IBM TS7650G 3958 DD6 ProtecTIER Deduplication Gateway

Version 3 Release 4

Installation Roadmap Guide

SC27-8901-01

Note:
Before you use this information and the product it supports, read the information in the *Safety and Environmental Notices* publication, SC27-4622 and "Notices" sections of this publication.

Edition notice

This edition applies to ProtecTIER® version 3.4.3.1 for the TS7650G 3958 DD6 and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Figures

Tables

Homologation statement

Attention: This product may not be certified in your country for connection by any means whatsoever to interfaces of public telecommunications networks. Further certification may be required by law prior to making any such connection. Contact an IBM representative or reseller if you have any questions.

About the installation roadmap

The installation procedures that are described in this document are for IBM® service personnel only. They include instructions for installing, cabling, and configuring the TS7650G servers and any hardware components that are included in the purchase of the TS7650G:

- Installing the hardware components in the customer-supplied frames at the customer site.
- Connecting the cables from the TS7650G components to the customer Ethernet network and host system.
- Configuring ProtecTIER RAS on the 3958 DD6 Gateway servers.
- Verifying RAS configuration and testing Call Home.
- Configuring ProtecTIER for use with the TS7650G.
- Installing the ProtecTIER Replication Manager.
- Using ProtecTIER Manager.
- Changing the system date and time.
- Validating system function (clustered configuration only).

What is not covered in this document

- Physical installation of the disk controllers or disk expansion modules. Disk components must be installed before the installation of the TS7650G.
- Configuration and setup of any hardware components that were not included in the purchase of the TS7650G. Components such as the disk controller and disk expansion modules must be configured and operational before the installation of the TS7650G.
- Creation and configuration of replication grids.
- Daily use and ongoing maintenance of the ProtecTIER, ProtecTIER Manager, and ProtecTIER Replication Manager, software.
- Hardware or software troubleshooting.
- References to the enablement of ProtecTIER Replication Manager, such as procedures and worksheets, were removed. The customer is now directed instead to the *IBM ProtecTIER User's Guide for VTL Systems*, GA32-0922.

Terminology

destination, target
This document uses the terms destination and target interchangeably.

shelf A container of VTL cartridges within a ProtecTIER repository.

TS7650G or Gateway
These are terms for IBM's virtualization solution from the TS7650 family that does not include a disk storage repository, allowing the customer to choose from a variety of storage options. The TS7650G consists of the following:

Server There are five types of server that have been used in the Gateway. The following are the currently supported servers:

3958 DD6
This is a high performance server available since March 2016. The enclosure, or chassis, has space for two controller

nodes in the rear, which accommodates a two-node cluster configuration in a 2u platform and eliminates the external cluster connection kit. In the front, the 3958 DD6 contains 24 SAS drive slots (only 2 of which actually contain SAS drives). The remaining 22 slots are unused by ProtecTIER, do not have any function, and are filled with dummy carriers. The 3958 DD6 also includes redundant power supplies in the rear of the unit.

3958 DD5
This server, which first shipped in May 2012, is based on the IBM System x7143 model. When used as a server in the TS7650G, its machine type and model are 3958 DD5. Use this machine type and model for service purposes.

3958 DD4
This server became available in December 2010 and is based on the IBM System x3850 X5 Type 7145-PBR. When used as a server in the TS7650G, its machine type and model are 3958 DD4. Use this machine type and model for service purposes.

System console
The system console is a TS3000 System Console (TSSC). This document uses the terms *system console* and *TSSC* interchangeably. The TSSC is not available (and does not work) with the 3958 DD6.

Under IBM best practices, the TS7650G also contains the following:

Disk controller
The customer must choose the disk controller for use with the TS7650G. A list of TS7650 compatible controllers can be generated at the IBM System Storage Interoperation Center.

Disk expansion unit
The customer must choose the disk expansion unit for use with the TS7650G. A list of TS7650 compatible expansion units can be generated at the IBM System Storage Interoperation Center.

IBM Tivoli Assist On-site (AOS)
IBM Tivoli Assist On-site (AOS) is a web-based tool that enables a remote support representative in IBM to view or control the management node desktop. More information is located at the Tivoli AOS website.

virtual tape library (VTL)
The ProtecTIER virtual tape library (VTL) service emulates traditional tape libraries. By emulating tape libraries, ProtecTIER VTL allows you to switch to disk backup without replacing your entire backup environment. Your existing backup application can access virtual robots to move virtual cartridges between virtual slots and drives. The backup application perceives that the data is being stored on cartridges while ProtecTIER actually stores data on a deduplicated disk repository.

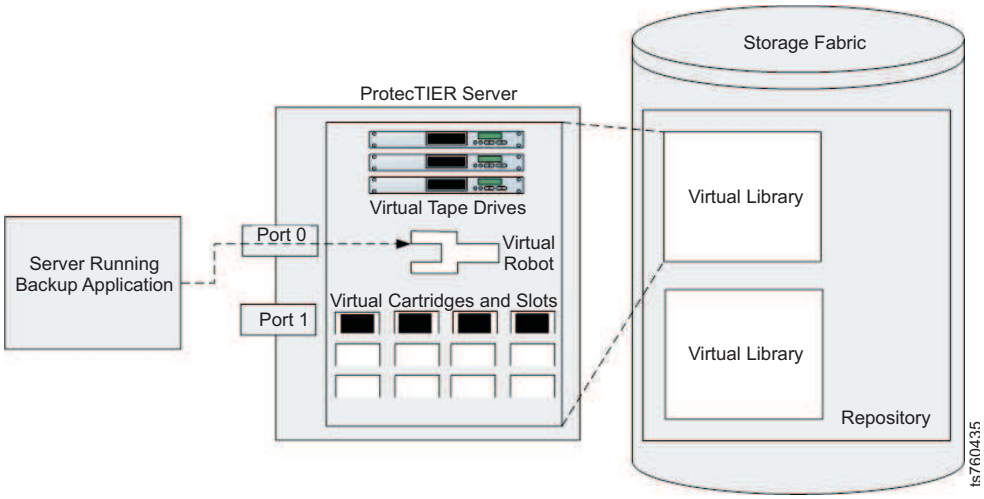


Figure 1. Virtual tape library (VTL) emulation

visibility switching
The automated process that transfers the visibility of a VTL cartridge from its master to its replica and vice versa. The visibility switching process is triggered by moving a cartridge to the source library Import/Export (I/E) slot. The cartridge will then disappear from the I/E slot and appear at the destination library's I/E slot. To move the cartridge back to the source library, the cartridge must be ejected to the shelf from the destination library. The cartridge will then disappear from the destination library and reappear at the source I/E slot.

server, node
This document uses the terms server and node interchangeably.

Information, help, and service

Online help

IBM maintains pages on the World Wide Web where you can get information about IBM products and services and find the latest technical information.

Table 1. IBM websites for help, services, and information

Description	World Wide Web address (URL)
IBM home page	http://www.ibm.com
Directory of worldwide contacts	http://www.ibm.com/planetwide
Support for IBM System Storage® and TotalStorage products	http://www.support.ibm.com The **IBM Support Portal** page displays. Do the following: 1. In the **Product Lookup** field, begin typing TS76. As you type, a list of matching products drops down below the input field. 2. Select your product from the drop down list. The product you select appears below the Search field in the **Search supports and downloads** section. Items specific to the product you selected appear in the five areas below the Search field. You can search for specific information, or select one of the links in the **Downloads, Product support content, Tools and resources, Featured links,** or **Common support links**. 3. To view a list of available fixes for your product, for example, click on → Downloads (drivers, firmware, PTFs). Alternatively, you can use the **Browse for a product** link. 1. Click **Browse for a product**. 2. Expand ► System Storage. 3. Expand ► Tape systems. 4. Expand ► Tape virtualization. The page shows a list of products. 5. Select your product from the list. The product you select appears below the Search field in the **Search supports and downloads** section.

Other useful websites

The most up-to-date information about this product, including documentation and the most recent downloads, can be found at the following websites:

- Information centers for the product:
  - IBM ProtecTIER TS7650 Customer Knowledge Center
  - IBM ProtecTIER TS7610 and TS7650 Combined Service Knowledge Center
- You can order publications through the IBM Publications Center: http://www-05.ibm.com/e-business/linkweb/publications/servlet/pbi.wss

- Access installation and technical support information at: http://www.ibm.com/support
- For DS8000® series information, go to:http://www-03.ibm.com/systems/storage/disk/ds8000/
- For XIV® information, go to: http://www.ibm.com/support/knowledgecenter/STJTAG/com.ibm.help.xivgen3.doc/xiv_kcwelcomepage.html
- The IBM website for independent software vendor (ISV) support is: https://www.ibm.com/isv/
- The IBM System Storage TS7600 with ProtecTIER Interoperability Matrix website can be found at: http://www-03.ibm.com/systems/support/storage/config/ssic/displayesssearchwithoutjs.wss?start_over=yes
- For the latest information about IBM xSeries products, services, and support, go to: http://www-03.ibm.com/servers/eserver/xseries/
- For product firmware and software downloads and associated driver code, go to: http://www-947.ibm.com/systems/support/storage/
- For accessibility information, go to: http://www-03.ibm.com/able/product_accessibility/index.html
- For the latest information about product recycling programs, go to: http://www.ibm.com/ibm/environment/

Telephone help

With the original purchase of the IBM TS7650G ProtecTIER Deduplication Gateway, customers have access to extensive support coverage. During the product warranty period, customers can call the IBM Support Center (1 800 426-7378 in the US). Product assistance is available under the terms of the hardware IBM warranty or the software maintenance contract that comes with product purchase. In the US and Canada, these services are available 24 hours a day, 7 days a week. In the UK, these services are available Monday through Friday, from 9:00 a.m. to 6:00 p.m.

Note: This product is equipped with a Software Call Home feature. When enabled, it notifies IBM Service of software error events. Not all countries currently support this feature.

Related IBM publications

ProtecTIER publications

IBM TS7650G ProtecTIER Deduplication Gateway Introduction and Planning Guide, GA32-0918

IBM TS7650G ProtecTIER Deduplication Gateway Installation Roadmap Guide, GA32-0921

IBM TS7650GProtecTIER User's Guide for VTL Systems, GA32-0922

IBM TS7650GProtecTIER User's Guide for FSI Systems, GA32-2235

IBM TS7650G ProtecTIER Deduplication Gateway Problem Determination and Service Guide, GA32-0923

IBM TS7650 ProtecTIER Software Upgrade Guide, SC27-3643

DS8000 publications

The following publications provide more documentation about the IBM System Storage DS8000 storage subsystem.

- *IBM DS8000 Storage System Introduction and Planning Guide for Customer Configuration*
- *IBM DS8000 Storage System User Manual*

XIV publications

The following publications provide more documentation about the IBM XIV Storage System:

- *IBM XIV Storage System (Types 2810 and 2812) Model A14 (Gen2) Introduction and Planning Guide for Customer Configuration*
- *IBM XIV Storage System User Manual*
- *IBM XIV Storage System Pre-Installation and Network Planning Guide for Customer Configuration*
- *IBM XIV Storage System Theory of Operation*

How to send your comments

Your feedback is important in helping to provide the most accurate and highest quality information.

