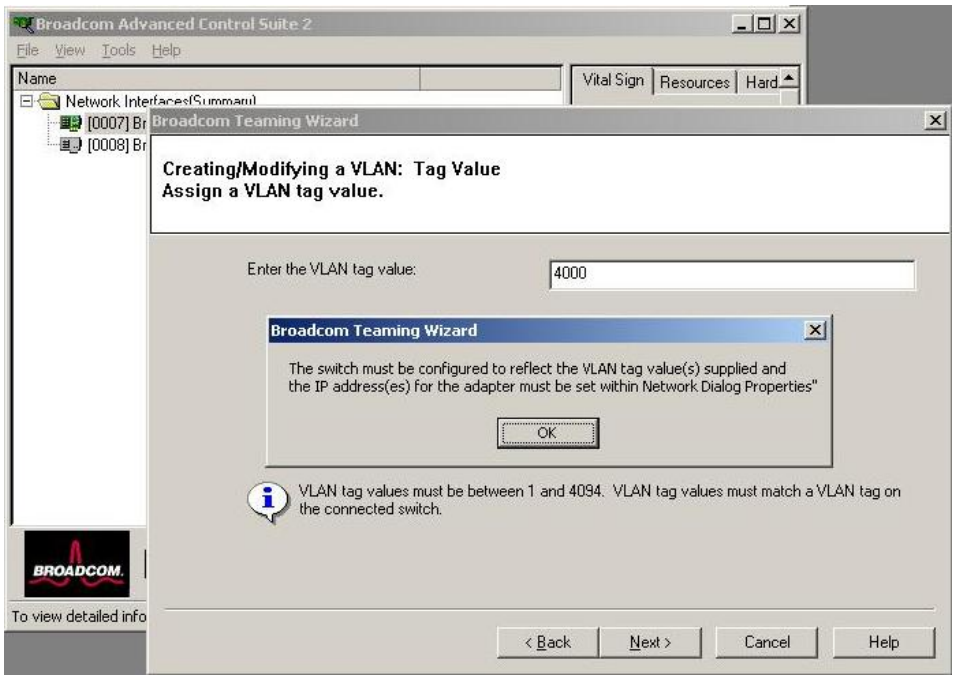
13. Select **Tagged** for the VLAN type; then, click **Next**.



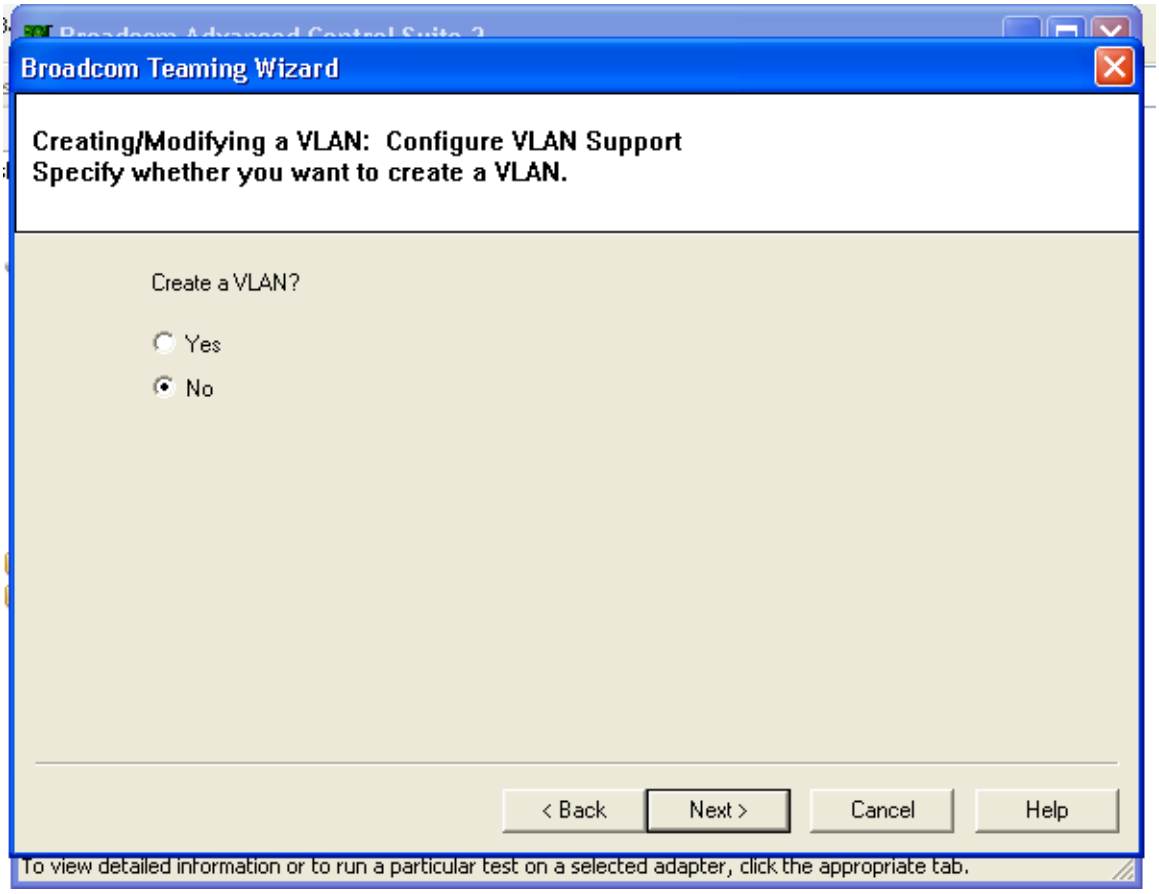
14. Enter VLAN tag value of 4000 in the **Enter the VLAN tag value:** field; then, click **Next**.



