System i

System i integration with BladeCenter and System x: iSCSI Network Planning Guide

Version 6 Release 1

System i

System i integration with BladeCenter and System x: iSCSI Network Planning Guide

Version 6 Release 1

Note

Before using this information and the product it supports, read the information in “Notices,” on page 35.

This edition applies to version 6, release 1, modification 0 of IBM i5/OS (product number 5761–SS1) and to all subsequent releases and modifications until otherwise indicated in new editions. This version does not run on all reduced instruction set computer (RISC) models nor does it run on CISC models.

Contents

What’s new for V6R1

Read about new or significantly changed information for the System i® integration with BladeCenter® and System x™ topic collection.

iSCSI Network Planning Guide

The iSCSI Network Planning Guide was moved from the System i integration with BladeCenter and System x (www.ibm.com/systems/i/bladecenter/) Web site to the i5/OS® Information Center.

This guide will help you plan for the connection between the System i hardware and the BladeCenter or System x hardware.

This planning guide is also included in the System i integration with BladeCenter and System x: iSCSI-attached System x and blade Systems PDF file.

How to see what’s new or changed

To help you see where technical changes have been made, the information center uses:

- The » image to mark where new or changed information begins.
- The « image to mark where new or changed information ends.

In PDF files, you might see revision bars (|) in the left margin of new and changed information.

To find other information about what’s new or changed this release, see the Memo to users.

iSCSI Network Planning Guide

Use this guide to plan the network connections for the System i and blade or System x hardware.

You will fill in the work sheets at the end of this document with the values that will help you configure your servers later. Do not fill in the work sheets until directed to do so.

You can download this guide as a separate PDF. See System i integration with BladeCenter and System x: iSCSI Network Planning Guide.

The items in the planning work sheets are referred to throughout this document using item identifiers (IDs). For example the Name entry in the i5/OS service processor configuration object work sheet is referred to using item ID SP1. The following work sheet item ID naming convention is used throughout this guide:

SP*n* Items in the i5/OS service processor configuration object work sheet

XSP*n* Items in the BladeCenter or System x service processor configuration work sheet

RS*n* Items in the i5/OS remote system configuration object work sheet

CQ*n* Items in the iSCSI initiator work sheet

NH*n* Items in the i5/OS network server host adapter object work sheet

CS*n* i5/OS connection security configuration object work sheet

Configuration objects

i5/OS objects configure aspects of the integrated server connection and hardware.

Figure 1 on page 4 shows the hardware, connections, and i5/OS objects for the integrated server. The item IDs for the fields in the iSCSI network planning work sheets are listed next to components in the image. Use this figure to identify the fields as you do the following tasks.

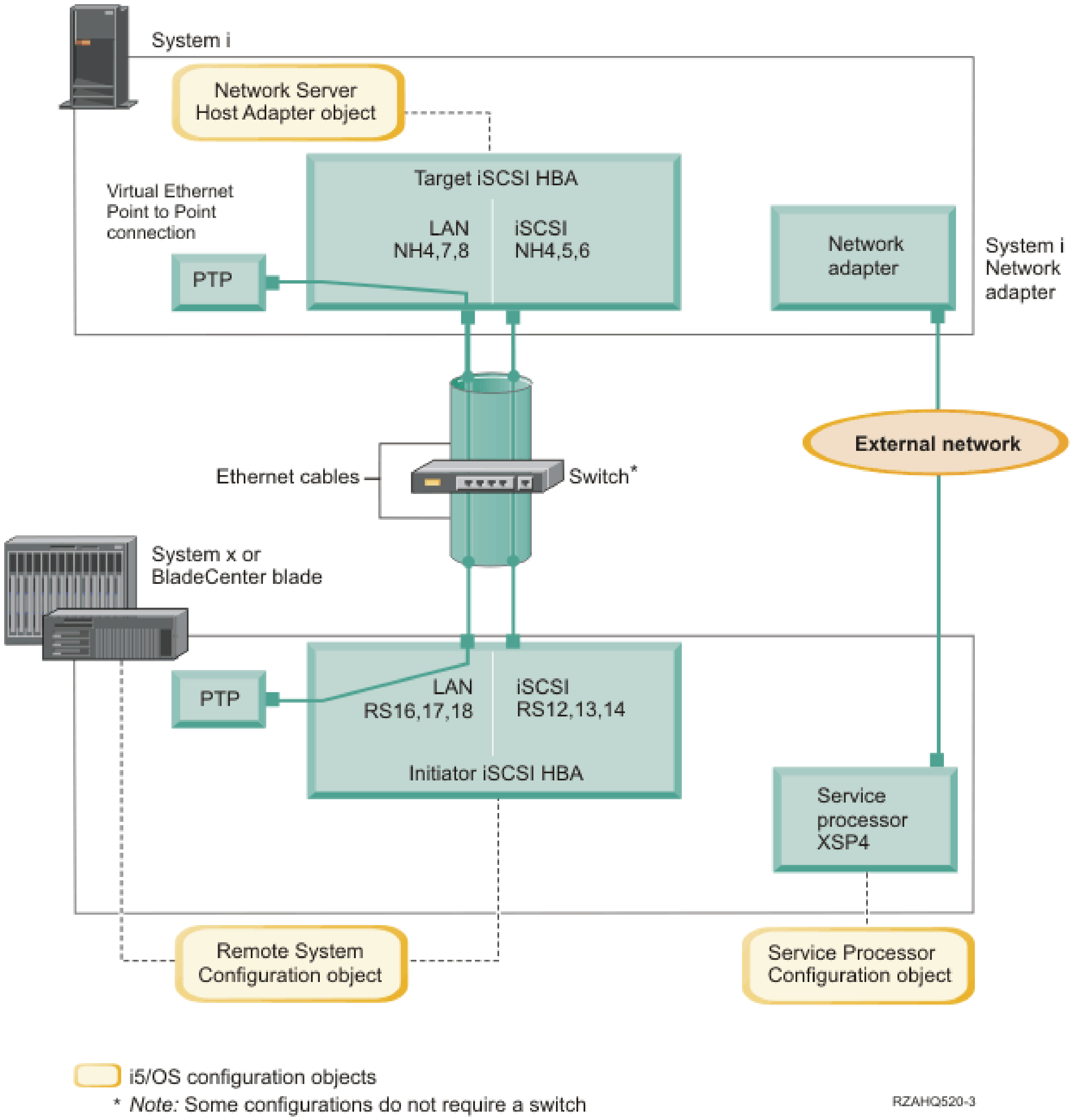

System i
Network Server Host Adapter object
Target iSCSI HBA
Virtual Ethernet Point to Point connection
LAN NH4,7,8
iSCSI NH4,5,6
PTP
Network adapter
System i Network adapter
External network
Ethernet cables
Switch*
System x or BladeCenter blade
PTP
LAN RS16,17,18
iSCSI RS12,13,14
Initiator iSCSI HBA
Service processor XSP4
Remote System Configuration object
Service Processor Configuration object
i5/OS configuration objects
* Note: Some configurations do not require a switch
RZAHQ520-3

Figure 1. i5/OS configuration objects for iSCSI-attached integrated servers

Recording the configuration information

Do these tasks to select an addressing scheme for the iSCSI network for the integrated server.

You should be familiar with the information in Concepts for iSCSI-attached integrated servers.

Planning network addresses

You need to specify some of the network addresses for the iSCSI network for the integrated server.

You need to define values for your iSCSI network that include addresses for all of the connections shown in “Configuration objects” on page 3. If you are not sure what value to use, you can use the values in “Selecting IP addresses for the System x or blade iSCSI initiator” on page 15 and “Selecting IP addresses for the System i iSCSI HBA” on page 19. These examples assume that your iSCSI network uses an isolated Ethernet switch and you do not have another network using IP addresses that start with 192.168.99.

If you plan to use your own address scheme, you can verify it with the addresses in the examples.

Planning for the service processor connection

Do these steps to record the information for the service processor configuration object.

- If you have already created an i5/OS service processor configuration object for the BladeCenter management module or the System x service processor, do the following steps.
  1. Reuse the existing service processor configuration object.
  2. Record the existing service processor configuration object name in work sheet item **SP1**.
  3. Put a check in the box labeled **Existing** in work sheet item **SP1**.
  4. Continue to “Planning for the remote system configuration” on page 9.
- If you need to create a new i5/OS service processor configuration object:
  1. Put a check in the box labeled **New** in worksheet item **SP1**.
  2. Continue with the following tasks.