To submit any comments about this book or any other IBM System Storage TS7600 with ProtecTIER documentation:

- Send your comments by e-mail to starpubs@us.ibm.com. Be sure to include the following information:
  - Exact publication title and version
  - Publication form number (for example, GC53-1196-03)

– Page, table, or illustration numbers that you are commenting on with a detailed description of any information that should be changed

Chapter 1. Overview

The IBM TS7650G ProtecTIER Deduplication Gateway is available in multiple configurations:

- Stand-alone, or single node (VTL and FSI) on 3958-DD6
- Stand-alone VTL on 3958-DD6
- Clustered VTL on 3958-DD6
- Stand-alone VTL on 3958-DD4 and 3958-DD5
- Clustered VTL on 3958-DD4 and 3958-DD5

The purchase of the stand-alone, or single node, TS7650G 3958 DD6 includes the following hardware and software:

- One hardware enclosure with rack mounting hardware
- 2 power cool modules
- 1 SAS logging drive
- 1 node controller which includes:
  - 2 CPUs (2695v2)
  - 1 SSD (128 GB)
  - 1 Emulex 00WT000 8 Gbps Gen 5 Fibre Channel PCIe 3.0 Quad-Port Host Bus Adapter (HBA)
  - 1 built-in 1 Gbps Ethernet port
  - 2 built-in 10 Gbps Ethernet ports
  - For VTL configuration, 1 Emulex LPe 15004 8 Gbps low profile Gen 5 Fibre Channel PCIe 3.0 Quad-Port HBA
  - For FSI configuration, either 1 Intel Quad-Port 1 Gbps Ethernet card, or 1 Intel Dual-Port 10 Gbps Ethernet card
  - 1 blanking plate, which is required to fill the second controller slot vacancy; the single node 3958 DD6 cannot operate without it
  - 2 power cords to connect the PDUs in the rack
  - 1 licensed, preinstalled copy of Red Hat Enterprise Linux version 5.11 Advanced Platform
  - 1 licensed, preinstalled copy of IBM ProtecTIER V3.4.0

The purchase of the clustered gateway for the 3958 DD6 includes the following hardware and software:

- One gateway server (IBM machine type and model 3958 DD6) with two internal controllers
  - The lower internal control unit is ProtecTIER Server Node A
  - The upper internal control unit is ProtecTIER Server Node B
- One UTP Cat 6 cable
- Two licensed, preinstalled copies of Red Hat Linux version 5.11 Advanced Platform
- Two licensed, preinstalled copies of IBM ProtecTIER

The following cluster server combinations are supported:

- One 3958 DD6 enclosure with two internal controllers (either VTL or FSI)

- One 3958 DD6 enclosure with two internal controllers with one node VTL and one node FSI

For either configuration of the TS7650G to be fully functional, more hardware components are required. These components are purchased separately. They must be installed and configured at the customer site before TS7650G installation begins. Hardware components that are suitable for use include:

Stand-alone gateway

- One SAN to Storage Fiber Channel HBA disk controller
- Enclosure with one controller
- Two or more 25-m LC/LC Fibre Channel cables (Feature Code AGK2)

Clustered Gateway

- Two SAN to Storage Fiber Channel HBA disk controllers
- Enclosure with two controllers, or canisters
- The second canister requires an AGK6 feature (1U controller with 10 Gb/s ethernet)
- Two or more 25M LC/LC Fibre Channel cables (Feature Code AGK2)
- One 36u frame

Note: The hardware that the customer purchases might differ from the listed components.

TS7650G ship group

Hardware ship group

The hardware ship group includes the *IBM TS7650 with ProtecTIER Publications* CD, which contains the following service and customer documentation for the IBM TS7650G ProtecTIER Deduplication Gateway:

- *IBM TS7650G ProtecTIER Deduplication Gateway Installation Roadmap Guide*, GA32-0921
- *IBM TS7650G ProtecTIER Deduplication Gateway Introduction and Planning Guide*, GA32-0918
- *IBM ProtecTIER User's Guide for VTL Systems*, GA32-0922
- *IBM Problem Determination and Service Guide for the TS7650G ProtecTIER Deduplication Gateway*, GA32-0923
- *IBM Labeling Instructions for the TS7650 ProtecTIER Deduplication Appliance and TS7650G ProtecTIER Deduplication Gateway*, PN 95P8942
- *Statement of Limited Warranty*

Software ship group

The software ship group includes the following items:

IBM ProtecTIER Enterprise Edition **DVD**
: This DVD contains the software for the gateway server that runs on the Red Hat Linux operating system that is installed on the server. The server uses the software to present the attached disk storage to host systems as "virtual tape" and for other functions such as data deduplication.

IBM ProtecTIER Manager **DVD**
: This DVD contains the files that are required to install the ProtecTIER

Manager graphical user interface on customer workstations. Typically, the workstations are connected to the TS7650G through the customer Ethernet network. ProtecTIER Manager is used to manage the virtual tape that is presented to host systems by the server.

IBM ProtecTIER Maintenance and Recovery Disk
This disk contains the Red Hat Enterprise Linux V5.11 Advanced Platform operating system software, with the ProtecTIER kickstart configuration file (`ks.cfg`). If system recovery becomes necessary, use this DVD to reinstall Red Hat Linux on the affected TS7650G servers.

Important installation information

Important:

- During the initial setup of the 3958 DD6, do not change the default IP address of the BMC. Changing this IP address causes you to loose connectivity during the installation.
- The installation requires the customer to provide a frame, and have it available and ready for use at the customer site. TS7650G sales agreements might include a frame and disk storage as part of the order. However, installation of frames and disk storage are not included in the gateway installation process, and requires more planning and coordination.
- A USB keyboard and graphics-capable monitor are required to complete the installation. These must be provided by the customer. The optimum screen resolution for the ProtecTIER GUI is 1280 x 1024.
- Complete the installation of the TS7650G before you install any miscellaneous equipment specification (MES) features. The installation instructions for an MES feature assume that you are adding the feature to an installed TS7650G.
- For any upgrade scenario involving new hardware ordered from IBM, the ProtecTIER code must be upgraded to version 3.4.3 **before** completing the procedures in this document. For information about how to upgrade from ProtecTIER version 2.4, 2.5, 3.1, or 3.3 to ProtecTIER version 3.4.3, see the *IBM TS7650 ProtecTIER Software Upgrade Guide*, SC27-3643, and complete the ProtecTIER software upgrade before continuing.

Taking inventory and organizing components

Before you begin installation, use the remote customer system inventory (RCSI) application and the barcode scanner to inventory the components to ensure that the shipment is complete. Next, consult the Worldwide Customized Installation Instructions (WCII) for any updated instructions and use them to plan your installation steps.

Unpacking and taking inventory of components

About this task

After you unpack the boxes, use the Remote Customer System Inventory (RCSI) application to automate the inventory process tasks before installing a system or MES.

Procedure

1. Follow the unpacking instructions that are on a sheet inside the top of the shipping box.

2. Download the inventory checklist for the customer's order from the RCSI application website at http://w3.rchland.ibm.com/~cuii/CustomizableContent/rcsi.htm.
3. Use the barcode reader to scan all the components of the shipment and compare them to the inventory checklist. The manufacturing order number (MFGNO) for the barcode scanner is 1AM8BG7. The plant number (PLORN) for the barcode scanner is LF2555. The RCSI application might need you to enter the PLORN.

Figure 2. Barcode reader

Note: You can find more information on using the barcode scanner and the RCSI application at the RCSI application website at http://w3.rchland.ibm.com/~cuii/CustomizableContent/rcsi.htm.

Organizing installation flow

About this task

Preparing components for installation and consulting the WWCI can help streamline the installation process.

Procedure

1. Prepare components for installation when necessary.
2. Scan the WWCI at http://w3.rchland.ibm.com/projects/WCII/cgi-bin/wciireq.pl for any updates to installation instructions and use the information to plan the installation steps.

Disk storage configuration guidelines

Gateway servers can attach to various disk storage technologies, which might have different installation and support terms that depend upon machine type. Warranty service upgrades (WSUs) or an installation service contract might be required for storage devices considered customer setup (CSU), or not considered IBM setup. See the *IBM ProtecTIER Implementation and Best Practices*, Redbooks publication SG24-8025, available at: http://www.redbooks.ibm.com/Redbooks.nsf/RedpieceAbstracts/sg248025.html?Open for more detailed information about how to set up IBM storage systems.

If the disk storage is not operational when you arrive at the customer site, take the following steps:

1. Assess the situation to determine whether you can do the task yourself, or if more IBM resources are required:
   - You can install the physical disk storage if the machine types are properly entitled.
   - If more installation resources are required, contact the next level of support for advice on how to proceed.

   Note: Advanced setup tasks, including LUN configuration and mirroring, are outside the scope of normal installation support and might warrant more charges.
2. If IBM disk storage was purchased without IBM installation services, a Service Contract (SC44) is required for disk storage and frame installation. There is an extra charge with an SC44.

Responsibilities matrix

The hardware and software upgrade, configuration, and replication configuration processes require participation from the customer and the coordinated efforts of several personnel, such as a Support Service Representative (SSR).Table 2 shows the responsibilities for each type of contributor.

Table 2. Responsibilities matrix

Task	Customer	Trained ProtecTIER Specialist or LBS (or both)	SSRs
Complete the planning, preparation, and installation tasks that are described in the *IBM TS7650G ProtecTIER Deduplication Gateway Introduction and Planning Guide*, GA32-0918.	▪		
Meet the preinstallation requirements that are outlined in the *IBM TS7650G ProtecTIER Deduplication Gateway Introduction and Planning Guide*, GA32-0918	▪		
Complete the worksheets that are provided in the *IBM TS7650G ProtecTIER Deduplication Gateway Introduction and Planning Guide*, GA32-0918.	▪		
Purchase, install, and configure (if necessary), all hardware components not included in the purchase of the gateway. See the *IBM ProtecTIER Implementation and Best Practices*, Redbooks publication SG24-8025, available at: http://www.redbooks.ibm.com/Redbooks.nsf/RedpieceAbstracts/sg248025.html?Open.	▪		

Table 2. Responsibilities matrix (continued)

Task	Customer	Trained ProtecTIER Specialist or LBS (or both)	SSRs
Ensure that a separate USB keyboard and graphics-capable monitor are available for use during installation.	▪		
Oversee project management for the installation and integration of the engagement.		▪	
Oversee change management and process control for the installation.		▪	
Coordinate and schedule IBM resources for customer installations, and act as a point of contact for coordination of installation services.		▪	
Schedule and facilitate planning and solution assurance conference calls.		▪	
Create and document the installation service process.		▪	
Install the TS7650G hardware components that were purchased with the gateway into the server and disk storage frames.			▪
Label and connect power, Ethernet, and Fibre Channel cables, as necessary and applicable.			▪
Connect the TS7650G to the customer local area network and replication network, if applicable.			▪
Power on the system.			▪
Verify accuracy of hardware installation and cabling. Perform visual check of fault indicator LEDs.			▪
Configure the RAS package on the servers.			▪
Test Call Home on the servers.			▪
Configure ProtecTIER on the stand-alone server or Server A (the bottom server in a clustered DD6) and create the file systems.		▪	
Install ProtecTIER Replication Manager on one of the ProtecTIER servers that are being used for replication, if applicable.		▪	
Install ProtecTIER Manager on the ProtecTIER Manager workstation, register each server as a new ProtecTIER node, and create the repository.		▪	
Verify cluster operation, if applicable.		▪	
Perform RAS verification tasks.		▪	
Update the ProtecTIER software on the newly installed servers, if applicable.		▪	
Release the system to the customer. Advise the customer that it is their responsibility to create and configure the replication grid, if applicable.		▪	
Document and report installation results.		▪	

Chapter 2. Configurations that use IBM hardware

Components for use with the TS7650G are purchased separately by the customer and might not be from IBM.

- Unlike previous TS7650G models, the 3958 DD6 does not support a TSSC. RAS service capabilities, supplied through the TSSC on previous servers is performed using the Electronic Customer Care (ECC) feature embedded in ProtecTIER software V3.4 for 3958-DD6 servers.

Important:

- This document references IBM 4.8 TB Fibre Channel Disk Controllers and IBM 7.2 TB Fibre Channel Disk Expansion Units in many of the hardware installation figures, examples, and procedures.

  The IBM TS7650G supports the DS5000 disk controller, the DS8000 disk controller, Storwize V7000 Storage Controller and the XIV disk controller, as well as various non-IBM storage solutions. If the customer has elected to use disk storage components other than the IBM disk controllers and expansion units mentioned above, the figures, examples, and procedures in this document will not apply to the configuration on which you are working. Therefore, it is suggested that you determine the make and model of the disk storage components in use and, if necessary, obtain the related product documentation before you begin installation of the gateway.
- For TS7650G servers, the RAS function does not send Call Home packages for problems with any of the disk storage products attached to the server.
- The actual frames that are used for your installation might be different from the frames (3952 F05 Frame) used in the examples.

About the 3958 DD6 server

The 3958 DD6 server is shipped with Red Hat Linux version 5.11 and the ProtecTIER V3.4.3 software preinstalled.

Server rear view (VTL)

When configured for VTL, the 3958 DD6 servers are equipped with the following components:

- One full height PCIe 2.0
- One low profile PCIe 2.0
- One 1 gigabit (Gb) Ethernet port
- Two Ethernet 1 Gb or 10 Gb ports
- Two 12 Gb mini SAS-HD ports
- Two USB 2.0 ports (rear)
- Onboard 12 Gb SAS (non-RAID)

See Figure 3 on page 8 and Table 3 on page 8.