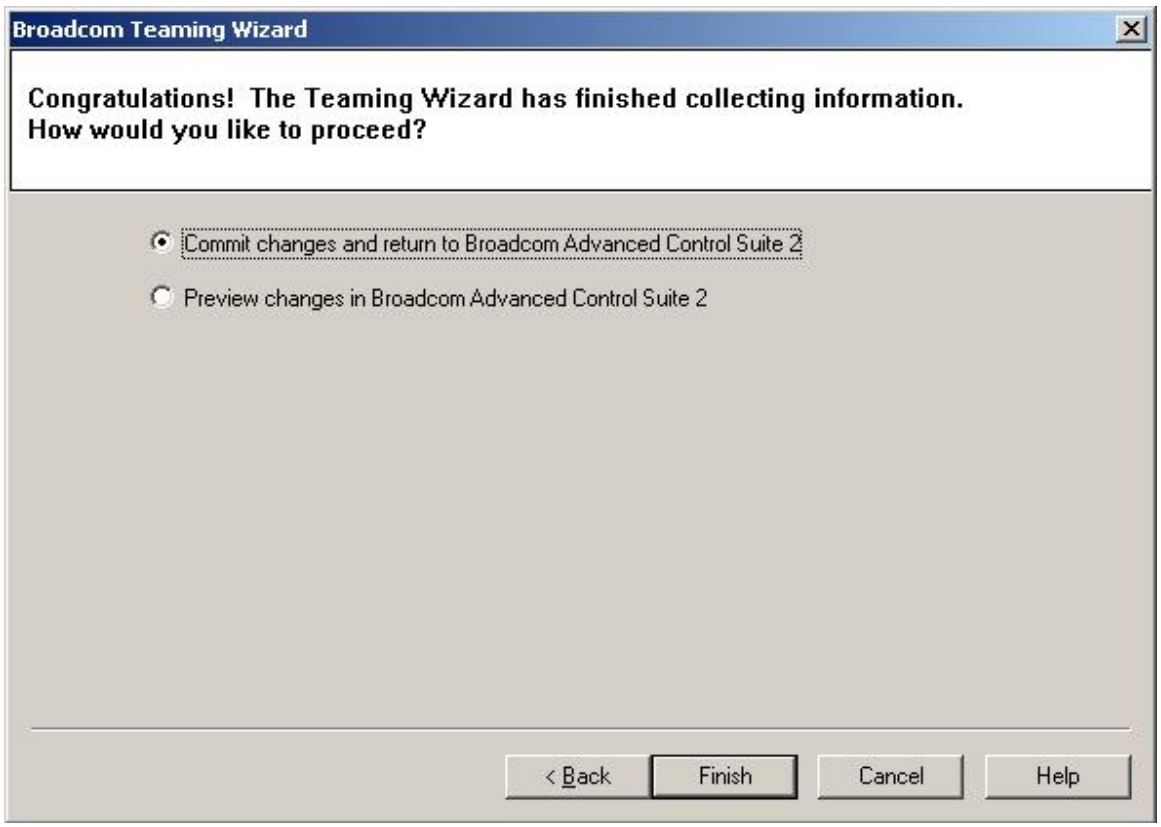
15. Click **OK** in the Broadcom Teaming Wizard pop-up window.