Related reference

“i5/OS service processor configuration object work sheet” on page 24
Use this work sheet to record the values for the i5/OS service processor configuration object.

Identifying a BladeCenter or System x service processor type

Do these steps to record the type of service processor that is installed in the integrated server hardware.

A BladeCenter enclosure (chassis) can have a:

- Management Module (MM)
- Advanced Management Module (AMM)

A System x model can have a:

- Remote Supervisor Adapter II (RSA II) and a Baseboard Management Controller (BMC)
- BMC only

If you are not sure whether your System x model has an RSA II or just a BMC (without an RSA II), see the BladeCenter and System x models supported with iSCSI Web page (www.ibm.com/systems/i/bladecenter/iscsi/servermodels/).

- If the Web page shows that your System x model has an **Included** or **Required** RSA II SlimLine service processor, then your service processor type is an RSA II.
- If the Web page shows that an RSA II SlimLine service processor is **Optional** for your System x model then you need to check your System x model order information to determine if an RSA II SlimLine service processor (part 73P9341) is included as part of your system configuration.

Put a check in the box next to your service processor type in worksheet item **XSP1**.

Related reference

“i5/OS service processor configuration object work sheet” on page 24
Use this work sheet to record the values for the i5/OS service processor configuration object.

Selecting a service processor discovery method

The service processor is a part of a BladeCenter server or a System x product. It has the interface used to power the server on and off. When i5/OS receives information, it saves the information and presents interfaces for interacting with and managing that server.

For the BladeCenter or System x service processor interface, use an external network, such as a company's campus LAN or intranet, rather than using the iSCSI network. The i5/OS operating system uses this interface to discover the service processor and to manage the state of the hosted system. i5/OS is not set up to run these tasks on the iSCSI network. See "Considerations for connecting service processors to i5/OS" on page 22 for considerations that might affect how you configure your network for i5/OS to service processor communications.

The i5/OS operating system can use the following methods to discover a server on its network. Not all options work for all types of service processors.

Discovery by IP address

- This discovery method is recommended since it supported by all types of service processors and does not require a DNS server or support for multicast addressing.

Discovery by host name

- You can use this discovery method for Remote Supervisor II (RSA II), Management Module, or Advanced Management Module service processors. The network that the service processor is connected to must include a DHCP server.

Discovery by service location protocol (SLP)

You can use this discovery method for Remote Supervisor II (RSA II), Management Module, or Advanced Management Module service processors. This discovery method is supported only if you use IBM® Director to discover the server. If you use the Service Processor Manager function of i5/OS Integrated Server Support, then use either the discovery by IP address or discovery by host name method.

Decide the discovery method you will use for the service processor and do one of the following:

To check which methods work with which service processors, and to see more information on these methods see Service processor connection for integrated servers.

- If you select **discovery by IP address**, do the following steps.
  1. Put a check in the box labeled Internet address in work sheet item **SP4**.
  2. Optional: Record the service processor host name in work sheet item XSP2 (can be blank). If the service processor is connected to the same LAN that your other systems (PCs, servers, etc.) are connected to, then you would normally assign a host name to the service processor using your normal LAN host name assignment policies, the same as if you were adding another PC to your network.
  3. Put a check in the box labeled **Disabled (for DHCP)** in work sheet item **XSP3**.
  4. Fill in address values for work sheet items **XSP4**, **XSP5**, and **XSP6**.

     You need to choose a TCP/IP address subnet that allows the i5/OS operating system and the service processor to communicate readily.

     If the service processor is connected to the same LAN that your other systems (PCs, servers, etc.) are connected to, then you would normally assign an IP address to the service processor using your normal LAN IP address assignment policies, the same as if you were adding another PC to your network.
- If you **select discovery by host name**, do the following steps.
  1. Put a check in the box labeled Host name in work sheet item **SP3**.

2. Record the service processor host name in work sheet item **XSP2**. If the service processor is connected to the same LAN that your other systems (PCs, servers, etc.) are connected to, then you would normally assign a host name to the service processor using your normal LAN host name assignment policies, the same as if you were adding another PC to your network.

   Important: Make sure that the service processor host name that you specify is registered in your network domain name server (DNS).
3. Put a check in the box labeled **Enabled** (for DHCP) in work sheet item **XSP3**.
4. Leave work sheet items **XSP4**, **XSP5**, and **XSP6** blank.

Related reference

"i5/OS service processor configuration object work sheet" on page 24
Use this work sheet to record the values for the i5/OS service processor configuration object.

Recording the system serial number and type/model

Do these steps to record the serial and type/model information for the integrated server hardware.

1. On the BladeCenter or System x chassis, find the label that contains the system serial number, type and model values. If you are installing a blade, find the values for the BladeCenter chassis. Do not use the label on the blade.
2. If you are installing a System x model with only a BMC service processor (no RSA II) installed, leave worksheet items **SP5** and **SP6** blank. Continue to "Assigning an i5/OS Server Processor Configuration object name."
3. For all other configurations, do the following steps.
   a. Record the serial number value in worksheet item **SP5**.
   b. Record the type and model values in worksheet item **SP6**. Do not include a space or dash ('-') in the type and model value. For example, record `88721RU` for a System x model x460 with type 8872 and model 1RU.

Related reference

"i5/OS service processor configuration object work sheet" on page 24
Use this work sheet to record the values for the i5/OS service processor configuration object.

Assigning an i5/OS Server Processor Configuration object name

You need to assign a name to the i5/OS service processor configuration object that you will create to configure the i5/OS connection to the BladeCenter or System x service processor.

The service processor configuration object name can be from 1 to 10 characters in length, consisting of characters a-z, A-Z, 0-9 and special characters '$', '#' and '@'. The first character cannot be a number.

You can define your own naming convention to help you associate the service processor configuration name to the physical hardware (BladeCenter or System x model) that contains the service processor.

For example, you could use SP*sssssss* where *sssssss* is the last 7 characters of the BladeCenter chassis (not the blade) or the System x serial nmber.

Notes:

1. The service processor configuration name cannot match the associated i5/OS remote system configuration name.
2. Using the NWSD name as part of the service processor configuration name works fine for simple configurations where there is a one-to-one relationship between NWSDs and service processors. However, in more complex configurations, the same service processor configuration might be used by multiple NWSDs. For example, multiple NWSDs could be defined to use the same service processor hardware (multiple blades in a BladeCenter) or the NWSD could be switched to use different "hot spare" server hardware, so that the service

processor configuration is used with a different NWSD than it was originally created for. In these cases, it might be confusing to use the NWSD name as part of the service processor configuration name.

Record values for the following work sheet items.

1. Fill in the name you choose in work sheet item **SP1**.
2. Fill in a description of the object (up to 50 characters) in item **SP2**.

Related reference

"i5/OS service processor configuration object work sheet" on page 24
Use this work sheet to record the values for the i5/OS service processor configuration object.

Selecting a Login ID and Password for the Service Processor

When you connect directly to the BladeCenter or System x service processor via a LAN, you must specify a login ID (user name) and password.

It is strongly recommended that you define a unique login ID that will be used only by the i5/OS partition or system that will control your BladeCenter or System x through its service processor. Each BladeCenter or System x service processor can only have one controlling partition or system. A BladeCenter Advanced Management Module (AMM) allows more than one controlling partition or system if properly configured – see "Considerations for multiple connections to a BladeCenter Advanced Management Module" on page 9. Use a naming convention that ties the service processor login ID to the hosting i5/OS logical partition (or the system name for a non-partitioned system). For example, if the hosting i5/OS logical partition name is ROCH03, then the service processor login ID could be set to ROCH03.

You can use the system BIOS interface, the Management Module (MM) or Advanced Management Module (AMM), or the RSA II Web interfaces to set the login ID and password. You also need this information to synchronize the i5/OS service processor configuration with the BladeCenter or System x service processor before installing the operating system on the server. i5/OS uses the login ID and password to connect to the System x or blade model to do specific management tasks (for example, to start the server).