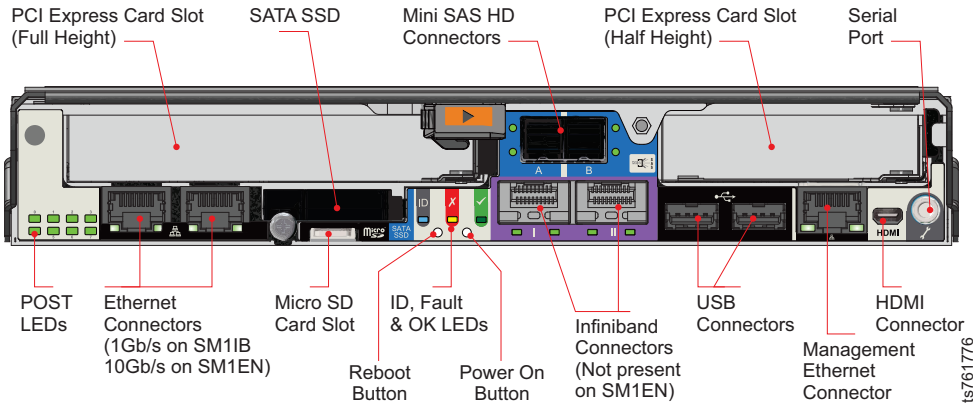


Figure 3. 3958 DD6 server rear view with VTL configuration

Table 3. 3958 DD6 server rear view: Slot assignments, ports, and connections for VTL

VTL use	**Explanation**
PCI Express card slot (full height)	Host Bus Adaptor (HBA) for front end communications - VTL requires Emulex 00WT000 HBA
SATA SSD	There are 2 serial ATA solid state drives (SSDs) (one internal, one accessible from the rear panel)
Mini SAS HD connector	SAS controller and associated device driver to allow applications running on the server to communicate with the drives in the enclosure and the SAS expander.
PCI Express card slot (half height)	1 8Gbps Emulex LPe 15004 Quad port for back-end disk attach
Serial port	
HDMI connector	The type D Micro HDMI connector (along with a VGA to Micro HDMI Converter supplied by the customer) can be used to attach a monitor, which will display the output from the x86 host system. Plugging a keyboard and mouse into the USB ports then gives access to the controller as per a standard PC.
Management Ethernet connector	Through the management Ethernet port you can gain access to log into the x86 subsystem. This also serves as the port for connection to the BMC.
USB connectors	You can plug a keyboard and mouse into the USB ports to use with a monitor you connect to the HDMI port. The Right USB connector is also used for USB code upgrade and configuration.
Infiniband Connectors	Not currently supported.
Power on button	
ID, fault, and OK LEDs	• The ID LED is blue when the module is being identified • The Fault LED is amber when there is a fault in the controller • The OK LED is green when the controller is operating correctly, and flashing green when there is a controller VPD error
Reboot button	
Micro SD card slot	The use of the Micro SD card slot is not currently supported.
Ethernet Connectors	Two Ethernet ports on the left side of the rear panel can be attached to a replication network, or a cluster network on a dual node DD6.

Table 3. 3958 DD6 server rear view: Slot assignments, ports, and connections for VTL (continued)

VTL use	Explanation
POST LEDs	Power On Self Test LEDs are used to show the boot progress of the x86 subsystem. If it fails to boot, the LEDs will show what stage of the process was being performed when the problem occurred.

Server front view

The server front view shows the 24 slots for serial-attached SCSI (SAS) drives. The enclosure front panel incorporates an Operator's (Ops) Panel housed on the left hand mounting flange and connected to the Midplane via a flexible cable.

Figure 4. 3958 DD6 server front view

Operators (Ops) panel

The operator panel (sometimes abbreviated as "ops panel") provides basic status for the enclosure

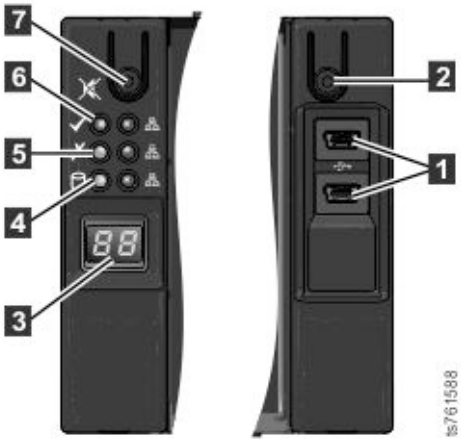


Figure 5. 3958 DD6Ops panels

Table 4. 3958 DD6

Item	Description
1	USB sockets
2	Power button
3	Unit display
4	Logical Fault LED
5	Module Fault LED

Table 4. 3958 DD6 (continued)

Item	Description
6	System Power LED
7	Input/Mute Switch

Single node configuration for the 3958 DD6

For a list of what the single node 3958 DD6 includes, see Chapter 1, "Overview," on page 1.

Unlike the 3958 DD5, the 3958 DD6 does not require an IBM TSSC and the accompanying KVM kit for installation, service, and maintenance of the TS7650G. RAS service capabilities are performed by Electronic Customer Care (ECC), an integrated service tool that provides automation of error reporting through the Call Home feature embedded in ProtecTIER software V3.4 for 3958-DD6 servers.

For the TS7650G to be fully functional, other hardware components (purchased separately) are required. These components include frames, disk controllers, and disk expansion modules.

See Figure 6 on page 11 for an example of the server frame layout.

EIA Holes	EIA Unit		EIA Unit	EIA Holes
106	36	Empty (1u)	36	106
103	35	Empty (1u)	35	103
100	34	Empty (1u)	34	100
97	33	Empty (1u)	33	97
94	32	Empty (1u)	32	94
91	31	Empty (1u)	31	91
88	30	Empty (1u)	30	88
85	29	Empty (1u)	29	85
82	28	Empty (1u)	28	82
79	27	Empty (1u)	27	79
76	26	Empty (1u)	26	76
73	25	Empty (1u)	25	73
70	24	Empty (1u)	24	70
67	23	Empty (1u)	23	67
64	22	Empty (1u)	22	64
61	21	Empty (1u)	21	61
58	20	Empty (1u)	20	58
55	19	Empty (1u)	19	55
52	18	Empty (1u)	18	52
49	17	Empty (1u)	17	49
46	16	Empty (1u)	16	46
43	15	Empty (1u)	15	43
40	14	Empty (1u)	14	40
37	13	Empty (1u)	13	37
34	12	Empty (1u)	12	34
31	11	Empty (1u)	11	31
28	10	Empty (1u)	10	28
25	9	Empty (1u)	9	25
22	8	Empty (1u)	8	22
19	7	Empty (1u)	7	19
16	6	ProtecTIER Server (2u)	6	16
13	5		5	13
10	4	Empty (1u)	4	10
7	3	Power Distribution Unit (1u)	3	7
4	2	Power Distribution Unit (1u)	2	4
1	1	Empty (1u)	1	1

ts761743

Figure 6. Stand-alone gateway server frame layout

Clustered configuration for the 3958 DD6

The clustered configuration for the 3958 DD6 includes two controllers in the same 2U enclosure.

One configuration for a clustered TS7650G server with IBM hardware includes the following components:

- Two SAN to Storage Fiber Channel HBA disk controllers

- Enclosure with two controllers, or canisters
- The second canister requires an AGK6 feature (1U controller with 10 Gb/s ethernet)
- Two or more 25M LC/LC Fibre Channel cables (Feature Code AGK2)
- One 36u frame

Chapter 3. Installing the TS7650G 3958 DD6 hardware

Use the checklist in the next section to keep track of your progress during the installation process.

Attention: Follow the unpacking instructions that are at the top just inside the box.

Installation workflow checklist for the 3958 DD6

Table 5. Installation workflow checklist

✓	Task	Description	Where to find information
Section 1: Perform pre-installation verification			
☐	1–1	The disk components are installed in suitable frames. Responsibility of the client or ProtecTIER Specialist.	If this task was not completed before your arrival, see “Important installation information” on page 3 and “Disk storage configuration guidelines” on page 5.
☐	1–2	The frames are in a suitable location.	N/A
☐	1–3	The disk controllers are located within 25 m (82 ft.) cable length of the servers.	N/A
☐	1–4	All RAID, logical drive, and LUN configuration is completed.	Customer If these tasks were not completed before your arrival, see “Important installation information” on page 3 and “Disk storage configuration guidelines” on page 5.
☐	1–5a	In VTL and FSI, one IP address is assigned for use with a single node installation. Two IP addresses are assigned for use with clustered VTL: • One for 3958 DD6 Server A (single node and clustered) • One for 3958 DD6 Server B (clustered only)	Customer
☐	1–5b	For FSI with 1Gb network interface card (NIC), up to seven IP addresses are assigned for use in a stand-alone installation. • Three for server internal ports (2 for replication and 1 for external). • Four for the Ethernet ports For FSI with 10Gb NIC card, up to 5 IP addresses are assigned for use in a stand-alone installation. • Three for server internal ports (2 for replication and 1 for external). • Two for the Ethernet ports.	Customer

Table 5. Installation workflow checklist (continued)

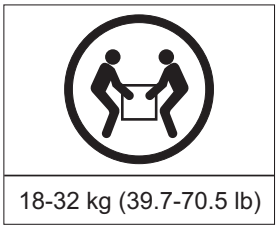
✓	Task	Description	Where to find information
☐	1–6	A separate USB keyboard and graphics-capable monitor (requires a VGA to micro-HDMI adaptor) are available for use during installation. Ideally, these should remain attached.	Customer
☐	1–7	One or more PCs on the local area network (LAN) are designated as ProtecTIER Manager workstations.	Customer
☐	1–8	A VGA to microHDMI converter to attach the graphics-capable monitor.	Customer
Section 2: Install the gateway components			
☐	2–1	Have the customer suspend all I/O activity. Turn off any components that are on.	See the component-specific documentation for power-off instructions.
☐	2–2	Install the 3958 DD6 enclosure (either stand alone, or clustered).	"Installing the ProtecTIER server 3958 DD6" on page 15
Section 3a: Apply cable labels and make cable connections for a stand-alone installation			
☐	3a–1	Label and connect stand-alone installation power connections.	"Power connections" on page 21.
☐	3a–2	Label and connect the back-end fibre channel cables	"Connecting back-end fibre channel cables on the 3958 DD6" on page 21.
☐	3a–3	Label and connect back end Fibre Channel connections.	"Connecting front-end cables on the 3958 DD6" on page 23, then go to section 4.
Section 3b: Apply cable labels and connect cables for clustered installation			
☐	3b–1	Label and connect 1 Cat6 Ethernet cable between the two controllers in the enclosure.	"Cabling a clustered installation for the 3958 DD6" on page 24.
☐	3b–2	Label and connect clustered installation Fibre Channel connections.	"Connecting back-end fibre channel cables on the 3958 DD6" on page 21.
Section 4: Turn on all components			
☐	4–1	Have customer turn on the disk expansion modules.	"Powering up the components on the 3958 DD6" on page 24.
☐	4–2	Turn on the disk controllers.	"Powering up the components on the 3958 DD6" on page 24.
☐	4–3	Turn on power to the enclosure.	"Powering on the servers on the 3958 DD6" on page 25.
Section 5: Connect the keyboard and monitor for use with theTS7650G in doing RAS configuration and verification. Keyboard and monitor should be supplied by the customer.			
Section 6: SSR releases the system to trained ProtecTIER specialist or LBS representative			
☐	6-1	Configure Server A.	Chapter 5, "Configuring Server A," on page 39.
☐	6–2	Install ProtecTIER Manager.	Chapter 6, "Installing ProtecTIER Manager on workstations," on page 55.
☐	6–3	Create the repository.	"Creating the repository" on page 65.
☐	6–4	Configure Server B in a cluster.	Chapter 8, "Configuring Server B," on page 69.
☐	6–5	Test the clustered system.	Chapter 9, "Validating the servers," on page 83.