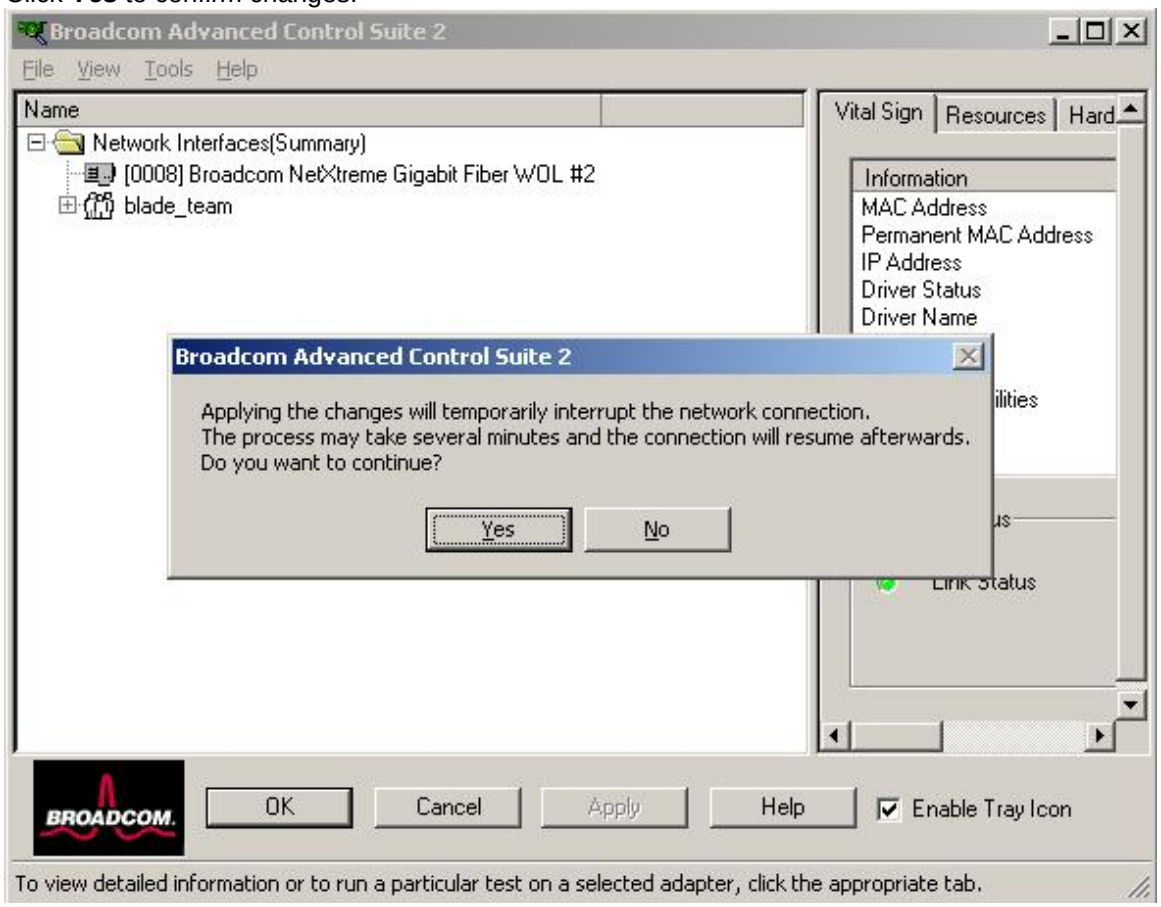
16. Select **No** when asked if you want to create a VLAN; then, click **Next**.