Important: In order for the unique login ID to be effective, it is strongly recommended that you do the following where instructed in later steps.

- Disable or change the default login ID. Service processors have a default login ID of USERID (upper case) with a password of PASSW0RD (upper case, where 0 is the number 0 instead of the letter O). This action protects against unauthorized access to your server.
- If the service processor is currently configured with login IDs that are used by management servers other than the local i5/OS host system (Service Processor Manager or IBM Director Server on another system), disable these login IDs.

If your company has multiple installations of management servers on the same network, take previously mentioned actions to ensure that the service processor does not refuse a connection from the i5/OS operating system. Connection refusal occurs when another management server is already connected. For more information, see Service Processor Connection Refused in the IBM Software Knowledge Base.

1. Fill in the new **Login ID** and **Password** values for i5/OS to use in worksheet items **XSP7** and **XSP8**.
2. If the service processor is a Management Module in a BladeCenter or an RSA II in a System x model, you can configure **additional login IDs** and passwords for your administrators to access the service processor from any web browser connected on the same network. If you want to do this, fill in the new **Login ID** and **Password** values for your administrators to use in worksheet items **XSP9** and **XSP10**. You can create up to 12 login ID/password combinations in each service processor. For most environments, you should create an additional login ID and password for use by your administrators.

Related reference

"i5/OS service processor configuration object work sheet" on page 24
Use this work sheet to record the values for the i5/OS service processor configuration object.

"BladeCenter or System x service processor work sheet" on page 26
Use this work sheet to plan the values for the BladeCenter or System x service processor.

Considerations for multiple connections to a BladeCenter Advanced Management Module

If you have a BladeCenter system with an Advanced Management Module (AMM) and firmware BPET23A or later, it can be configured to allow more than one controlling partition or system.

The AMM allows multiple concurrent command mode connections. These connections can be used to allow several management servers (Service Processor Managers or IBM Director Servers), to control the blades in the IBM BladeCenter system.

- Each blade within the BladeCenter should still be controlled (varied on) by a single partition or system at any one time.
- You should change the default Login ID and password for the AMM or disable it as mentioned above. Each partition or system can share Login IDs and passwords or each can have its own unique Login ID and password.
- Each partition or system will need its own i5/OS service processor configuration object for the BladeCenter AMM and each i5/OS service processor configuration object must be synchronized with the BladeCenter AMM.

The AMM must be configured to allow concurrent command-mode connections. The AMM Web interface is used to do this:

1. Sign on to the AMM web interface.
2. Select **Network Protocols** under **MM control**.
3. Page down to the **TCP Command Mode Protocol** section.
4. Change the **command mode** value to the number of desired concurrent connections.
5. Required: Restart the AMM. Use the **Restart MM** option under the **MM control** section.
6. Use the **Login Profiles** under **MM control** to add, change or disable Login IDs and passwords.

Planning for the remote system configuration

The remote system configuration object defines the communications connections for iSCSI and virtual Ethernet traffic for the System x or blade hardware that will be connecting to the i5/OS operating system.

- If you have already created a remote system configuration object for the System x or blade hardware:
  - Reuse the existing remote system configuration object.
  - Record the existing remote system configuration object name in worksheet item **RS1**.
  - Put a check in the box labeled **Existing** in worksheet item **RS1**.
  - Continue with "Planning for the network server host adapter (NWSH) object" on page 17.
- If you need to create a new i5/OS remote system configuration object:
  - Put a check in the box labeled **New** in worksheet item **RS1**.
  - Continue with the following tasks.

Related reference

"i5/OS remote system configuration object work sheet" on page 27
Use this work sheet to select the parameters you will use to create the remote system configuration object for the integrated server.

Recording the blade system serial number and type/model

Do these steps if you are installing a blade system.

1. Open the transparent cover on the front face of the blade server.

2. Record the blade serial number value in worksheet item **RS4**.
3. Record the blade type and model values in worksheet item **RS5**.

   Note: Do not include a space or dash (-) in the type and model value.
   For example, record `8843E9U` for an HS20 blade with type 8843 and model E9U.

Related reference

"i5/OS remote system configuration object work sheet" on page 27
Use this work sheet to select the parameters you will use to create the remote system configuration object for the integrated server.

Selecting a name for the remote system configuration

You need to assign a name to the i5/OS remote system configuration object that you will create to configure the attributes of the iSCSI attached BladeCenter blade or System x model.

The remote system configuration object name can be from 1 to 10 characters in length, consisting of characters a-z, A-Z, 0-9 and special characters '$', '#' and '@'. The first character cannot be a number.

You can define your own naming convention to help you associate the remote system configuration name to the physical server hardware (BladeCenter blade or System x model).

An example naming convention that provides the suggested hardware association is RS*sssssss* where *sssssss* is the last 7 characters of the BladeCenter blade (not chassis) or System x serial number. The appropriate serial number was previously recorded in worksheet item **SP5** for a System x model or worksheet item **RS4** for a blade.

Notes:

1. The remote system configuration name cannot match the associated i5/OS service processor configuration name.
2. You can use the NWSD name as part of the remote system configuration name for simple configurations where there is a one-to-one relationship between NWSDs and the hardware that they use.

   However, in more complex configurations, the same remote system configuration might be used by multiple NWSDs. For example, multiple NWSDs could be defined to use the same remote system hardware (multiple production or test servers defined to use the same System x hardware at different points in time) or the NWSD could be switched to use different "hot spare" server hardware, so that the remote system configuration is used with a different NWSD than it was originally created for. In these cases, it might be confusing to use the NWSD name as part of the remote system configuration name.

1. Fill in the name you choose in worksheet item **RS1**.
2. Fill in a description of the object (up to 50 characters) in item **RS2**.

Related reference

"i5/OS remote system configuration object work sheet" on page 27
Use this work sheet to select the parameters you will use to create the remote system configuration object for the integrated server.

Selecting a boot parameter delivery method

An integrated server iSCSI HBA must be configured after it is installed in the System x or blade hardware. Do these steps to select the parameters that you will use.

Before you begin, you need to decide whether to use dynamic addressing (the default) or to use manual addressing for your iSCSI initiator. See Boot modes and parameters for more information about dynamic addressing using the built-in DHCP server. After you begin installing the integrated server, use the iSCSI initiator configuration interface to specify parameters.

You can select either dynamic or manual addressing.

You can use dynamic addressing for most environments. This method requires fewer manual configuration steps and allows some configuration information to be automatically generated, such as iSCSI qualified names (IQNs). With dynamic addressing, the iSCSI attached server uses an integrated DHCP server and you do not need to have a general purpose DHCP server in your network. The integrated DHCP server is intended exclusively to deploy boot parameters to the iSCSI initiator and is not a general purpose DHCP server. When a network server description (NWSD) is varied on, the initiator system is automatically configured with the parameters provided in the i5/OS remote system configuration object.

If you use manual addressing method, some integrated server functions are more difficult to implement, such as the integrated server hot spare capability.

You need the values that you record in the iSCSI network planning work sheets for either method.

- If you use **dynamic** addressing, you configure the parameters in the i5/OS remote system configuration object and the system sends them to the initiator system.
- If you use **manual** addressing, you need to configure both the remote system configuration object in i5/OS and the iSCSI initiator.

1. Put a check in the box next to the boot parameter delivery method you choose in work sheet item **RS6**.
2. Based on your choice for item **RS6**, do one of the following:
   - If you chose **Dynamically delivered to remote system via DHCP**:
     a. Put a check in the box next to the **Dynamic column** heading in the iSCSI initiator work sheet.
     b. Put a check in the box next to DHCP for Port 1 in work sheet item **CQ9**.
   - If you chose **Manually configured on remote system**:
     a. Put a check in the box next to the **Manual** column heading in the iSCSI initiator work sheet.
     b. Put a check in the box next to **Manual** for Port 1 in worksheet item **CQ9**.

Only one of the iSCSI initiator ports can be configured as the boot device during the server installation (the adapter boot mode is set to DHCP or Manual in the iSCSI initiator configuration utility). All other ports must be disabled for boot (the adapter boot mode is set to Disabled in the iSCSI initiator configuration utility), but can be used for non-boot storage or virtual Ethernet traffic.