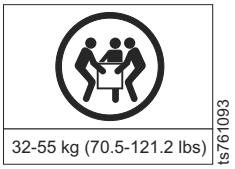
Table 5. Installation workflow checklist (continued)

✓	Task	Description	Where to find information
☐	6–6	Update ProtecTIER software on the servers.	Chapter 10, "Applying updates and fixes to the ProtecTIER software for version 3.4.3 and higher," on page 89.
☐	6–7	Reconfigure RAS settings (if needed)	"Configuring RAS" on page 29.
☐	6–8	Turn the system over to the customer. If replication is being used, advise the customer that it is their responsibility to create and configure the replication grid.	Chapter 11, "Releasing the system to the customer," on page 99

Installing the ProtecTIER server 3958 DD6

CAUTION:
Use safe practices when you lift boxes.





Before you begin

- Review the documentation that comes with the server and rack cabinet for safety and cabling information. The customer-supplied frame might be different from the IBM 3952 Tape Frame Model F05 shown in the figures in this chapter. Be sure to review the documentation that applies to the specific frame you are using, and adjust the procedures as required.
- Review the items that are required to install the server in the rack in the following list.
  - Slide rail components
  - Inner rail stoppers
- If the slide rails in your rack installation kit came with shipping thumbscrews, remove them before you begin the following installation procedure.

About this task

To install either single node or clustered 3958 DD6 in the rack, do the following tasks in order that is shown here.

1. "Installing the slide rails" on page 16
2. "Installing the rail stops" on page 17 (if required)
3. "Installing the server on the slide rails" on page 19

For server frame position, review the following sections about configuration.

- "Single node configuration for the 3958 DD6" on page 10. Summary: Server A installs into EIA positions 5 - 8
- "Clustered configuration for the 3958 DD6" on page 11. Summary:
  - In a single cluster configuration, both Server A and Server B are contained in the 3958 DD6 which is installed into EIA positions 5 - 6

Installing the slide rails

Before you begin

About this task

The left and right rail assembly are marked “LH” and “RH,” and “This Side Up” for correct orientation.

Remember: The left and right orientation of the slide rails is referenced from the front of the rack.

Procedure

1. Attach left and right chassis slides to the enclosure sides using 8 buttonhead screws provided.
2. Assemble the rack brackets to the rack posts as follows:

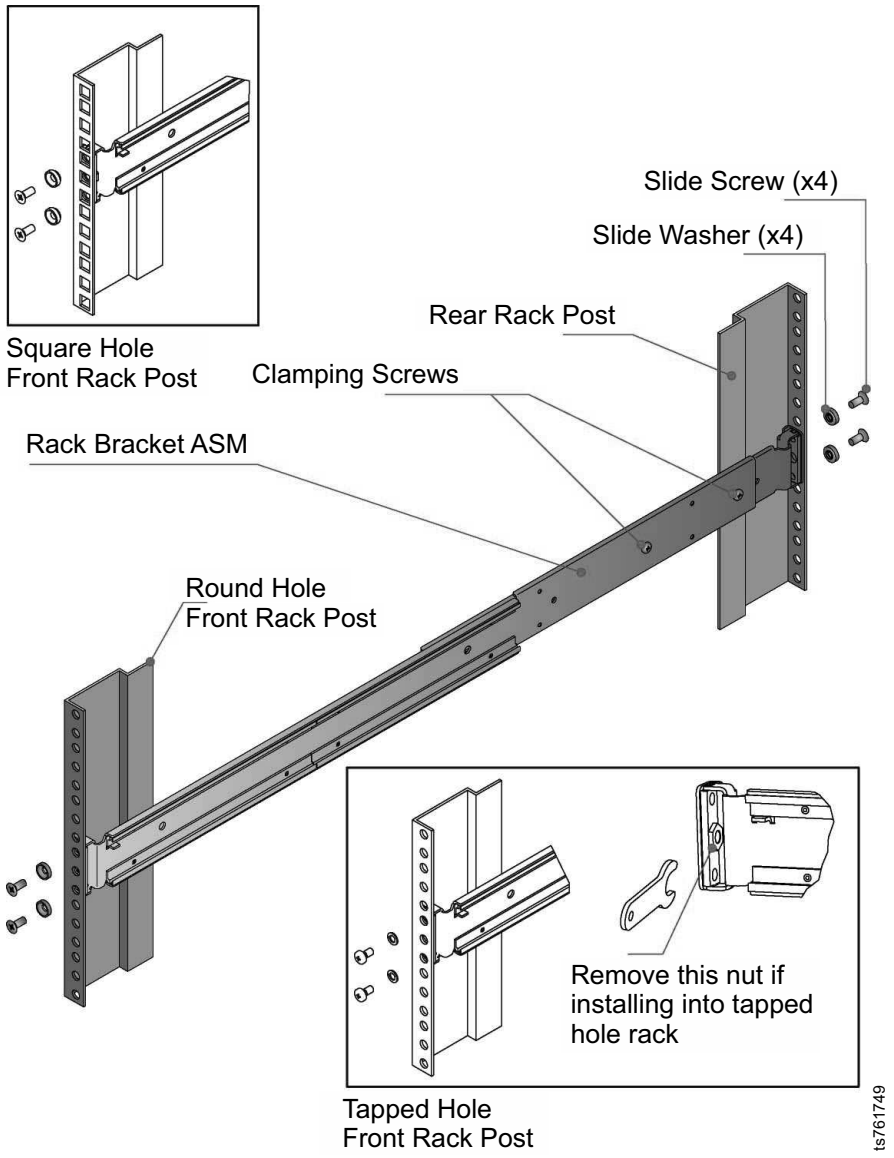


Figure 7. Slide rail components

a. Position the location pin at the rear of the rail into a rear rack post hole. Attach the bracket to the rear rack post using the washers and screws supplied. Do not tighten screws yet, leave them loose for now.
b. Extend rail to fit between the front and rear rack posts.
c. Attach the bracket to the front rack post using the washers and screws supplied. Do not tighten screws yet, leave them loose for now.
d. Tighten the two clamping screws located along the inside of the rear section of the rack bracket

Installing the rail stops

About this task

Use the steps below to attach the inner rail stoppers to the chassis.

Procedure

1. Ensure the Inner Rail is in the correct installation position.

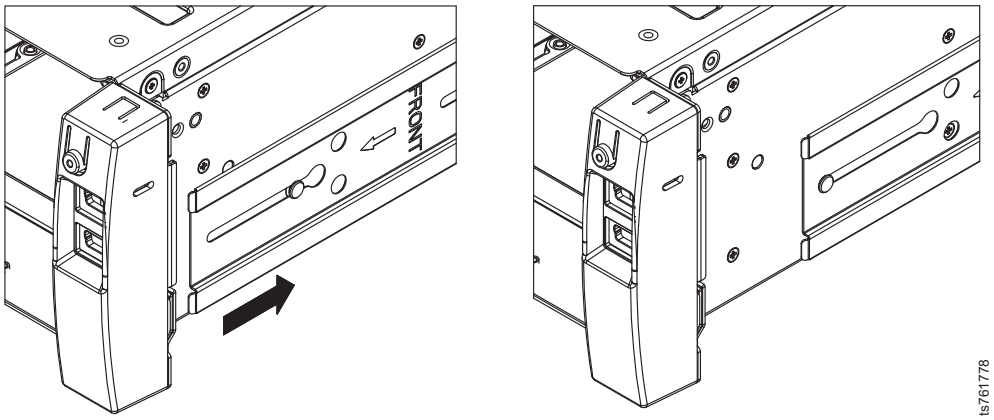


Figure 8. Correct position for the inner rail

2. Using a Phillips head #1 screwdriver remove and discard the highlighted screw from the chassis.

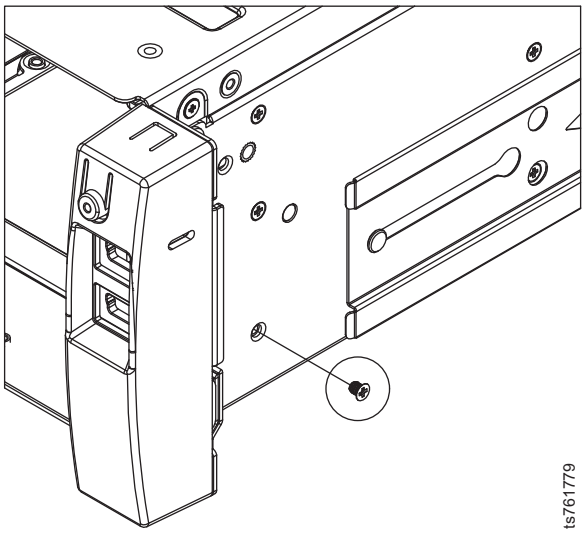


Figure 9. Remove the screw from the chassis

3. Position the provided Inner Rail Stopper as indicated, so as it doesn't overlap any sheet metal and install using the M2.5x6mm CSK screw provided. Tighten screw until secure.

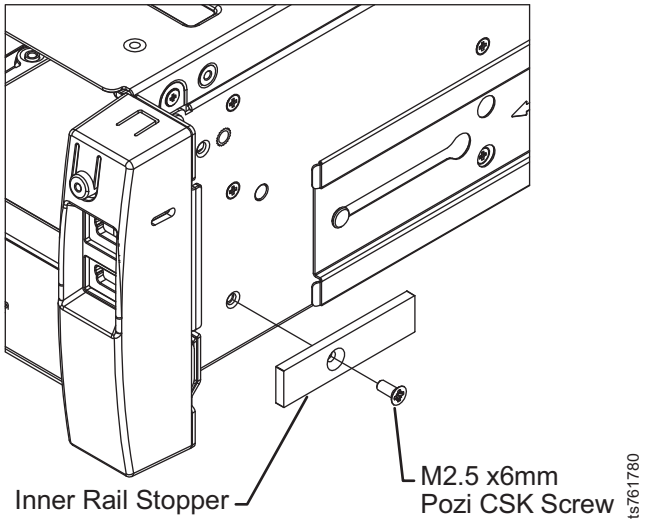


Figure 10. Position the rail stop and screw in place

4. Select one M2.5x6mm CSK screw and one Inner Rail Stopper from the provided kit.
5. Position the provided Inner Rail Stopper as indicated, so as it doesn't overlap any sheet metal and install using the M2.5x6mm CSK screw provided. Tighten screw until secure.

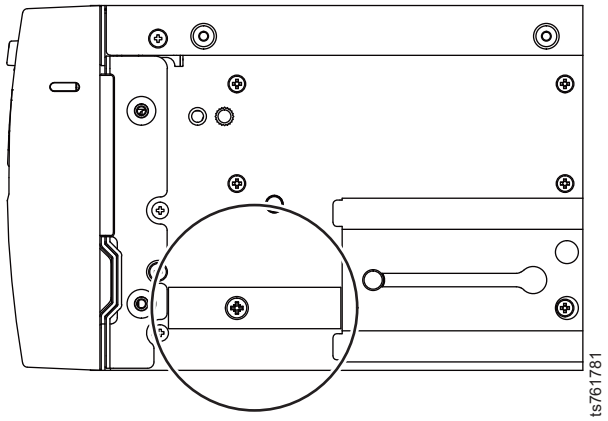


Figure 11. Correct placement of the inner rail stopper

6. Install the remaining rail stopper on the other side of the chassis as described in the preceding steps.

Installing the server on the slide rails

Procedure

Mount the enclosure into the rack as follows.

1. Lift the enclosure and align it with the rack rails.
2. Carefully insert the chassis slides into the rack rails and push fully home.
3. Tighten the rear rack bracket mounting screws.

4. Withdraw enclosure until it reaches the hard stops (approximately 400mm) and tighten the front rack bracket mounting screws.
5. Return the enclosure to the fully home position.

What to do next

Select one of the following options:

- If the rack cabinet is to remain in the current location, you are not required to install the shipping brackets.
- Continue with "Cable label application for 3958 DD6."

Cable label application for 3958 DD6

Applying cable labels

Apply the labels as you connect the cables in the following sections. When you apply labels, align the center reference lines on the label with the axis of the cable. See *IBM Labeling Instructions for the TS7650 ProtecTIER Deduplication Appliance and TS7650G ProtecTIER Deduplication Gateway*, PN 95P8942 for label placement guidelines and instructions.