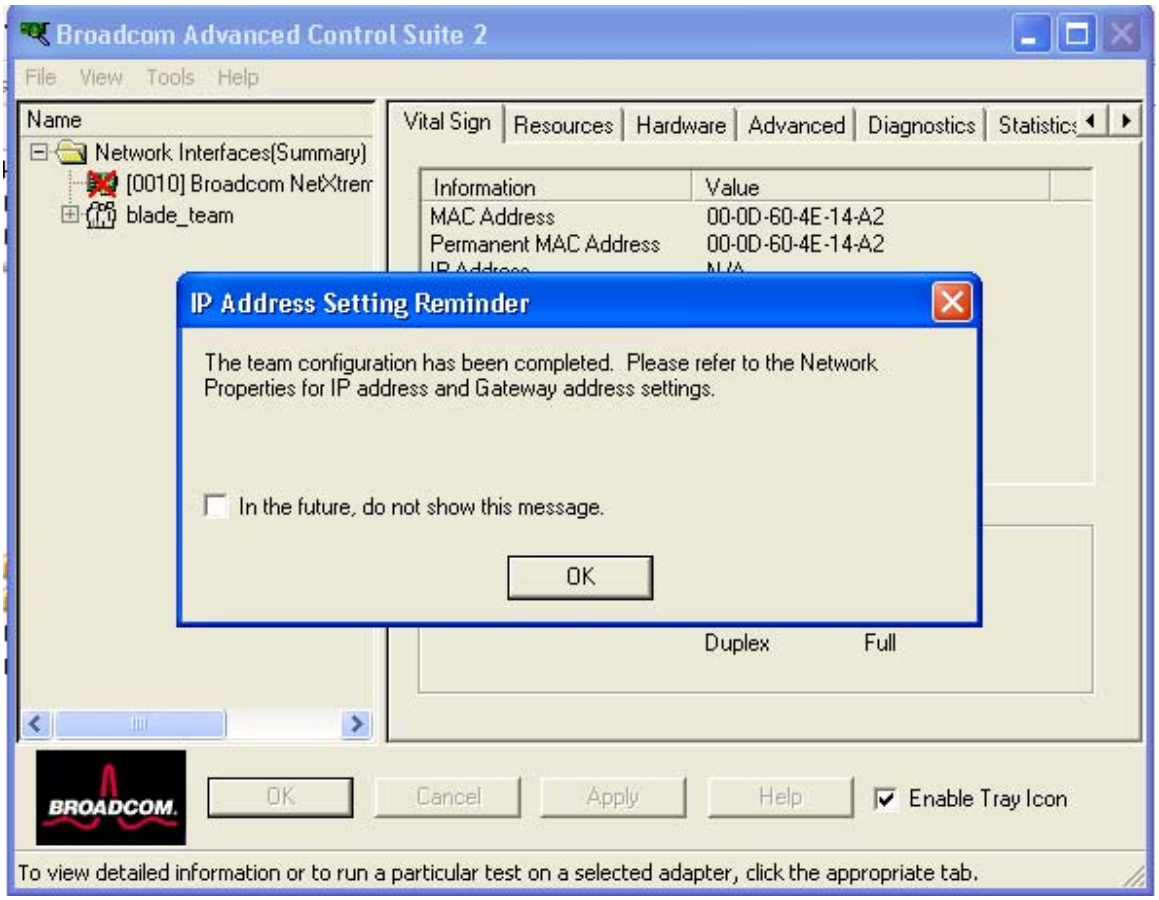
17. Select **Commit changes and return to Broadcom Advanced Control Suite 2**; then, click **Finish**.