Note: After the server installation is completed, if the server operating system supports multipath I/O, then additional ports can be enabled for boot.

Related reference

"i5/OS remote system configuration object work sheet" on page 27
Use this work sheet to select the parameters you will use to create the remote system configuration object for the integrated server.

Selecting Challenge Handshake Authentication Protocol (CHAP) settings

Challenge Handshake Authentication Protocol (CHAP) is used to authenticate the connection between the System x or blade initiator and the System i target.

CHAP protects against the possibility of an unauthorized system using an authorized system's iSCSI name to access storage. CHAP does not encrypt network traffic, but rather limits which system can access an i5/OS storage path.

There are two types of CHAP authentication.

One-way CHAP
The target (System i) authenticates the initiator (System x or blade).

Bidirectional CHAP

In addition to the one-way CHAP authentication described above, the initiator (System x or blade) also authenticates the target (System i). Bidirectional CHAP is supported in environments that use i5/OS V6R1 or later.

If you do not want to use CHAP, select **Disabled** for "i5/OS remote system configuration object work sheet" on page 27 items **RS7** and **RS10**. Continue with "Selecting maximum transmission unit (MTU) setting for the iSCSI network" on page 13.

Related reference

"i5/OS remote system configuration object work sheet" on page 27
Use this work sheet to select the parameters you will use to create the remote system configuration object for the integrated server.

Selecting parameters for target CHAP authentication for iSCSI-attached integrated servers:

Do the following steps to select parameters for target CHAP authentication.

1. Put a check next to **Enabled** in "i5/OS remote system configuration object work sheet" on page 27 item **RS7**.
2. Record the CHAP name in "i5/OS remote system configuration object work sheet" on page 27 item **RS8**. You can use the remote system configuration object name from item **RS1** as the CHAP name.
3. Record the CHAP secret.

   There are two approaches to assigning a CHAP secret. The strength of the CHAP secret that you should use depends on your environment.

   - If the iSCSI network is physically secure and there is no possibility that unauthorized parties can monitor the iSCSI network traffic, you can use a unique non-trivial CHAP secret that you assign. For example, use a combination of letters and numbers that is at least 8 characters long. If you choose this approach, then record the CHAP secret you choose in "i5/OS remote system configuration object work sheet" on page 27 item **RS9**.
   - If the iSCSI network is not physically secure or there is a possibility that unauthorized parties can monitor the iSCSI network traffic, use the remote system configuration option to generate a strong CHAP secret. If you choose this approach, then put a check in the box next to **Generate** in "i5/OS remote system configuration object work sheet" on page 27 item **RS9** and leave the CHAP secret value blank for now.

Selecting parameters for initiator CHAP authentication for iSCSI-attached integrated servers:

Use this information to select settings for initiator CHAP authentication.

If you do not want to configure initiator CHAP, select **Disabled** for "i5/OS remote system configuration object work sheet" on page 27 configuration item **RS10**. Continue with "Selecting maximum transmission unit (MTU) setting for the iSCSI network" on page 13.

If you want to configure initiator CHAP, do the following steps to select parameters.

1. Put a check next to **Enabled** in "i5/OS remote system configuration object work sheet" on page 27 item **RS10**.
2. Record the CHAP name in "i5/OS remote system configuration object work sheet" on page 27 item **RS11**. You can use the remote system configuration object name from item **RS1** as the CHAP name.
3. Record the CHAP secret.

   There are two approaches to assigning a CHAP secret. The strength of the CHAP secret that you should use depends on your environment.

   - If the iSCSI network is physically secure and there is no possibility that unauthorized parties can monitor the iSCSI network traffic, you can use a unique non-trivial CHAP secret that you assign. For example, use a combination of letters and numbers that is at least 8 characters long. If you choose this approach, then record the CHAP secret you choose in “i5/OS remote system configuration object work sheet” on page 27 item **RS12**.

- If the iSCSI network is not physically secure or there is a possibility that unauthorized parties can monitor the iSCSI network traffic, use the remote system configuration option to generate a strong CHAP secret. If you choose this approach, then put a check in the box next to **Generate** in “i5/OS remote system configuration object work sheet” on page 27 item **RS12** and leave the CHAP secret value blank for now.

Selecting maximum transmission unit (MTU) setting for the iSCSI network

The iSCSI network MTU value can be set to 1500 (normal frames) or 9000 (jumbo frames).

The iSCSI network normally uses standard 1500 byte frames. It is possible to configure iSCSI HBAs to use larger frames on the iSCSI network. However, under heavy traffic, many switches do not perform well with larger frames, degrading performance of both storage and virtual Ethernet. If you are not sure that your switch performs well with larger frames, it is recommended that you use the default settings for 1500 byte frames. As long as switch limitations are not affecting performance, setting the iSCSI HBA and switch MTU configuration to 9000 typically improves performance, especially virtual Ethernet performance. If you plan to use jumbo frame support, you need to configure it on the switch, if not already enabled.

Do the following steps to record the MTU settings that you will use.

1. Put a check in the box next to your Port 1 MTU choice in worksheet item **CQ16**.
2. If your server has a second port (for example, a blade with a dual port iSCSI HBA), then also put a check in the box next to your Port 2 MTU choice in worksheet item **CQ16**.

Related reference

“i5/OS remote system configuration object work sheet” on page 27
Use this work sheet to select the parameters you will use to create the remote system configuration object for the integrated server.

Recording iSCSI initiator (local adapter) MAC addresses

Do these steps to record the iSCSI initiator local adapter (MAC) address for your remote system configuration object. Depending on your iSCSI HBA type, do one of the following:

Depending on the iSCSI initiator adapter type, look in the following locations for the adapter address.

- For a System x model, the iSCSI initiator is either an iSCSI HBA or an Ethernet Network Interface Card (NIC). Note the label that is attached to the tail stock (or on the system unit for an embedded Ethernet NIC) with sets of 12–digit hexadecimal values. These are unique addresses that are assigned for the adapter.

  Important: The System x iSCSI HBA parts 30R5201 and 30R5501 look identical to the System i iSCSI HBA features 5783 and 5784, but they have different firmware, so they are not interchangeable. If you get them mixed up and use an iSCSI HBA in the wrong system, it does not work. If you are not sure which system type a particular iSCSI HBA is for, look for the CCIN values on the tail stock of the iSCSI HBA card. See iSCSI host bus adapter (iSCSI HBA) for a list of iSCSI HBAs and the associated CCIN values.

- For a blade model, the iSCSI initiator adapter is either an iSCSI HBA I/O expansion module on the blade or an Ethernet NIC on the blade. There are labels on the box of the adapter and on the adapter itself. The label has sets of 12–digit hexadecimal values. These are unique addresses that are assigned for the adapter. For iSCSI HBAs with two ports, the label shows four addresses. Each port has an iSCSI address and a TOE address. For Ethernet NICs with two ports, the label shows two addresses.

For more information about these addresses, see iSCSI Network.

Note: Record the MAC addresses. Later on, you use the iSCSI initiator configuration function to configure the adapters and you can verify the values. The management Module Web interface can show the addresses (use the Hardware VPD link and look under the BladeCenter Server MAC addresses).

For an iSCSI HBA, perform the following steps to record the iSCSI initiator local adapter (MAC) address.

1. Look for the word 'iSCSI' on the label. Record the address information in pairs of digits in work sheet item **RS13**. A portion of the address is filled in for you, one example is for a System x adapter and the other is for a blade adapter. Choose the example that matches the first 3 sets of characters. The iSCSI connection is used for disk traffic.
2. Look for the word 'TOE' on the label. Record the address information in pairs of digits in work sheet item **RS17**. A portion of the address is filled in for you, one example is for a System x adapter and the other is for a blade adapter. Choose the example that matches the first 3 sets of characters. TOE stands for TCP Offload Engine. Think of it as an I/O processor for the adapter. The TOE is used for virtual Ethernet LAN traffic.

For an Ethernet NIC that is used as an iSCSI initiator, look for the word MAC on the label. Record the address information in pairs of digits in work sheet items RS13 and RS17. Note that the same adapter address is used for both the SCSI and LAN interfaces.

Related reference

"i5/OS remote system configuration object work sheet" on page 27
Use this work sheet to select the parameters you will use to create the remote system configuration object for the integrated server.