Table 6. Label legend

Abbreviation	Meaning in IBM best practices installations	Meaning in other installations
E1	Ethernet 1 (eth0)	Replication network 1
E2	Ethernet 2 (eth1)	Replication network 2
E3	Ethernet 3 (eth2)	Customer LAN and BMC
DD6A	ProtecTIER server (3958 DD6)	Same
DD6A	The only ProtecTIER server in a single-node configuration or the bottom ProtecTIER server in a clustered configuration	Same
DD6B	The second ProtecTIER server in a clustered configuration, located in the same enclosure and above DD6A	Same
EXP	Disk expansion module (Feature Code 3707: 4.8 TB Fibre Channel Disk Expansion Unit)	Local equivalent disk expansion system enclosure
H1	Disk controller host port 1	Same
H2	Disk controller host port 2	Same
HOST	Customer host	Same
P1	Disk controller drive port 1	Same
P2	Disk controller drive port 2	Same
REPL	Replication	Same
SC KVM	System console KVM assembly	Same
SM	Designation for the system management (SYS MGMT) port on the DD6 server	Same
L PSU	Left PSU	Left power supply
R PSU	Right PSU	Right power supply
VTL	Virtual Tape Library storage	Same

What to do next

Choose one of the following options:

- If you are installing a stand-alone configuration, go to “Cabling a single node installation for the 3958 DD6.”
- If you are installing a clustered configuration, go to “Cabling a clustered installation for the 3958 DD6” on page 24.

Cabling a single node installation for the 3958 DD6

After you install the hardware, you must connect cables and apply cable labels to the components included in the purchase of the TS7650G single node gateway. For other supported components, see the manufacturers documentation for details.

You install cables to connect the 3958 DD6 to front-end interfaces such as hosts and backups, and to back-end interfaces such as storage devices and repositories. Front-end interfaces can be either fibre channel (for VTL) or Ethernet (for FSI). Back-end interfaces use only fibre channel.

Note: Category 6, or higher, cable is required for all Ethernet connections.

Power connections

Note: The power distribution units might already be installed in the frame in a location different from what is shown in the illustration. For consistency and ease when troubleshooting, consider relocating the power distribution units to match the figure entitled "Single node power connections on the DD6."

Procedure

Label and connect the power cables.

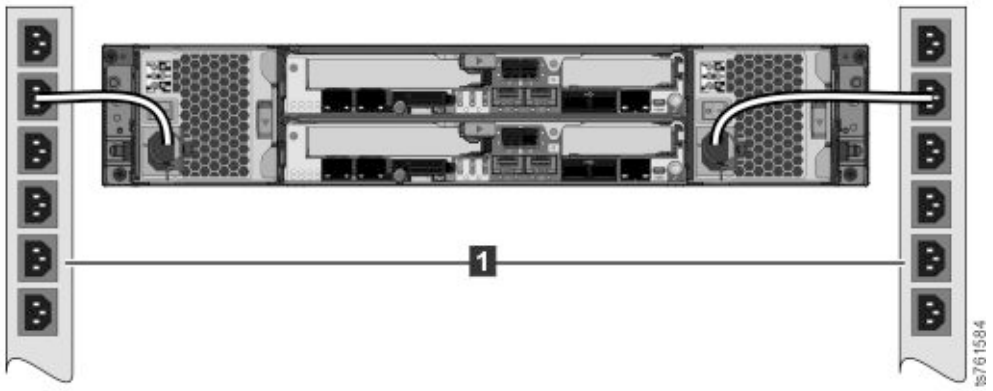


Figure 12. Single node power connections on the DD6

Connecting back-end fibre channel cables on the 3958 DD6

After you make the power connections, you next connect the Fibre Channel cables and apply cable labels to theTS7650G in a single node configuration. DD6 supports the following fibre cards on VTL: Emulex LPe15004 for backend and Emulex 00WT000 for the front end.

Important:

This document references IBM 4.8 TB Fibre Channel Disk Controllers and IBM 7.2 TB Fibre Channel Disk Expansion Units in many of the hardware installation figures, examples, and procedures.

The IBM TS7650G supports the DS5000 disk controller, the DS8000 disk controller, Storwize V7000 Storage Controller and the XIV disk controller, as well as various non-IBM storage solutions. If the customer has elected to use disk storage components other than the IBM disk controllers and expansion units mentioned above, the figures, examples, and procedures in this document will not apply to the configuration on which you are working. Therefore, it is suggested that you determine the make and model of the disk storage components in use and, if necessary, obtain the related product documentation before you begin installation of the gateway.

For TS7650G servers, the RAS function does not send Call Home packages for problems with any of the disk storage products attached to the server.

Procedure

Connect Fibre Channel cables between the ProtecTIER server and the storage components according to Figure 13. To help track your progress during this task, consider making the connections from top to bottom. Follow the order in which the tasks are listed in the table and mark the "✓ when complete" column after you make the connection and label the cable.. The back-end connections for an FSI configuration are identical to the VTL connections.

Note: Figure 13 shows a VTL configuration.

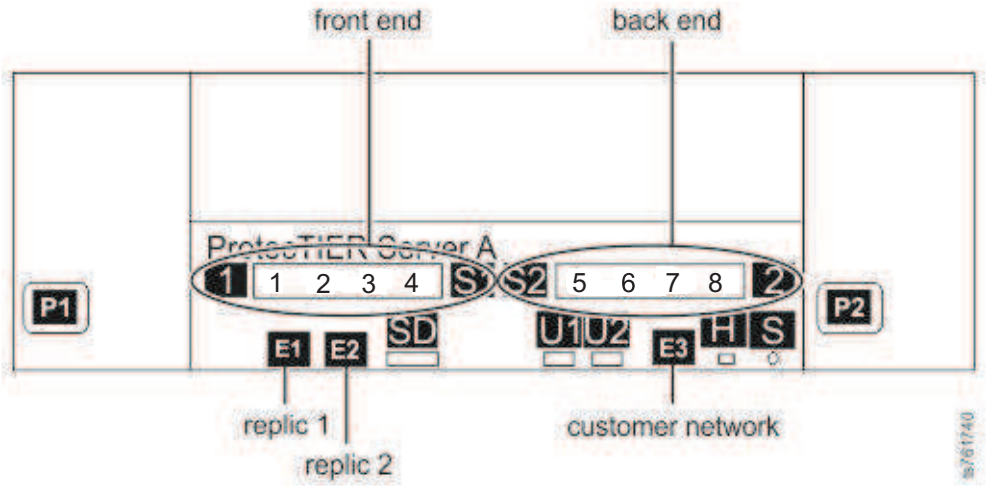


Figure 13. Fibre Channel connections for single node configuration on a DD6

Table 7. Back-end connections for single node configuration (VTL or FSI

✓ when complete	Item	From	To	Remarks
	5	DD6 A	Customer specified SAN switch or Disk Controller	
	6	DD6 A	Customer specified SAN switch or Disk Controller	

Table 7. Back-end connections for single node configuration (VTL or FSI (continued)

✔ when complete	Item	From	To	Remarks
	7	DD6 A	Customer specified SAN switch or Disk Controller	
	8	DD6 A	Customer specified SAN switch or Disk Controller	

Connecting front-end cables on the 3958 DD6

If you are installing a single node VTL, connect front-end Fibre Channel cables between ProtecTIER server A and the customer host Fibre Channel network. The 3958 DD6 supports the Emulex 00WT000 for the front end connections.

Procedure

1. Connect Fibre Channel cables between the ProtecTIER server and the customer host Fibre Channel network according to Figure 14. To help track your progress during this task, consider making the connections from top to bottom. Follow the order in which the tasks are listed in the table and mark the "✔ when complete" column after you make the connection and label the cable..

   Note: Figure 13 on page 22 shows a VTL configuration.

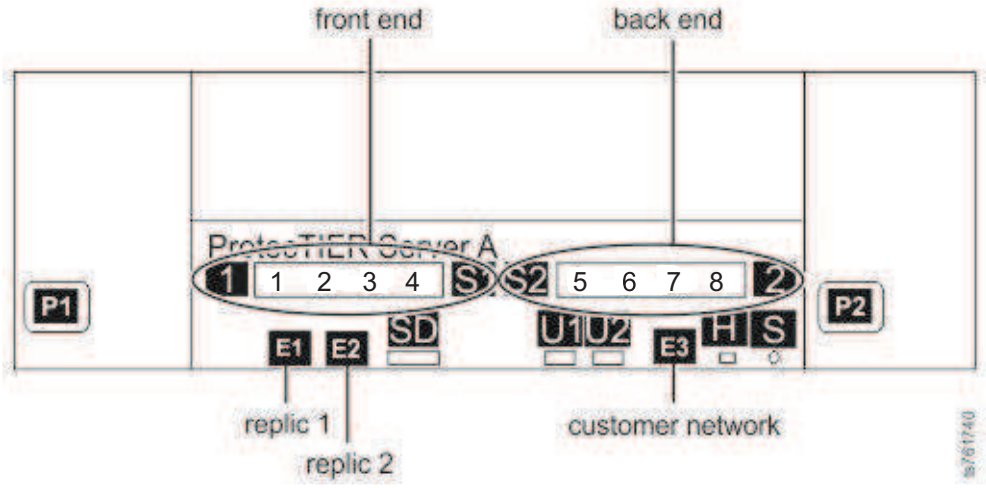


Figure 14. Front-end Fibre Channel connections for single node configuration on a DD6

Table 8. Front-end connections for single node configuration

✔ when complete	Item	From	To	Remarks
	1	DD6 A	Customer specified SAN switch or host port	
	2	DD6 A	Customer specified SAN switch or host port	
	3	DD6 A	Customer specified SAN switch or host port	
	4	DD6 A	Customer specified SAN switch or host port	

2. Continue with “Powering on the servers on the 3958 DD6” on page 25

Connecting front-end cables on the 3958 DD6

If you are installing a single node FSI, connect front-end 1 Gbps or 10 Gbps ProtecTIER ports and the customer host Ethernet network.

Procedure

1. Connect Etherneyt cables between the ProtecTIER server and the customer host Ethernet network according to Figure 15. To help track your progress during this task, consider making the connections from top to bottom. Follow the order in which the tasks are listed in the table and mark the "✓ when complete" column after you make the connection and label the cable..

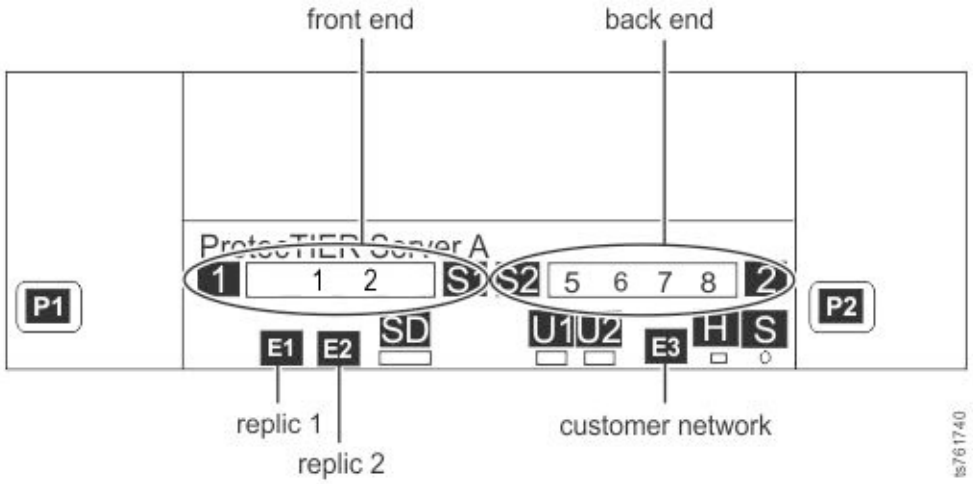


Figure 15. Front-end Ethernet connections for single node configuration on a DD6

Table 9. Front-end connections for single node configuration

✓ when complete	Item	From	To	Remarks
	1	DD6 A	Customer specified Ethernet switch or host port	
	2	DD6 A	Customer specified Ethernet switch or host port	

2. Continue with “Powering on the servers on the 3958 DD6” on page 25

Cabling a clustered installation for the 3958 DD6

In a clustered configuration use a Cat6A cable to connect the Ethernet 1 connections on each controller together for networking.

Powering up the components on the 3958 DD6

Power up the hardware components in the order in the following list.

1. Frame breakers
2. Power distribution units
3. AC power to the enclosures
4. Disk expansion modules

5. Disk controllers

For more information about power-up procedures for each component type, see the related sections that follow.

Power on indicators

There are three LEDs labeled OK, Fault and ID on the rear on the canister During startup, all three light up for less than a second. When the other two lights go off, the OK light blinks for more than a minute. When the OK light stops blinking, the Fault LED blinks once and the OK LED remains on. When all systems are operating in a normal state, only the OK light remains illuminated.