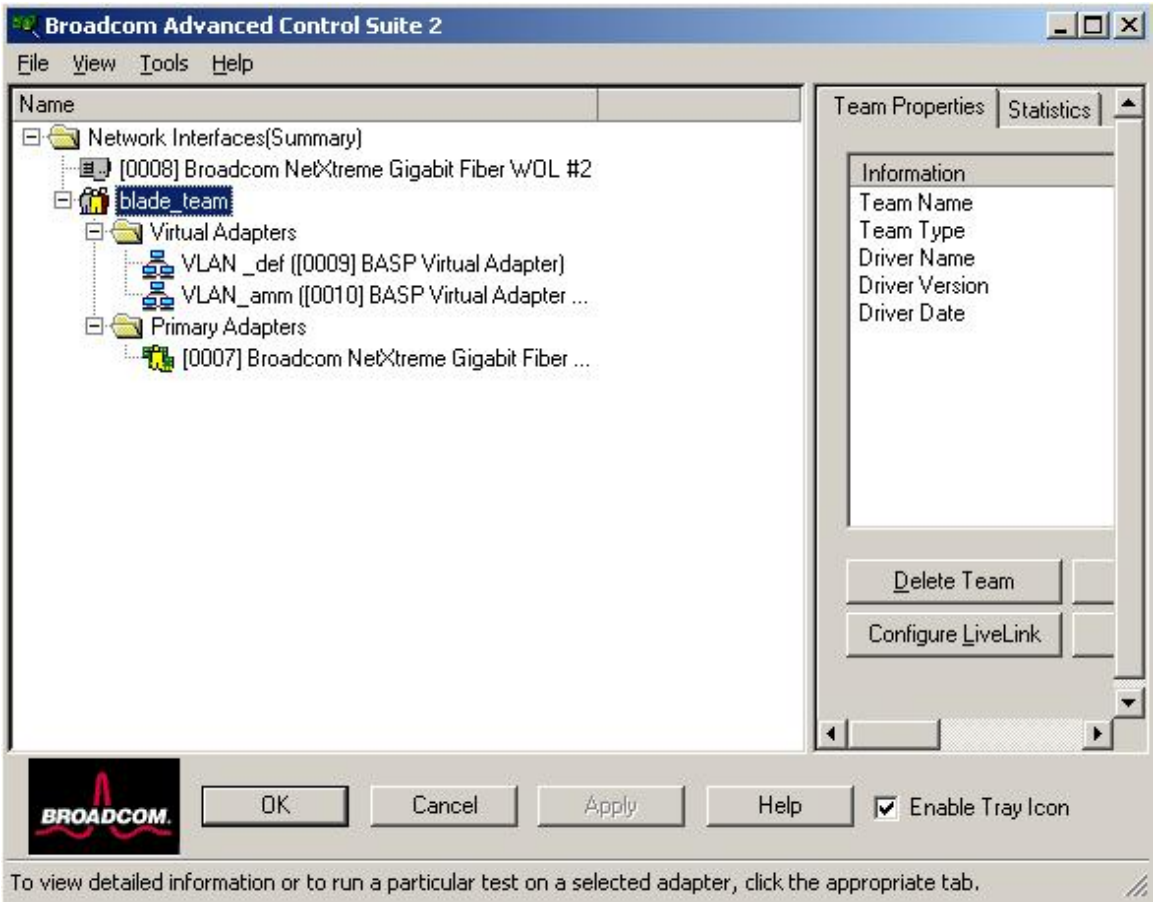
18. Click **Yes** to confirm changes.