Selecting IP addresses for the System x or blade iSCSI initiator

You need to select an IP address scheme for SCSI and LAN interfaces of the iSCSI initiator before you configure your server. You can use the sample information in this table or use your own scheme.

You can use the convention in this example for up to 19 hosted systems connected to the same switch. The shaded portions signify addressing for additional adapters in the same server. If you want to plan for more than 19 hosted systems on the same switch, see "Expanding on the iSCSI network addressing scheme for integrated servers" on page 20.

Notes:

1. The last digits of the Internet address is a concatenation of a system number and a port number (for example, system 1, port 1 = 11. Add 4 to this for the LAN addresses). If you use this convention, you can assign any numbers to systems, ports, and iSCSI initiators within the indicated ranges.
2. This table gives sample IP addresses for the physical iSCSI network. Do not use these IP addresses for any virtual Ethernet networks you might have. The physical network and the virtual Ethernet network must use IP addresses on different subnets. If you have a network for your Hardware Management Console (HMC), it should not be on the same subnet as the iSCSI or virtual Ethernet networks.

Table 1. Sample address scheme for the iSCSI network

	Configuration parameter	**iSCSI port 1**	**iSCSI port 2**	**iSCSI port 3**	**iSCSI port 4**
Hosted system 1	SCSI interface				
	Internet address	192.168.99.**11**	192.168.99.**12**	192.168.99.**13**	192.168.99.**14**
	Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
	Gateway address[1]	blank	blank	blank	blank
	LAN interface				
	Internet address	192.168.99.**15**	192.168.99.**16**	192.168.99.**17**	192.168.99.**18**
	Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
	Gateway address[1]	blank	blank	blank	blank
Hosted system 2	SCSI interface				
	Internet address	192.168.99.**21**	192.168.99.**22**	192.168.99.**23**	192.168.99.**24**
	Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
	Gateway address[1]	blank	blank	blank	blank
	LAN interface				
	Internet address	192.168.99.**25**	192.168.99.**26**	192.168.99.**27**	192.168.99.**28**
	Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
	Gateway address[1]	blank	blank	blank	blank
...	...	...	...	...	...
Hosted system 19	SCSI interface				
	Internet address	192.168.99.**191**	192.168.99.**192**	192.168.99.**193**	192.168.99.**194**
	Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
	Gateway address[1]	blank	blank	blank	blank
	LAN interface				
	Internet address	192.168.99.**195**	192.168.99.**196**	192.168.99.**197**	192.168.99.**198**
	Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
	Gateway address[1]	blank	blank	blank	blank

Note: You can leave the gateway address blank because these System x and blade iSCSI initiators are on the same switch and subnet as the System i iSCSI targets. Routers are not supported in the iSCSI network.

Do these steps to record IP addresses.

1. Fill in the **SCSI interface internet address and subnet mask** from the table above (or use your own value) in work sheet items **RS14** and **RS15**.
2. Fill in the **LAN interface internet address** and subnet mask from the table above (or use your own value) in work sheet items **RS18** and **RS19**.

   Related reference

   "i5/OS remote system configuration object work sheet" on page 27
   Use this work sheet to select the parameters you will use to create the remote system configuration object for the integrated server.

Selecting the initiator iSCSI Qualified Name (IQN)

If you checked **Manually configured on remote system** (manual addressing) for the **Boot parameter delivery method** in worksheet item RS6, then you need to configure the initiator (System x or blade) iSCSI Name (IQN) value manually.

The initiator iSCSI Name (IQN) format is:

iqn.1924-02.com.ibm:*sssssss*.i*p*

where

- *sssssss* is the serial number of the System x (see item SP5) or blade (see item RS4) server in lower case characters
- *p* is the System x/blade iSCSI HBA interface/port number (0=first interface/port).

Record the initiator IQN values in worksheet item **CQ6.**

Related reference

"i5/OS remote system configuration object work sheet" on page 27
Use this work sheet to select the parameters you will use to create the remote system configuration object for the integrated server.

Selecting the target iSCSI Qualified Name (IQN)

If you checked **Manually configured on remote system** (manual addressing) for the **Boot parameter delivery method** in worksheet item **RS6**, then you need to configure the target (System i) iSCSI Name (IQN) value manually.

The target iSCSI Name (IQN) format is

iqn.1924-02.com.ibm:*sssssssi*.*nnnnnnnn*.t*p*

where

- *sssssss* is the System i serial number in lower case letters.

  Note: You can display the System i serial number by entering `DSPSYSVAL QSRLNBR` at the i5/OS command line.
- *i* is the System i logical partition ID.
- *nnnnnnnn* is the network server description (NWSD) name in lower case.
- *p* is the storage path number from the NWSD (1=first and only storage path for new installations).

Record the target IQN value in worksheet item **CQ10**.

Related reference

"i5/OS remote system configuration object work sheet" on page 27
Use this work sheet to select the parameters you will use to create the remote system configuration object for the integrated server.

Planning for the network server host adapter (NWSH) object

The network server host adapter (NWSH) device description defines the communications connections for iSCSI and virtual Ethernet traffic to i5/OS.

An NWSH object represents a port for an iSCSI host bus adapter (HBA) that is installed inside the System i product or its associated expansion units.

- If you have already created a NWSH device description for the port for the target iSCSI HBA installed in the System i product, use the existing object.

1. Record the existing NWSH object name in worksheet item **NH1**.
2. Put a check in the box labeled **Existing** in worksheet item **NH1**.
3. Look up the local SCSI interface internet address in the NWSH and record it in worksheet item **NH5**. See Displaying network server host adapter properties.
4. Go to "Planning for the i5/OS connection security configuration object" on page 19.

- If you need to create a new i5/OS remote system configuration object:
  1. Put a check in the box labeled **New** in worksheet item **NH1**.
  2. Continue with the following tasks.

Related reference

"i5/OS network server host adapter object work sheet" on page 32
Use this work sheet to plan the parameters you will use to create the network server host adapter (NWSH) object.

Selecting a name for the NWSH

You need to assign a name to the i5/OS network server host adapter (NWSH) device description object that you will create to configure the System i iSCSI HBA.

The NWSH name can be from 1 to 10 characters in length, consisting of characters a-z, A-Z, 0-9 and special characters '$', '#' and '@'. The first character cannot be a number.

You can define your own naming convention for the NWSH name.

An example naming convention that associates the NWSH with the iSCSI HBA hardware is:

NH*sssssss*

where *sssssss* is the last 7 characters of the System i iSCSI HBA serial number.

1. Fill in the name you choose in worksheet item **NH1**.
2. Also fill in a description of the object (up to 50 characters) in item **NH2**.

Related reference

"i5/OS network server host adapter object work sheet" on page 32
Use this work sheet to plan the parameters you will use to create the network server host adapter (NWSH) object.

Selecting a hardware resource name

The iSCSI HBA hardware resource name will not be available until the iSCSI HBA is actually installed in the System i platform.

Leave worksheet item **NH3** blank. You will fill in this value after you install the target iSCSI HBA in the System i product.

Related reference

"i5/OS network server host adapter object work sheet" on page 32
Use this work sheet to plan the parameters you will use to create the network server host adapter (NWSH) object.

Selecting a connection type for the NWSH

There are two ways that iSCSI HBAs in a System i product can physically connect to a System x or a blade system.

- If this Network server host adapter (NWSH) object will be connected to an Ethernet switch, put a check in the box by **Network** in "i5/OS network server host adapter object work sheet" on page 32 item **NH9**.

- If this Network server host adapter (NWSH) object will be connected directly to an iSCSI HBA port in a System x product or to a pass through module in a blade system, put a check in the box next to **Direct** in "i5/OS network server host adapter object work sheet" on page 32 item **NH9**.

Selecting IP addresses for the System i iSCSI HBA

Use this information to select IP addresses for the target iSCSI HBA installed in the System i product.

The information from the table below can be used to configure SCSI and LAN interfaces for your System i iSCSI HBA(s). You can use the convention in this example for up to 19 System i HBAs connected to the same switch. If you want to plan for more than 19 System i HBAs on the same switch, see section 4.1 Expanding on the iSCSI network addressing scheme, for additional considerations. The shaded columns designate having more than one iSCSI HBA in the System i platform.