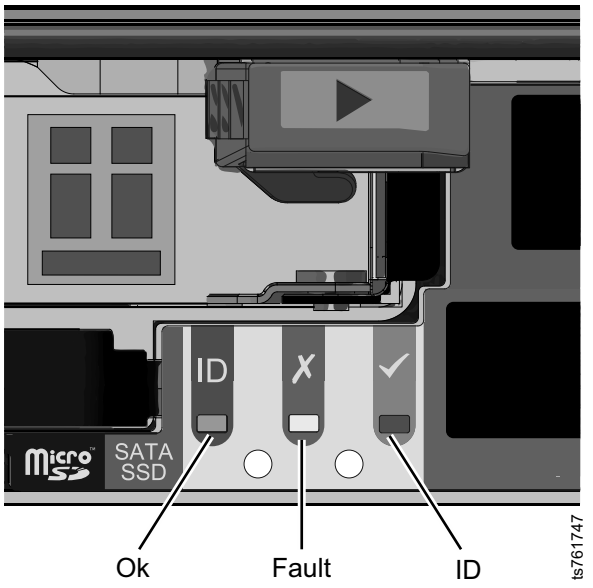


Figure 16. Power on indicators on the rear of the canister

Powering on the disk expansion modules

In general, it is best to power on the disk expansion units before you power on the disk controllers.

Powering on the disk controllers

For power-on instructions, see the documentation that came with the specific disk controllers in the installation.

Powering on the servers on the 3958 DD6

About this task

This is the recommended manual power on sequence for a TS7650G server.

Procedure

1. Using the frame's UPO switch or the customer's circuit breaker, restore power to the frame (or frames).
2. Power on all expansion units.
3. Power on all storage controllers.
4. Attach the AC power cords to the PCMs or PSUs.

The chassis policy is "always on" so the BMC causes a staged boot of the x86 subsystem.

On starting up, the Genesis Enclosure Management (GEM) software performs an enclosure validation procedure. This is the process of determining whether the PSUs can supply sufficient power for the system's high power elements (such as the CPU, chipset and drives). This protects against mis-configuration of the hardware. Until this validation has succeeded, power consumption is kept under 60W.

5. Turn on the power switch on each of the PCM/PSU rear panels. The BMC will start to boot.
6. Press the power button on the server's rear panel.

   The server will power on. The System Power LED on the left front operator information panel indicates if the system is in Standby mode (amber) or if it is powered on and operational (green). If the LED does not come on, there is no power to the system.

Visual inspection of indicator and fault LEDs

Visually inspect the indicator and fault LEDs on all TS7650G servers and other hardware components.

- Verify that the eth1 and eth2 Ethernet links (to replication or cluster) indicate 10Gbps and that eth3 (customer network) is at 1Gbps. All connections must be at a minimum of 1000 Mbps for the cluster configuration to work.
- If all link-up indicators and fault LEDs show normal operation, close the front and rear covers of the frames.
- If an amber LED on any component is lit, see the documentation for the component to diagnose and remedy the problem. The network power switch displays an amber light for "normal" operation status. See the *IBM Problem Determination and Service Guide for the TS7650G ProtecTIER Deduplication Gateway*, GA32-0923 for more information.

Next steps

When the TS7650 Gateway Server based on the 3958 DD6 is successfully installed the SSR continues with the following instructions:

- Configure ProtecTIER RAS (Reliability, Availability, Serviceability) on the ProtecTIER server or servers
- Perform RAS verification and test Call Home

After the SSR completes the RAS configuration and verification, the trained ProtecTIER specialist follows the instructions in Chapter 5, "Configuring Server A," on page 39 through Chapter 9, "Validating the servers," on page 83 to:

- Configure ProtecTIER on Server A
- Install ProtecTIER Manager and create the data repository
- Configure ProtecTIER on Server B (cluster only)
- Validate cluster configuration (cluster only).

When all SSR and trained ProtecTIER specialist tasks are complete, the trained ProtecTIER specialist turns the system over to the customer.

Note: In a replication environment, the trained ProtecTIER specialist also informs the customer that before replication is fully functional, the customer must create

and configure the replication grid. Instructions for doing so are in the *IBM ProtecTIER User's Guide for VTL Systems*, GA32-0922.

Chapter 4. Enabling ProtecTIER RAS functions on the 3958 DD6

ProtecTIER RAS was installed during manufacturing. However, it must be enabled for the TS7650G server to interact with Call Home, log collection, and system health monitoring.

Before you begin

TS7600 products depend on RAS to gather logs at the time of the failure and send a Call Home packet. When RAS is not enabled, the customer must call 1(800) IBM SERV (in North America, only) or visit http://www.ibm.com/planetwide/ to obtain hardware support.

Further disaster recovery information to assist the customer in restoration is available in the *IBM ProtecTIER User's Guide for VTL Systems*, GA32-0922, on the *IBM TS7650 with ProtecTIER Publications* CD.

Verify that the following prerequisites are met before you start RAS enablement:

1. The disk components are installed, configured, cabled, and powered-on.
2. A graphics-capable monitor and USB keyboard are available for use during the installation process.
3. The customer-provided information that is requested in Appendix A, "Company information worksheet," on page 101.

About this task

The ProtecTIER RAS enablement procedure does the following tasks:

- Collects machine properties for the machine type reported product data (MRPD) from the system, and requests system and customer information from the IBM service representative who is installing the system.

Configuring RAS

You configure ProtecTIER RAS on the server or servers in both single node and clustered TS7650G configurations by using commands from the **ProtecTIER Configuration** menu.

Before you begin

Note: Enabling and configuring RAS is an offline procedure; respond `yes` when prompted to stop VTFD services. The services normally restart automatically upon completion of RAS configuration, but this procedure includes steps to verify the restart and, if required, to restart the services manually. You can configure RAS either now or during the ProtecTIER installation.

About this task

During the installation, you are prompted to enter the system and customer contact information listed. You must have the information for each server in the cluster. Consider collecting the necessary information before you start the installation, so it is readily available when needed. This information can be found

on the completed Company Information and IP address worksheets. See Appendix A, “Company information worksheet,” on page 101 and Appendix B, “IP address worksheet,” on page 105 for details about the information that you must enter.

- Business company name
- System location
- Callback number
- Voice phone number
- Disk array machine type and model number
- Disk array serial number
- Customer number
- Country code

  Note: This number is the two-digit, IBM-assigned country code that is used to order software or to acquire software support. Do not confuse this number with the three-digit RETAIN country code.
- Simple Mail Transfer Protocol (SMTP) server IP address (optional)
- Customer email address (optional)

Procedure

1. Establish a connection to Server A. To do so:
   a. Attach a USB keyboard to any open USB port on the back of the server.
   b. Attach a graphics-capable monitor to the video port on the back of the server.

   Note: If you are unable to connect to the server with this procedure, try to use the server BMC and your service notebook. See “Direct connection with a USB keyboard and monitor” on page 115 for instructions.
2. At the command prompt, log in to the ProtecTIER server (see 2 on page 42 of Chapter 5, “Configuring Server A,” on page 39).

   Note: During the boot cycle, the ProtecTIER file systems are mounted. If the message: `Running...` displays, press Enter to proceed to the login prompt.

3. Enable RAS on the server with the following method:
   a. At the command line, type `menu` and press Enter. The **ProtecTIER Service** menu displays.

```
--------------------------------------------------------------------------
  ProtecTIER Service Menu running on rasddx
--------------------------------------------------------------------------
   1) ProtecTIER Configuration (...)
   2) Manage ProtecTIER services (...)
   3) Health Monitoring (...)
   4) Problem Alerting (...)
   5) Version Information (...)
   6) Generate a service report
   7) Generate a system view
   8) Update ProtecTIER code

   E) Exit
--------------------------------------------------------------------------
>>> Your choice?
```

   b. Type the numeral corresponding to **ProtecTIER Configuration** and press Enter.

      The **ProtecTIER Configuration** menu displays.

```
--------------------------------------------------------------------------
  ProtecTIER Service Menu running on rasddx
  ProtecTIER Configuration (...)
--------------------------------------------------------------------------
   1) Configure ProtecTIER node
   2) Recover Configuration for a replaced server
   3) Configure machine serial number for a replaced server
   4) Configure RAS
   5) Update Time, Date, Timezone & Timeserver(s)
   6) Scan storage interconnections
   7) File Systems Management (...)
   8) Configure replication (...)
   9) IP Network configuration (...)
   10) Update Firmware
   11) Update the System's name
   12) Validate configuration
   13) Single node - code upgrade (for Support Use Only)

   B) Back
   E) Exit
--------------------------------------------------------------------------
>>> Your choice?
```

c. Type the numeral corresponding to **Configure RAS** and press Enter. Output similar to the following screen appears. Values that are shown are for example purposes only. Follow the instructions and respond to prompts with information gathered on Appendix A, "Company information worksheet," on page 101 and Appendix B, "IP address worksheet," on page 105 to complete the configuration process.

   Tip: You can use the key combinations `Shift+Page Up` and `Shift+Page Down` to move through lists of items that do not fit entirely on the screen.

   Note: If you do not configure the SMTP server now, you are prompted again during ProtecTIER setup. See Chapter 5, "Configuring Server A," on page 39.

```
Begin Processing Procedure

Stopping Cluster Services                                        [ Done ]
Configuring RAS
Configuring RAS network                                          [ Done ]
Configuring IMM/RSA                                              [ Done ]

Please provide the following information:
-----------------------------------------
Customer SMTP server IP address (optional):
Customer number:
     Input should be 7 alphanumeric: abcderf
Country code:
     Input should be 2 or 3 alphanumeric: av
Business company name, e.g. IBM, (optional):
Machine location, e.g. Server room, (optional):
MODEM Phone number, (optional):
Voice Phone number, (optional):

Please check the following values:
----------------------------------
Customer SMTP server IP address:
     The first administrator email-address:
     The second administrator email-address:
     The third administrator email-address:
Customer number: abcderf
Country code: av
Business company name:
Machine location:
MODEM Phone number:
Voice Phone number:
Are you sure you want to submit these RAS values? (yes|no|quit) y
Saving configuration                                             [ Done ]
RAS Configuration ended successfully

End Processing Procedure Successfully

Press <ENTER> to continue
```

4. When RAS configuration is complete on Server A, choose one of the following options:
   - If you are installing a single node configuration, go to "RAS verification" on page 35.
   - If you are installing a clustered configuration, go to step 5.
5. Disconnect the USB keyboard and monitor from Server A and connect them to Server B.

   Note: If you are unable to connect to the server with this procedure, try to use the server BMC and your service notebook. See Appendix C, "Connect to BMC using a web-browser," on page 113 for instructions.

6. Repeat steps 2 on page 30 and 3 on page 31 to configure RAS on Server B.
7. When RAS configuration is complete on both servers, go to "RAS verification" on page 35.

Verifying the Ethernet connections for the clustered TS7650G 3958 DD6

Before you verify RAS configuration, ensure that the Ethernet connections for the cluster are configured correctly.