19. Click **OK**.

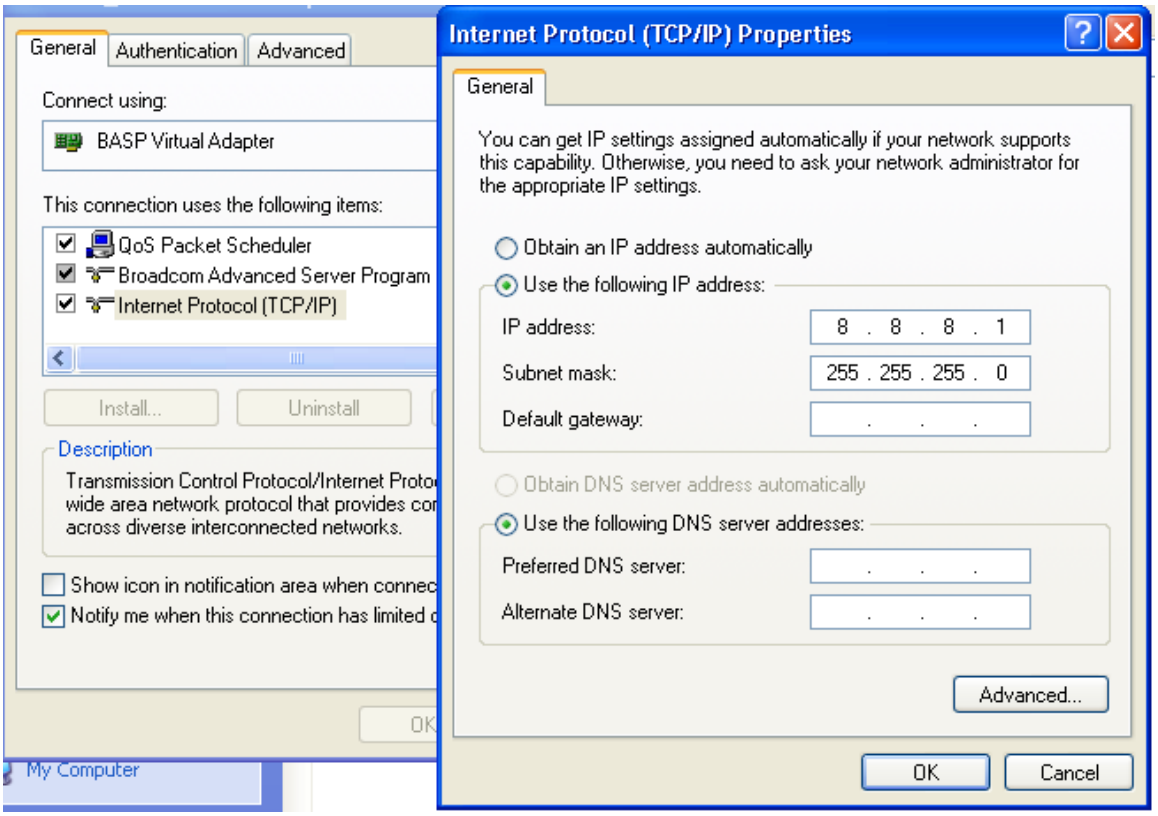

Broadcom Advanced Control Suite 2
File View Tools Help
Name
Network Interfaces(Summary)
[0010] Broadcom NetXtrem
blade_team
Vital Sign
Resources
Hardware
Advanced
Diagnostics
Statistics
Information
Value
MAC Address
00-0D-60-4E-14-A2
Permanent MAC Address
00-0D-60-4E-14-A2
IP Address Setting Reminder
The team configuration has been completed. Please refer to the Network Properties for IP address and Gateway address settings.
In the future, do not show this message.
OK
Duplex
Full
BROADCOM
OK
Cancel
Apply
Help
Enable Tray Icon
To view detailed information or to run a particular test on a selected adapter, click the appropriate tab.