- For System i i iSCSI HBAs, the last digit is 200 + an iSCSI HBA number (+ 20 more for LAN). If you use this convention, you can assign numbers to systems, ports and iSCSI HBAs within the indicated ranges any way you want.
- This table gives suggested IP addresses for the physical iSCSI network. Do not use these IP addresses for any virtual Ethernet networks you might have. The physical network and the virtual Ethernet network must use IP addresses on different subnets. If you have a network for your HMC, it should not be on the same subnet as the iSCSI or virtual Ethernet networks.

Table 2. Suggested IP addresses for the physical iSCSI network

	Configuration parameter	**iSCSI HBA 1**	**iSCSI HBA 2**	**iSCSI HBA 3**	**...**	**iSCSI HBA 19**
System i	Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0	...	255.255.255.0
	SCSI interface					
	Internet address	192.168.99.**201**	192.168.99.**202**	192.168.99.**203**	...	192.168.99.**219**
	Gateway address[1]	blank[1]	blank[1]	blank[1]	...	blank[1]
	LAN interface					
	Internet address	192.168.99.**221**	192.168.99.**222**	192.168.99.**223**	...	192.168.99.**239**
	Gateway address[1]	blank[1]	blank[1]	blank[1]	...	blank[1]

Note:

1. You can leave the gateway address blank because these System x and blade iSCSI HBAs will be on the same switch and subnet as the System i HBAs. Routers are not supported in the iSCSI network.

1. Fill in the **Subnet mask** in worksheet item **NH4**.
2. Fill in the **SCSI interface internet address** and **gateway** in worksheet items **NH5** and **NH6**.
3. Fill in the **LAN interface internet address** and **gateway** in worksheet items **NH7** and **NH8**.

Related reference

"i5/OS network server host adapter object work sheet" on page 32
Use this work sheet to plan the parameters you will use to create the network server host adapter (NWSH) object.

Planning for the i5/OS connection security configuration object

A connection security configuration object is required for iSCSI-attached integrated servers. All of the iSCSI-attached integrated servers on your system can share the same connection security configuration object.

You should not change any settings for this object.

1. If you have an existing connection security configuration object:
   a. Reuse the existing connection security configuration object.

   b. Record the existing connection security configuration object name in work sheet item **CS1**.
   c. Put a check in the box labeled **Existing** in work sheet item **CS1**.
   d. Skip the remainder of this section.
2. If you need to create a new i5/OS connection security configuration object:
   a. Put a check in the box labeled **New** in worksheet item **CS1**.
   b. Continue with the following task.

   Related reference

   "i5/OS connection security configuration object work sheet" on page 33
   Use this work sheet to record the parameters for the network security configuration object.

Assigning a connection security configuration object name

Select a name for the i5/OS connection security configuration object.

The connection security configuration object name can be from 1 to 10 characters in length, consisting of characters a-z, A-Z, 0-9 and special characters '$', '#' and '@'. The first character cannot be a number.

Use the same connection security object for all iSCSI attached servers that are connected to your i5/OS partition. It is recommended to use a fixed name such as NOIPSEC for the connection security configuration object.

Do the following steps to record the name.

1. Fill in the name you choose in worksheet item **CS1**.
2. Also fill in a description of the object (up to 50 characters) in item **CS2**.

   Related reference

   "i5/OS connection security configuration object work sheet" on page 33
   Use this work sheet to record the parameters for the network security configuration object.

Advanced planning topics

Consider the following items when planning for an iSCSI network.

Expanding on the iSCSI network addressing scheme for integrated servers

Consider these things if you are planning for an iSCSI network that might support multiple switches or more than 19 iSCSI HBA ports.

- If you use a second switch and do not connect it directly to a switch in the 192.168.99 network, you can repeat the IP addressing convention shown in the tables in "Selecting IP addresses for the System x or blade iSCSI initiator" on page 15 and "Expanding on the iSCSI network addressing scheme for integrated servers." Use IP addresses that start with 192.168.98 instead of 192.168.99. This is a separate IP subnet.
- With a subnet mask of 255.255.255.0 there are 254 IP addresses available. IP addresses with a last digit of 0 or 255 should not be used with this subnet mask.
- If you anticipate eventually having an iSCSI network with more than 19 System i iSCSI HBAs or more than 19 hosted systems, you may modify the IP address convention in the tables to maximize the use of all 254 available IP addresses.
- If you anticipate eventually needing more than 254 IP addresses, consider using a different subnet mask to begin with, to avoid the need to change this later.
  – For 510 IP addresses, use a subnet mask of 255.255.254.0
  – For 1022 IP addresses, use a subnet mask of 255.255.252.0
  – For 65534 IP addresses, use a subnet mask of 255.255.0.0

- For the above subnet masks, you must use IP addresses that start with a number less than 192.

- In IP networking, different subnets may be interconnected using routers. IBM does not currently support routers in the iSCSI network. However, if you want to design your iSCSI network to maximize hot spare potential involving the future possibility of routers in the iSCSI network, you should modify the IP address convention in the tables slightly. Routers typically do not forward packets sent to IP addresses that are reserved for private networks. This includes all IP addresses that start with the following digits:
  - 10
  - 172.16 through 172.31
  - 192.168

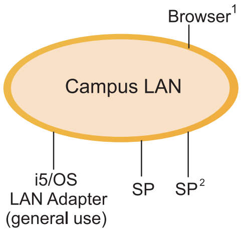
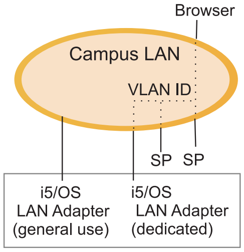
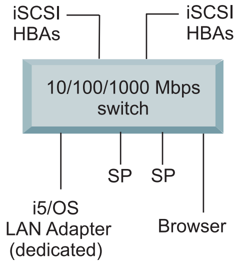
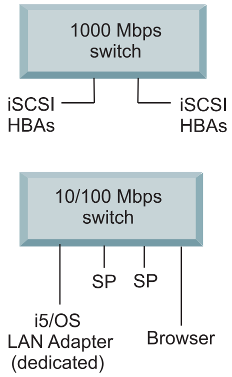
  Therefore, consider using IP addresses that start with different digits, such as 192.169.

Considerations for connecting service processors to i5/OS

Use this information to compare configurations between i5/OS and the service processor for the integrated server.

You might want to consider using an isolated network, instead of your company's campus LAN or intranet, for connecting your BladeCenter and System x service processors with your i5/OS logical partition. This decision involves considerations of hardware, remote management, security, and multiple management server (Service Processor Manager or IBM Director Server). The following table summarizes different connection methods. Different service processors are shown to illustrate scalability.

Table 3. Connection methods

	Campus LAN or Intranet		**Physically isolated network**	
Network Hardware Configuration	Any-to-any network  Browser[1] Campus LAN i5/OS LAN Adapter (general use) SP SP[2]	Logically isolated network For example, this network might include VLAN switches configured with a unique VLAN ID.  Browser Campus LAN VLAN ID SP SP i5/OS LAN Adapter (general use) i5/OS LAN Adapter (dedicated)	One switch for both iSCSI HBAs and service processor connections  iSCSI HBAs iSCSI HBAs 10/100/1000 Mbps switch SP SP i5/OS LAN Adapter (dedicated) Browser	Separate switches for iSCSI HBAs and service processors  1000 Mbps switch iSCSI HBAs iSCSI HBAs 10/100 Mbps switch SP SP i5/OS LAN Adapter (dedicated) Browser
Flexibility of remote management by using a Web Browser[3]	Better ◄ ► Worse			
	Browser can be anywhere on the campus LAN.	Browser must be connected to the logically isolated LAN.	Browser must be connected to the switch providing the service processor connection.	Browser must be connected to the switch providing the service processor connection.
Security[4]	Worse ◄ ► Better			
	Highest risk.	Lower risk than any-to-any network.	Low risk. Requires access to the switch providing the service processor connection.	Low risk. Requires access to the switch providing the service processor connection.
Multiple Management Server Coexistence[5] (Shared SP Login ID)	Worse ◄ ► Better			
	Any management server connected to the campus LAN might interfere.	Only management servers connected to the logically isolated LAN might interfere.	Only management servers connected to the switch providing the service processor connection might interfere.	Only management servers connected to the switch providing the service processor connection might interfere.