Procedure

1. Use `kudzu` to run this command and view the output to ensure that the Intel Ethernet cards and Broadcom Ethernet cards have the correct port assignments:
   - For VTL systems, the Intel Ethernet cards are assigned to ports eth0, eth1, and eth2.
   - The output is similar to the following example:

```
[root@chino ~]# kudzu -p -c network | grep -A3 "device:"
device: eth0
driver: e1000e
desc: "Intel Corporation 82571EB Gigabit Ethernet Controller (Copper)"
network.hwaddr: 00:15:17:df:8a:95
--
deviceId: 10bc
subVendorId: 8086
subDeviceId: 11bc
pciType: 1
--
device: eth1
driver: e1000e
desc: "Intel Corporation 82571EB Gigabit Ethernet Controller (Copper)"
network.hwaddr: 00:15:17:e8:7e:ef
--
deviceId: 10bc
subVendorId: 8086
subDeviceId: 11bc
pciType: 1
--
device: eth4
driver: e1000e
desc: "Intel Corporation 82571EB Gigabit Ethernet Controller (Copper)"
network.hwaddr: 00:21:5e:c5:96:b4
--
deviceId: 10bc
subVendorId: 8086
subDeviceId: 11bc
pciType: 1
--
device: eth11
driver: e1000e
desc: "Intel Corporation 82571EB Gigabit Ethernet Controller (Copper)"
network.hwaddr: 00:15:17:e8:7e:ee
--
deviceId: 10bc
subVendorId: 8086
subDeviceId: 11bc
pciType: 1
--
device: eth2
driver: e1000e
desc: "Intel Corporation 82571EB Gigabit Ethernet Controller (Copper)"
network.hwaddr: 00:15:17:df:8a:97
--
```

```
deviceId: 10bc
subVendorId: 8086
subDeviceId: 11bc
pciType: 1
--
device: eth3
driver: e1000e
desc: "Intel Corporation 82571EB Gigabit Ethernet Controller (Copper)"
network.hwaddr: 00:15:17:df:8a:96
--
deviceId: 10bc
subVendorId: 8086
subDeviceId: 11bc
pciType: 1
--
device: eth5
driver: e1000e
desc: "Intel Corporation 82571EB Gigabit Ethernet Controller (Copper)"
network.hwaddr: 00:15:17:e8:7e:ef
--
deviceId: 10bc
subVendorId: 8086
subDeviceId: 11bc
pciType: 1
--
device: eth6
driver: e1000e
desc: "Intel Corporation 82571EB Gigabit Ethernet Controller (Copper)"
network.hwaddr: 00:15:17:e8:7e:ef
--
deviceId: 10bc
subVendorId: 8086
subDeviceId: 11bc
pciType: 1
--
device: eth8
driver: e1000e
desc: "Intel Corporation 82571EB Gigabit Ethernet Controller (Copper)"
network.hwaddr: 00:15:17:e8:7e:ef
--
deviceId: 10bc
subVendorId: 8086
subDeviceId: 11bc
pciType: 1
--
device: eth7
driver: e1000e
desc: "Intel Corporation 82571EB Gigabit Ethernet Controller (Copper)"
network.hwaddr: 00:15:17:e8:82:de
--
deviceId: 10bc
subVendorId: 8086
subDeviceId: 11bc
pciType: 1
--
device: eth9
driver: e1000e
desc: "Intel Corporation 82571EB Gigabit Ethernet Controller (Copper)"
network.hwaddr: 00:15:17:e8:7e:ef
--
deviceId: 10bc
subVendorId: 8086
subDeviceId: 11bc
pciType: 1
--
device: eth10
driver: e1000e
```

```
desc: "Intel Corporation 82571EB Gigabit Ethernet Controller (Copper)"
network.hwaddr: 00:15:17:e8:7e:ef
--
deviceId: 10bc
subVendorId: 8086
subDeviceId: 11bc
pciType: 1
--
device: eth12
driver: bnx2
desc: "Broadcom Corporation NetXtreme II BCM5709 Gigabit Ethernet"
network.hwaddr: 00:21:5e:c5:96:b4
--
deviceId: 1639
subVendorId: 1014
subDeviceId: 03b5
pciType: 1
--
device: eth13
driver: bnx2
desc: "Broadcom Corporation NetXtreme II BCM5709 Gigabit Ethernet"
network.hwaddr: 00:21:5e:c5:96:b6
--
deviceId: 1639
subVendorId: 1014
subDeviceId: 03b5
pciType: 1
--
device: usb0
driver: cdc_ether
desc: "IBM RNDIS/CDC ETHER"
network.hwaddr: 02:21:5e:c5:b9:8b
--
deviceId: 4010
usbmfr: IBM
usbprod: RNDIS/CDC ETHER
[root@chino ~]
```

Note: The values for `hwaddrs` are specific to the Ethernet cards in each system.

2. Use `ethtool` to verify that a link is detected and operational on each port, as expected by the customer network configuration. Enter the following command for each port, replacing eth1 each time with the next port, for example, eth2, then eth3, then eth4, until all ports are checked.

   Note: If some ports are not used in the customer environment, such as the replication ports, they might be reported as not operational or have no link that is detectable. This appearance is the expected result if the ports are not being used.

   ```
   ifconfig eth1 up
   # ethtool eth1
   ```

3. Note the results of these procedures and pass them on to the trained ProtecTIER specialist/LBS representative for their use during ProtecTIER configuration.
4. Go to "RAS verification."

RAS verification

After RAS configuration, you must verify and validate RAS and test Call Home.

Remote support through Call Home

Remote support is available for the TS7650G through the Call Home capability provided either in the ProtecTIER software or with TSSC. Please note that TSSC with the Call Home feature is not available on the 3958 DD6 server; however, Call Home is supported for 3958 DD6 using native call home tools provided in the ProtecTIER software. The Call Home feature reports failures detected by the ProtecTIER servers. Whenever a failure is detected, Call Home sends detailed error information to IBM (*home*). The IBM Service Representative can then prepare an action plan to handle the problem before traveling to the affected installation. The appliance or gateway might also periodically send support information (such as configuration, code versions, and error logs) to IBM. Doing so speeds-up problem determination and fault resolution. When enabled on the appliance and gateway, Call Home uses a connection on your Ethernet network to transmit hardware and software problem reports to IBM. Call Home is enabled and tested by IBM Service Representatives during initial system installation.

When the Reliability, Availability, and Serviceability (RAS) software on the ProtecTIER server detects an error condition, Call Home sends detailed error information to IBM (*home*). If the error indicates a problem with a field replaceable unit (FRU), an IBM Service Representative can then prepare an action plan to handle the problem before traveling to your site.

The TS7650Gprovides four Call Home capabilities: Problem Call Home, Heartbeat Call Home, Test Call Home, and User-Initiated Call Home; descriptions follow. RAS sends data files that may be helpful to IBM Support Center personnel for all four types of Call Home. These data files include error logs and configuration information, such as the Machine Reported Product Data (MRPD) log.

Test Call Home
The IBM Service Representative sends a Test Call Home signal after enabling the Call Home feature during initial installation. You can also send a Test Call Home to ensure that the setup is correct and that the appliance or gateway can successfully open a Problem Management Record (PMR) in the IBM Remote Technical Assistance Information Network (RETAIN).

Problem Call Home
When RAS detects a problem, RAS initiates a Call Home operation to create a PMR in RETAIN. The PMR is a single page of text data that enables the Support Center or the Service Representative to access an action plan and a list of applicable FRU components.

Heartbeat Call Home
To ensure proper ongoing Call Home functionality, the system sends a Heartbeat Call Home on a regularly-scheduled basis. The heartbeat interval is user-defined.

User-Initiated Call Home
You can manually initiate Call Home from the TSSC GUI to collect a product engineering (PE) package.

For more information about Electronic Customer Care (ECC) and TSSC, refer to the following topics:

- Call Home through ECC
- Call Home through the TSSC

Running a test Call Home

To verify that Call Home is installed and enabled, you can run a test Call Home.

- To run a test Call Home from the command line, enter the following command:
  `/opt/ras/bin/rsCerCHTest`
- To run a test Call Home from the ProtecTIER Service menu (see ProtecTIER Service menu), type the option numbers to initiate a test Call Home.
  - For ProtecTIER V2.5 or earlier, select **Call Home Commands** > **Test Call Home**.
  - For ProtecTIER V3.1 or later, select **Problem Alerting** > **Send a Test Call Home**.

If the return message is `Test Call Home sent successfully`, then the system has completed the test. Contact your next level of support if you encounter any of the following problems:

- The test Call Home fails.
- The test Call Home does not show in the Call Home Queue.
- The **Call Home Switched** column retains an NA after enabling.

Chapter 5. Configuring Server A

About this task

Server A refers to either the only server in a single node configuration or the first (bottom) server in a clustered configuration. In the following procedures, the system output might also use the term *Node A* to mean the same thing. Commands are case-sensitive. Use care to enter the characters exactly as shown.

Note: If you are working with new servers (directly from the factory), the most current versions of Red Hat Linux and ProtecTIER software are preinstalled.

If you are not working with new servers (direct from the factory), you must install the most current versions of Red Hat Linux and ProtecTIER software code before you configure ProtecTIER.

Attention: If you are working with a clustered configuration, you must do the following tasks before you configure Server B:

- Configure Server A (this procedure)
- Install ProtecTIER Manager (Chapter 6, “Installing ProtecTIER Manager on workstations,” on page 55)
- Create a repository and file systems on Server A (Chapter 7, “Creating repositories,” on page 61)

Procedure

1. Configuration failure can result from IP address conflicts in installations with multiple servers. To prevent configuration failure, disconnect cables from replication (VTL and FSI) and customer host network Ethernet (FSI only) ports. Choose one of the following options, depending upon your installation.

   Option 1: VTL

   Remove replication cables from server ports that are labeled **19** and **20** in Figure 17.

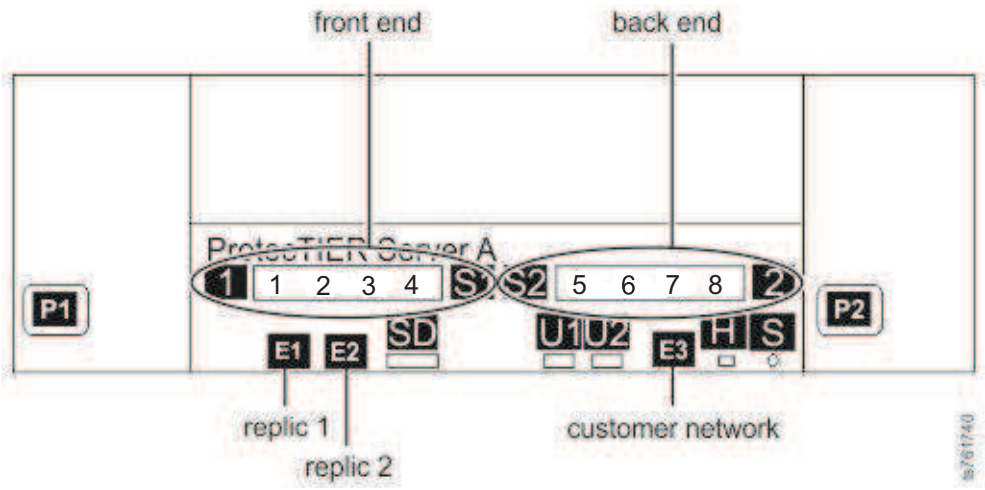


Figure 17. Customer and replication Ethernet connections for single node VTL configuration

Option 2: 1 Gb FSI (FC 3456)

a. Remove replication cables from server ports that are labeled **15** and **16** in Figure 18.

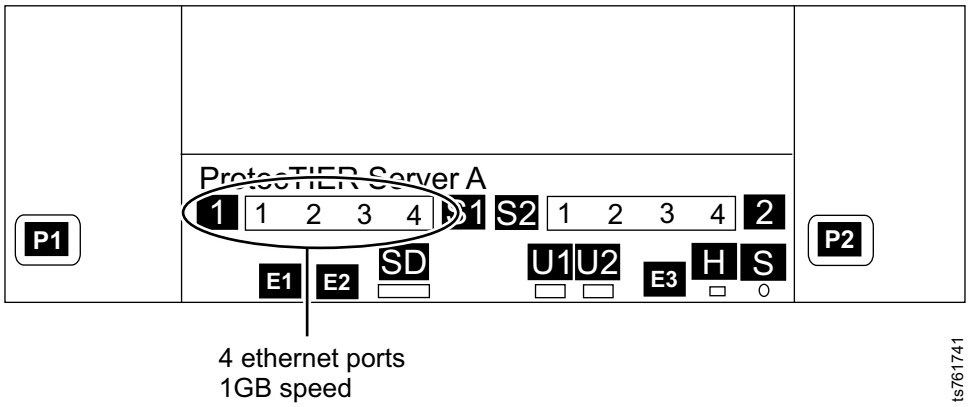


Figure 18. Customer and replication Ethernet connections for single node 1 Gb FSI configuration, Feature Code 3456

b. Remove customer host network Ethernet connections that are labeled **1 - 8** in Figure 19. Not all of these connections might exist, depending upon the customer.