20. Click **OK** to complete the configuration.

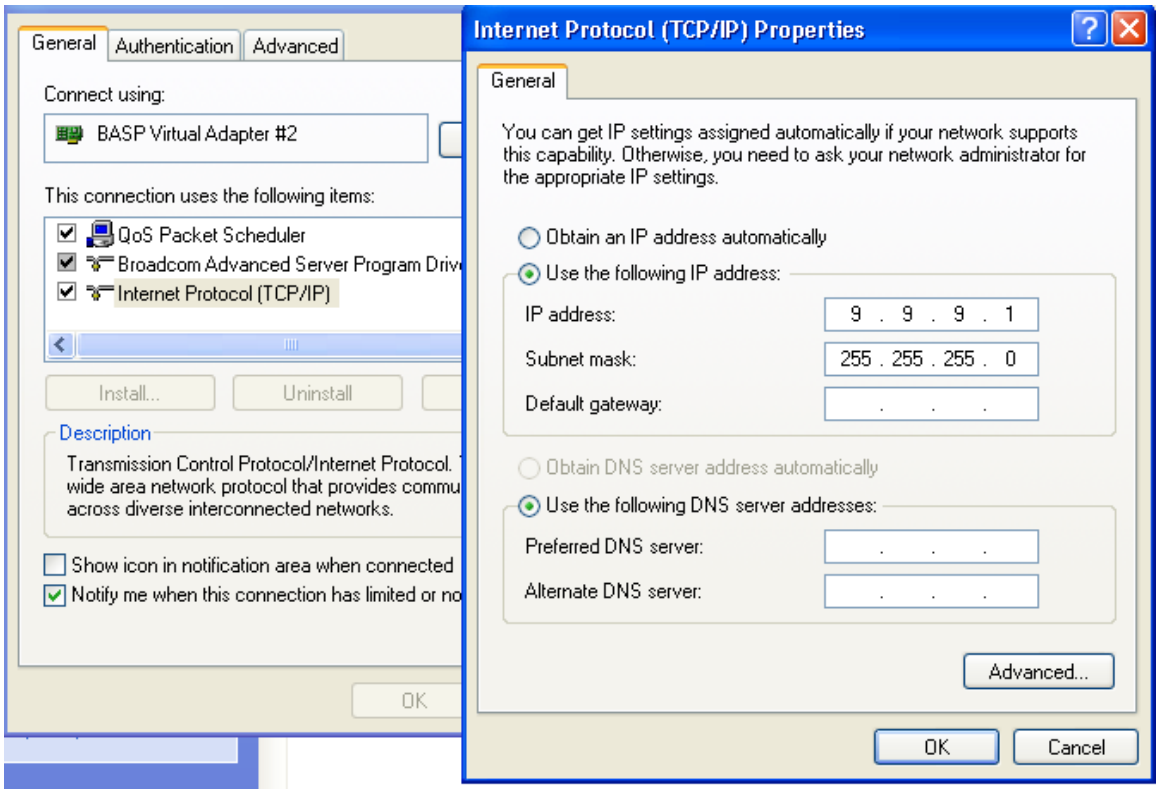


21. From the Start menu, select **Start->Setting->Network Connections** to configure the IP address for the two virtual interfaces that were just created.

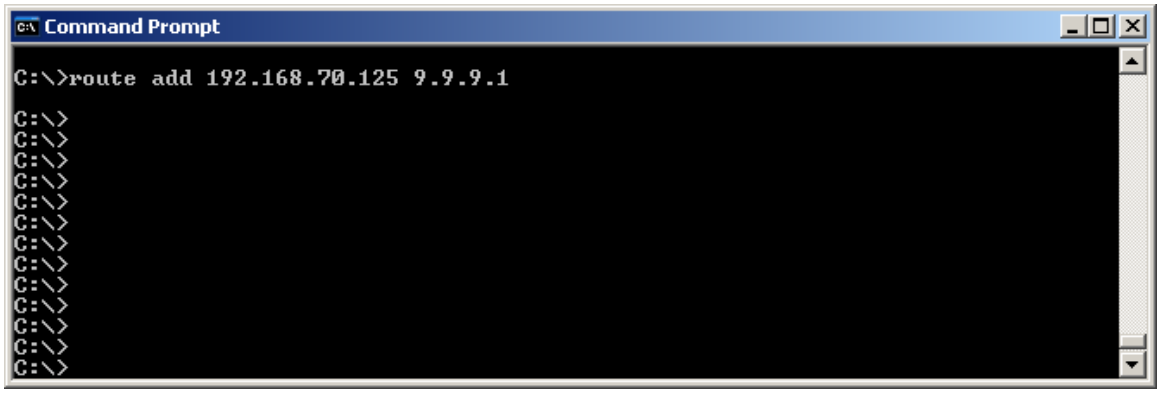
22. Right-click **VLAN_def Virtual Adapter** and select **Properties**; then, select **Internet Protocol (TCP/IP)** and enter the IP address and subnet mask. This is the IP address that will be used to communicate with the Production network.



23. Right-click **VLAN_amm Virtual Adapter** and select **Properties**; then, select **Internet Protocol (TCP/IP)** and enter the IP address and subnet mask. This is the IP address that will be used to communicate with the AMM using the CIN path.