Note:

1. *Browser* is a Web browser used for remote management.
2. *SP* is a System x RSA II or BladeCenter Management Module service processor.

3. The web browser management interface is supported by the BladeCenter Management Module and System x RSA II. It is not available for a System x model that only has a BMC service processor.
4. For example, consider the possibility of a LAN sniffer attack seeking a service processor password.
5. If your company has multiple management servers (Service Processor Managers or IBM Director Servers), pay attention to the following situations:
   - If you change the default login ID of the service processor as mentioned in "Selecting a Login ID and Password for the Service Processor" on page 8, then no other management servers interfere and this item does not apply to you.
   - If you do not change the default login ID of the service processor as mentioned in "Selecting a Login ID and Password for the Service Processor" on page 8, this item shows which management servers might interfere with the ability of i5/OS to access a service processor (especially a Management Module).
6. The Multiple Management Server Coexistence[5] (Shared SP Login ID) row applies to you only if you do not change the default service processor login ID.

iSCSI network planning work sheets

Use these work sheets to record the parameters you will use to install the integrated server.

i5/OS service processor configuration object work sheet

Use this work sheet to record the values for the i5/OS service processor configuration object.

This information is used to configure how the i5/OS operating system communicates with the BladeCenter or System x service processor. They are not used for the System i service processor.

Table 4. i5/OS service processor configuration object values

Item	Item Description	Value	
	General:		
SP1	Name[1,2,3]		□ New □ Existing
SP2	Description[4]		
	Service processor connection[5]		
SP3	□ Hostname	Refer to item **XSP2** value	
SP4	□ Internet address	Refer to item **XSP4** value	
	Enclosure identity:[6,7]		
SP5	Serial number [6,7]		
SP6	Manufacturer type and model [6,7]		

Notes:

1. For example, use the naming convention: SP*sssssss* where *sssssss* is the last 7 characters of the BladeCenter chassis (not blade) or System x serial number.
2. For an existing service processor configuration, do not fill out the remaining values in this worksheet.
3. On the CRTNWSCFG command, this is called “Network server configuration”.
4. On the CRTNWSCFG command, this is called “Text ’description’”.
5. On the CRTNWSCFG command, specify *YES for the enable unicast (ENBUNICAST) parameter.
6. Use the BladeCenter chassis (not blade) or System x serial number and type/model values.
7. Items **SP5** and **SP6** must be blank for a System x model if it only has a BMC service processor (no RSA II).
8. On the CRTNWSCFG command, specify *NONE for the initialize service processor (INZSP) parameter.

Related tasks

“Planning for the service processor connection” on page 5
Do these steps to record the information for the service processor configuration object.

“Identifying a BladeCenter or System x service processor type” on page 5
Do these steps to record the type of service processor that is installed in the integrated server hardware.

“Selecting a service processor discovery method” on page 6
The service processor is a part of a BladeCenter server or a System x product. It has the interface used to power the server on and off. When i5/OS receives information, it saves the information and presents interfaces for interacting with and managing that server.

“Recording the system serial number and type/model” on page 7
Do these steps to record the serial and type/model information for the integrated server hardware.

“Assigning an i5/OS Server Processor Configuration object name” on page 7
You need to assign a name to the i5/OS service processor configuration object that you will create to configure the i5/OS connection to the BladeCenter or System x service processor.

“Selecting a Login ID and Password for the Service Processor” on page 8
When you connect directly to the BladeCenter or System x service processor via a LAN, you must specify a login ID (user name) and password.

BladeCenter or System x service processor work sheet

Use this work sheet to plan the values for the BladeCenter or System x service processor.

Table 5. Parameters for the System x or BladeCenter service processor.

Item	Item Description	Value	
	General:		
XSP1	Service processor type [1]	□ MM (BladeCenter Management Module) □ AMM (Advanced Management Module) □ RSA II with BMC (System x model) □ BMC (System x model without an RSA II)	
XSP2	Host name[2]		
XSP3	DHCP	□ Enabled	□ Disabled
XSP4	IP address	N/A	
XSP5	Subnet mask	N/A	
XSP6	Gateway address	N/A	
	Login for **i5/OS** to connect to the service processor.		
XSP7	Login ID[3,4]		
XSP8	Password		
	Login for **administrators** to use to connect to the service processor (optional):		
XSP9	Login ID[3]		
XSP10	Password		

Notes:

1. Put a check in the box next to the type of service processor being used.
2. For an RSA II, MM or AMM, the hostname is optional if DHCP is disabled. The hostname is not supported for a System x model that has only a BMC service processor (no RSA II).
3. The login ID is called "User name" for a BMC or when using the web browser interface for an RSA II, MM or AMM.
4. Suggested naming convention for this login ID is to use the i5/OS logical partition name or system name.

Related tasks

"Selecting a Login ID and Password for the Service Processor" on page 8
When you connect directly to the BladeCenter or System x service processor via a LAN, you must specify a login ID (user name) and password.

i5/OS remote system configuration object work sheet

Use this work sheet to select the parameters you will use to create the remote system configuration object for the integrated server.

Table 6. i5/OS remote system configuration object parameters

Item	Item Description	Value	
	General:		
RS1	Name[1,2,3]		□ New □ Existing
RS2	Description [4]		
RS3	Service processor configuration	XXXXXX (Refer to item **SP1** value)	
	Remote system identity:[5]		
RS4	Serial number[5]		
RS5	Manufacturer type and model [5]		
	Boot Parameters:		
RS6	Boot parameter delivery method	□ Dynamically delivered to remote system via DHCP[6] □ Manually configured on remote system	
	CHAP Authentication		
RS7	Target CHAP	□ Enabled □ Disabled[11]	
RS8	CHAP name[7]		
RS9	CHAP secret		□ Generate
RS10	Initiator CHAP	□ Enabled □ Disabled[12]	
RS11	CHAP name[7]		
RS12	CHAP secret[8]		□ Generate
	Remote Interfaces:	**Interface (Port) 1**	**Interface (Port) 2**
	Remote SCSI Interface:		
RS13	Adapter address[9]	00 C0 DD __ __ __ OR 00 0D 60 __ __ __ OR __ __ __ __ __ __	00 C0 DD __ __ __ OR 00 0D 60 __ __ __ OR __ __ __ __ __ __
RS14	Internet address		
RS15	Subnet mask		
RS16	Gateway address	(Leave blank)	(Leave blank)
	Remote LAN interface:		
RS17	Adapter address[10]	00 C0 DD __ __ __ OR 00 0D 60 __ __ __ OR __ __ __ __ __ __	00 C0 DD __ __ __ OR 00 0D 60 __ __ __ OR __ __ __ __ __ __
RS18	Internet address		
RS19	Subnet mask		
RS20	Gateway address	(Leave blank)	(Leave blank)

Notes:

1. For example, you can use the naming convention RS*sssssss* where *sssssss* is the last 7 characters of the blade (not chassis) or System x serial number.
2. For an existing remote system configuration, do not fill out the remaining values in this work sheet.
3. On the Create Network Server Configuration (CRTNWSCFG) command, this is called "Network server configuration".
4. On the Create Network Server Configuration (CRTNWSCFG) command, this is called "Text 'description'".
5. This information is only required for blades. Use the blade (not chassis) serial number and type/model values.
6. Uses an integrated DHCP server. It does not require a general purpose DHCP server in your network.
7. You can use the remote system configuration name from work sheet item **RS1** as the CHAP name.
8. The CHAP secrets for target and initiator CHAP must not match.
9. For an iSCSI HBA, get this value from the System x or blade iSCSI label. For an Ethernet Network Interface Card (NIC), get it from the Ethernet NIC label.
10. For an iSCSI HBA, get this value from the System x or blade TOE label. For an Ethernet NIC, get it from the Ethernet NIC label.
11. On the Create Network Server Configuration (CRTNWSCFG) command, specify `*NONE` in the target CHAP name (CHAPAUT) to disable target CHAP.
12. On the Create Network Server Configuration (CRTNWSCFG) command, specify `*NONE` in the initiator CHAP name (INRCHAPAUT) to disable bidirectional CHAP.

Related tasks

"Planning for the remote system configuration" on page 9
The remote system configuration object defines the communications connections for iSCSI and virtual Ethernet traffic for the System x or blade hardware that will be connecting to the i5/OS operating system.

"Recording the blade system serial number and type/model" on page 9
Do these steps if you are installing a blade system.

"Selecting a name for the remote system configuration" on page 10
You need to assign a name to the i5/OS remote system configuration object that you will create to configure the attributes of the iSCSI attached BladeCenter blade or System x model.

"Selecting a boot parameter delivery method" on page 10
An integrated server iSCSI HBA must be configured after it is installed in the System x or blade hardware. Do these steps to select the parameters that you will use.

"Selecting Challenge Handshake Authentication Protocol (CHAP) settings" on page 11
Challenge Handshake Authentication Protocol (CHAP) is used to authenticate the connection between the System x or blade initiator and the System i target.

"Selecting maximum transmission unit (MTU) setting for the iSCSI network" on page 13
The iSCSI network MTU value can be set to 1500 (normal frames) or 9000 (jumbo frames).

"Recording iSCSI initiator (local adapter) MAC addresses" on page 13
Do these steps to record the iSCSI initiator local adapter (MAC) address for your remote system configuration object. Depending on your iSCSI HBA type, do one of the following:

"Selecting IP addresses for the System x or blade iSCSI initiator" on page 15
You need to select an IP address scheme for SCSI and LAN interfaces of the iSCSI initiator before you configure your server. You can use the sample information in this table or use your own scheme.

"Selecting the initiator iSCSI Qualified Name (IQN)" on page 17
If you checked **Manually configured on remote system** (manual addressing) for the **Boot parameter delivery method** in worksheet item RS6, then you need to configure the initiator (System x or blade) iSCSI Name (IQN) value manually.

"Selecting the target iSCSI Qualified Name (IQN)" on page 17
If you checked **Manually configured on remote system** (manual addressing) for the **Boot parameter delivery method** in worksheet item **RS6**, then you need to configure the target (System i) iSCSI Name (IQN) value manually.

iSCSI initiator work sheet

Select the parameters to configure the iSCSI initiator in the System x or blade hardware.

The values that should be filled into this work sheet are indicated by the Dynamic and Manual columns: R=Required, O=Optional and N/A=Not applicable.

Table 7. Parameters for the iSCSI initiator configuration function

		Addressing mode[1]		
Item	**Item Description**	□ **Dynamic**	□ **Manual**	**Value**
	Adapter settings:			
CQ1	LUNs per Target	O	O	**64**
CQ2	Initiator IP address by DHCP	R	R	**NO**[2]
CQ3	Initiator IP address	N/A	R	XX (Refer to item **RS14** values) XX
CQ4	Subnet mask	N/A	R	XX (Refer to item **RS15** values) XX
CQ5	Gateway IP address	N/A	R	Leave this field empty
CQ6	Initiator iSCSI Name[3]	N/A	R	**Port 1:** iqn.1924-02.com.ibm:______.i0
				Port 2 iqn.1924-02.com.ibm:______.i0
CQ7	Initiator Chap Name	O	O	Leave this field empty
CQ8	Initiator Chap Secret	O	O	Leave this field empty
	iSCSI Boot Settings:			
CQ9	Adapter Boot Mode[1]	R	R	**Port 1:**□ DHCP □Manual
				All other ports: Disabled.[4]
CQ10	Target IP	N/A	R	XX (Refer to item **NH5** value) XX

CQ11	Target iSCSI Name[6]	N/A	R	`iqn.1924-02.com`
				`.ibm:______.______.t1`

CQ12	Chap	R	R	□ Enabled □ Disabled
CQ13	Chap Name	O	O	XX (Refer to item **RS8** value) XX
CQ14	Chap Secret	O	O	XX (Refer to item **RS9** value) XX
CQ15	Bidirectional CHAP	O	O	XX (Refer to item **RS10** value) XX
	Advanced Adapter Settings:			
CQ16	MTU	O	O	**Port 1:** □1500 □ 9000
				Port 2: □1500 □9000

Notes:

1. The value for item **RS6** determines the Addressing Mode and the value for item **CQ9**. See "Selecting a boot parameter delivery method" on page 10.
2. The Initiator IP address by DHCP value must always be set to NO.
3. The initiator iSCSI Name (IQN) format is: iqn.1924-02.com.ibm:*sssssss*.i*p* where:
   - *sssssss* is the serial number of the System x (see item SP5) or blade (see item RS4) server in lower case
   - *p* is the System x/blade iSCSI HBA interface/port number (0=first interface/port).

4. Only one port can have the boot mode set to DHCP or Manual during the server installation. For all other ports, the adapter boot mode must be set to **Disabled**. Once the server installation is completed, if the server operating system supports multipath I/O, then additional ports can be enabled for boot.
5. The target iSCSI Name (IQN) format is: iqn.1924-02.com.ibm:*sssssssi.nnnnnnnn.tp* where:
   - *sssssss* is the System i serial number in lower case.
   - *i* is the System i logical partition ID.
   - *nnnnnnnn* is the network server description (NWSD) name in lower case letters.
   - *p* is the storage path number from the NWSD (1=first and only storage path for new installations).

i5/OS network server host adapter object work sheet

Use this work sheet to plan the parameters you will use to create the network server host adapter (NWSH) object.

Table 8. Parameters for the NWSH object

Item	Item Description	Value	
	General:		
NH1	Name[1,2,3]		□ New □ Existing
NH2	Description[4]		
NH3	Hardware resource name	CMN___	
	Local Interfaces:		
NH4	Subnet mask		
	Local SCSI Interface		
NH5	Internet address		
NH6	Gateway address		
	Local LAN Interface		
NH7	Internet address		
NH8	Gateway address		
NH9	Cable connection	□ Network □ Direct	

Notes:

1. For example, a naming convention might be NH*sssssss* where *sssssss* is the last 7 characters of the serial number for the target iSCSI HBA that is installed in the System i product.
2. For an existing NWSH, also fill in item NH5 by looking at the NWSH properties, but do not fill in the remaining values in this worksheet.
3. On the CRTDEVNWSH command, this is called “Device description”.
4. On the CRTDEVNWSH command, this is called “Text ’description’”.

Related tasks

“Planning for the network server host adapter (NWSH) object” on page 17
The network server host adapter (NWSH) device description defines the communications connections for iSCSI and virtual Ethernet traffic to i5/OS.

“Selecting a name for the NWSH” on page 18
You need to assign a name to the i5/OS network server host adapter (NWSH) device description object that you will create to configure the System i iSCSI HBA.

“Selecting a hardware resource name” on page 18
The iSCSI HBA hardware resource name will not be available until the iSCSI HBA is actually installed in the System i platform.

“Selecting IP addresses for the System i iSCSI HBA” on page 19
Use this information to select IP addresses for the target iSCSI HBA installed in the System i product.

i5/OS connection security configuration object work sheet

Use this work sheet to record the parameters for the network security configuration object.

Table 9. Values for the i5/OS connection security configuration object

Item	Item Description	Value	
	General:		
CS1	Name[1,2,3]		□ New □ Existing
CS2	Description[4]		

Notes:

1. Since IP security (IPSec) is not supported, the suggested name is: **NOIPSEC**.
2. For an existing connection security configuration, do not fill out the remaining values in this worksheet.
3. On the Create Network Server Configuration (CRTNWSCFG) command, this is called `Network server configuration`.
4. On the Create Network Server Configuration (CRTNWSCFG), this is called `Text 'description'`.

Related tasks

"Planning for the i5/OS connection security configuration object" on page 19
A connection security configuration object is required for iSCSI-attached integrated servers. All of the iSCSI-attached integrated servers on your system can share the same connection security configuration object.

"Assigning a connection security configuration object name" on page 20
Select a name for the i5/OS connection security configuration object.

Appendix. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation

Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, IBM License Agreement for Machine Code, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

BladeCenter
i5/OS
IBM
System i
System x

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Terms and conditions

Permissions for the use of these publications is granted subject to the following terms and conditions.

Personal Use: You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative works of these publications, or any portion thereof, without the express consent of IBM.

Commercial Use: You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED ″AS-IS″ AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Printed in USA