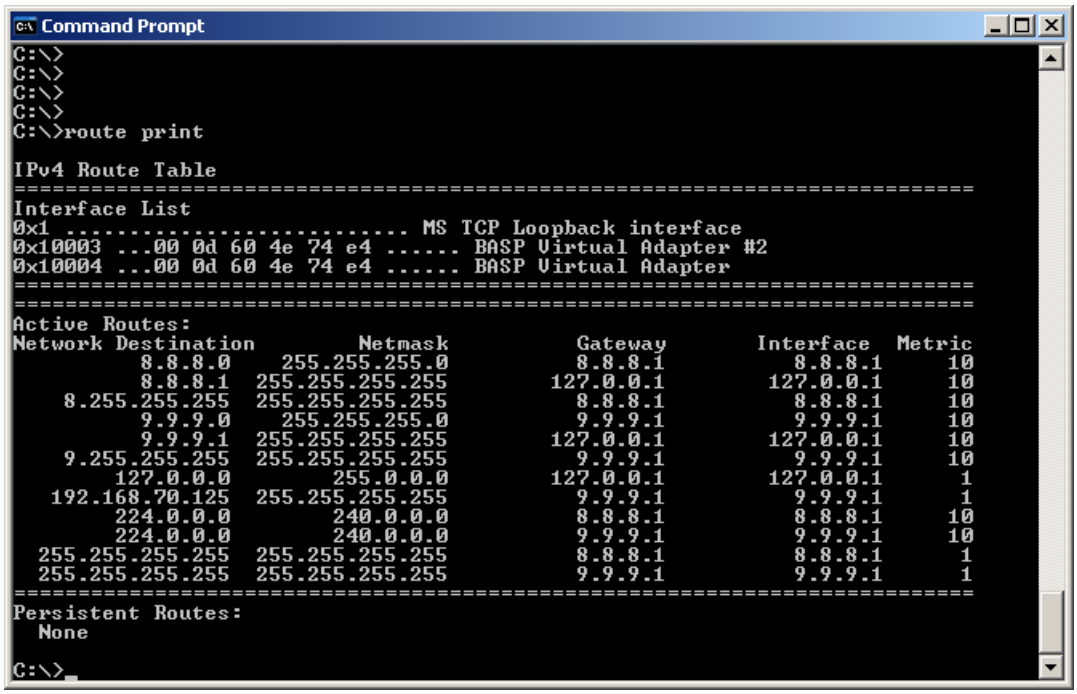


24. Open a command session and set the route for the AMM IP address by entering the following command at the `DOS C:\>` command prompt:
`route add 192.168.70.125 9.9.9.1`

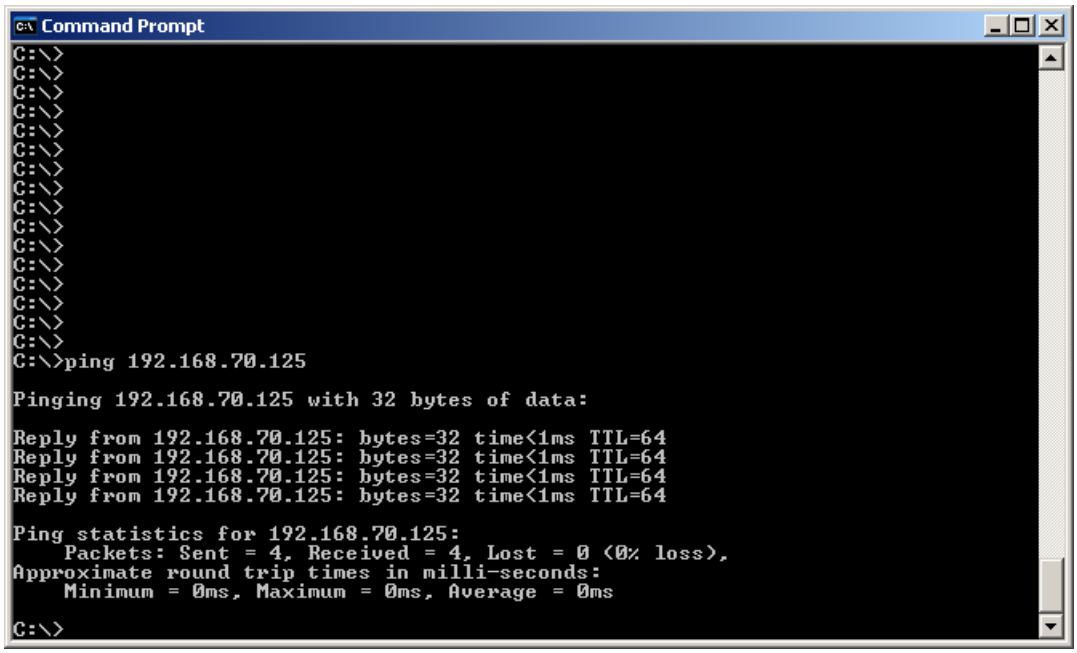


25. Enter the following command at the `DOS C:\>` command prompt:
    `route print`

    An indication should be returned showing that the route to 192.168.70.125 was added successfully.



26. You should now be able to ping from 9.9.9.1 to 192.168.70.125.



The CIN feature is now enabled and correctly configured for this blade device.