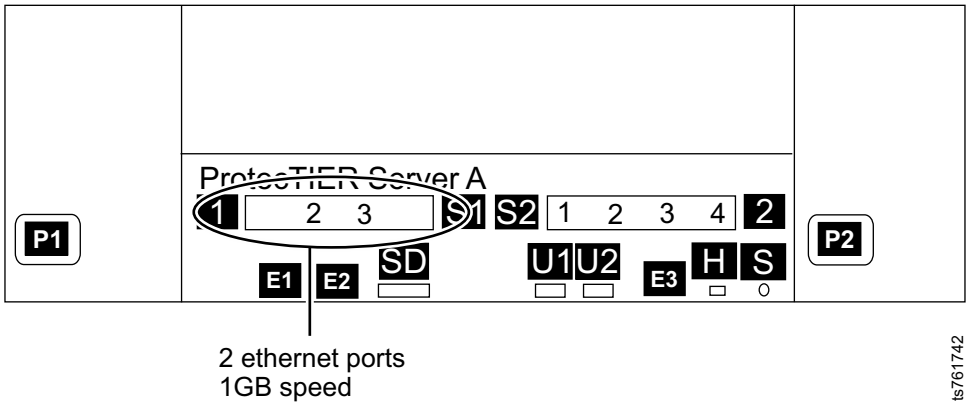


Figure 19. Customer and replication Ethernet connections for single node 1 Gb FSI configuration, Feature Code 3456

Remove cables.

Option 3: 10 Gb FSI (FC 3457)

a. Remove replication cables from server ports that are labeled **15** and **16** in Figure 20.

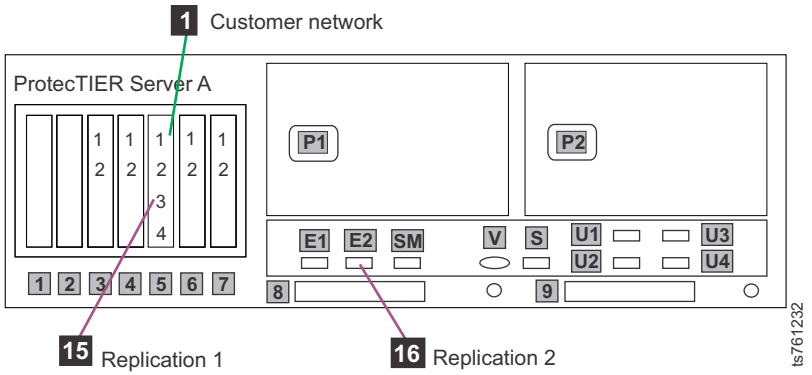


Figure 20. Customer and replication Ethernet connections for single node FSI configuration, Feature Code 3457

b. Remove customer host network Ethernet connections that are labeled **13 - 16** in Figure 21. Not all of these connections might exist, depending upon the customer.

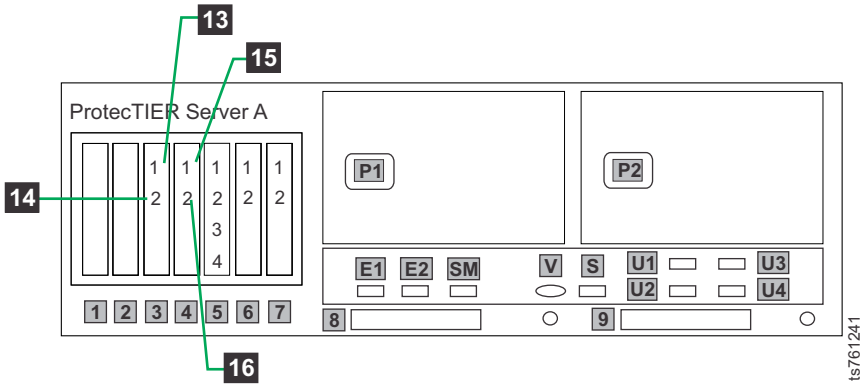


Figure 21. Customer and replication Ethernet connections for single node 10 Gb FSI configuration, Feature Code 3457

2. Log in to Server A.
   a. Connect the USB keyboard and monitor to Server A.
   b. Verify that Server A is powered up and the startup cycle is complete.

      Note: The startup cycle is complete when the system returns to a command prompt, or the message `RUNNING` is displayed on the monitor. Press Enter to get to the login prompt.
   c. If this is a clustered configuration, verify that Server B (the top server) is powered off.
   d. At the login prompt, type: `ptadmin` and press Enter.
   e. At the password prompt, type: `ptadmin` and press Enter.

3. At the command line, type `menu` and press Enter. The **ProtecTIER Service** menu displays.

```
--------------------------------------------------------------------------
  ProtecTIER Service Menu running on rasddx
--------------------------------------------------------------------------
   1) ProtecTIER Configuration (...)
   2) Manage ProtecTIER services (...)
   3) Health Monitoring (...)
   4) Problem Alerting (...)
   5) Version Information (...)
   6) Generate a service report
   7) Generate a system view
   8) Update ProtecTIER code

   E) Exit
--------------------------------------------------------------------------
>>> Your choice?
```

4. Type the numeral corresponding to `ProtecTIER Configuration` and press Enter. The **ProtecTIER Configuration** menu displays.

```
--------------------------------------------------------------------------
  ProtecTIER Service Menu running on rasddx
  ProtecTIER Configuration (...)
--------------------------------------------------------------------------
   1) Configure ProtecTIER node
   2) Recover Configuration for a replaced server
   3) Configure machine serial number for a replaced server
   4) Configure RAS
   5) Update Time, Date, Timezone & Timeserver(s)
   6) Scan storage interconnections
   7) File Systems Management (...)
   8) Configure replication (...)
   9) IP Network configuration (...)
   10) Update Firmware
   11) Update the System's name
   12) Validate configuration
   13) Single node - code upgrade (for Support Use Only)

   B) Back
   E) Exit
--------------------------------------------------------------------------
>>> Your choice?
```

5. Type the numeral corresponding to `Configure ProtecTIER node` and press Enter.

6. The system checks your hardware and presents one of two selection menus.
   Example (VTL)

```
1. VTL
```

   VTL is the only option
   Example (FSI)

```
1. FSI_10G
```

   CAUTION:

   FSI is not supported in clustered gateways in release 3.3. However, both FSI and are listed as choices on the installation menu. For clustered gateways, the only supported options are VTL ; do not choose FSI.

   If you are installing a clustered gateway, whichever option you choose for Server A now, you must choose the same option for server B later in this document.
7. Type the numeral corresponding to your choice and press Enter. A confirmation prompt like the following example displays.

```
About to execute:
Operation:    install
Model:        TS7650G
Application:  OST_10G

Continue? (yes|no)
```

8. Type yes to confirm your selection and press Enter. The system automatically starts the configuration process, with output similar to the following example.

   Note: These examples are for an configuration with FC 3457 (dual-port 10 Gb Ethernet adapters).

```
Stopping services, please wait
Stopping Cluster Services                                    [ Done ]
Services stopped
Checking Fence Device                                        [ Done ]
Checking BOM                                                 [ Done ]
Checking for existing nodes                                  [ Done ]
Checking Application Interfaces                              [ Done ]
Checking repository                                          [ Done ]
Checking installed applications                              [ Done ]
Checking local raid                                          [ Done ]
Checking conditions done
```

9. The installation process prompts you to enter IP addresses for primary and secondary NTP servers and information for external application interfaces, as shown in the following example output. When prompted for the IP addresses of the NTP primary and secondary servers, choose one of the following options:
   - If you do not want to use NTP servers, press Enter when prompted without entering IP addresses.
   - If you want to use NTP servers, enter the IP address for the primary and secondary NTP servers when prompted and press Enter after each.

     Note: NTP servers are required for use in FSI installations in which Active Directory is used when you set up file system authentication through the ProtecTIER Manager user interface. You can enter the IP addresses for the NTP servers now or later, but they must be entered before you set up file system authentication.

   The following paragraphs deal with the external application interface IP addresses to be entered.

   ProtecTIER exposes virtual interfaces to the host, such as a media server with the plug-in installed. In version 3.4.3, the physical Ethernet ports are assigned to one virtual application interface. Currently, the physical ports are assigned to virtual interface eth0 or eth1, depending on the server configuration. This assignment option is used to group several physical interfaces into a single virtual interface, and create a bond configuration of several physical interfaces. Each virtual interface used must be configured with a corresponding IP address.

   Attention: Each configured IP address on the same server needs to be on a different subnet, and each subnet needs to be on a different VLAN. If separate subnets and VLAN's are not used, in certain environments and networks, network packets can move to other subnets, which can harm network performance and potentially reduce the network's quality of service.

   In addition, each virtual interface containing more than one physical interface (configured as a bond) needs to be configured with a load balancing method. For a server with 10 Gb interfaces, where bonding is implemented, the recommended load balancing method is Link Aggregation Control Protocol (LACP) with L3L4.

   For more information about bonding, the different load balancing methods, and whether to configure bonds at all, refer to the *IBM ProtecTIER Implementation and Best Practices*, Redbooks publication SG24-8025, available at: http://www.redbooks.ibm.com/Redbooks.nsf/RedpieceAbstracts/sg248025.html?Open or the *IBM ProtecTIER Implementation and Best Practices*, Redbooks publication SG24-8025, available at: http://www.redbooks.ibm.com/Redbooks.nsf/RedpieceAbstracts/sg248025.html?Open.

```
Please provide the following information:
-----------------------------------------
NTP server timeserver, IP Address (optional):
NTP server secondary_timeserver, IP Address (optional):
ApplicationInterface external, IP Address [192.168.10.161]: 9.148.220.157
ApplicationInterface external, Netmask [255.255.255.0]: 255.255.252.0
ApplicationInterface external, Default Gateway [192.168.10.1]: 9.148.220.4
ApplicationInterface external, Hostname [node1]: popeye
```

10. When prompted to confirm your choices as shown in the following example, verify that they are correct, type y and press Enter.

```
Please check the following values:
---------------------------------
NTP server timeserver, IP Address:
NTP server secondary_timeserver, IP Address:

ApplicationInterface external, IP Address: 9.148.220.157
ApplicationInterface external, Netmask: 255.255.252.0
ApplicationInterface external, Default Gateway: 9.148.220.4
ApplicationInterface external, Hostname: popeye

Are you sure you want to submit these values? (yes|no|quit) y
```

If you did not configure RAS in "Configuring RAS" on page 29, you are prompted to configure the SMTP server as shown in the following example. If you configured the SMTP server earlier during RAS configuration, this output does not appear. If you did not configure the SMTP server earlier and want to do so now, use the information on the completed Company Information and IP address worksheets. See Appendix A, "Company information worksheet," on page 101 and Appendix B, "IP address worksheet," on page 105 for details about the information that you must enter.

```
Please provide the following information:
-----------------------------------------
Customer SMTP server IP address (optional):
Customer number:
     Input should be 7 alphanumeric: abcderf
Country code:
     Input should be 2 or 3 alphanumeric: av
Business company name, e.g. IBM, (optional):
Machine location, e.g. Server room, (optional):
MODEM Phone number, (optional):
Voice Phone number, (optional):

Please check the following values:
----------------------------------
Customer SMTP server IP address:
     The first administrator email-address:
     The second administrator email-address:
     The third administrator email-address:
Customer number: abcderf
Country code: av
Business company name:
Machine location:
MODEM Phone number:
Voice Phone number:
Are you sure you want to submit these RAS values? (yes|no|quit)
```

11. The configuration process continues, with output similar to the following example.

```
Configuring network                                          [ Done ]
Restarting Network Service                                   [ Done ]
Configuring Application Interfaces                           [ Done ]
Stopping cluster                                             [ Done ]
Configuring cluster                                          [ Done ]
Starting cluster                                             [ Done ]
Installing NTP                                               [ Done ]
Set interfaces addresses                                     [ Done ]
Starting VTFD                                                [ Done ]
Starting RAS                                                 [ Done ]
Collecting RAS Persistent configuration                      [ Done ]
Running RAS Eth Agent                                        [ Done ]
validation will start in 10 seconds
Testing customer network connectivity                        [ Done ]
Testing connectivity to the Default Gateway                  [ Done ]
Getting number of nodes                                      [ Done ]
This is a 1 node cluster, will not test fencing
validation ended
install ended successfully

End Processing Procedure Successfully

Press <ENTER> to continue
```

12. Press the Enter key to return to the **ProtecTIER Configuration** menu.
13. Go to "Defining the date and time."

Defining the date and time

In a clustered configuration, if both servers are running, run these procedures from only one of the servers. The change takes effect on both nodes.

About this task

Choose one of the following sequences of procedures:

- If you are not using an NTP server, do the procedures in the following sections in order.
  1. "Setting the timezone" on page 48
  2. "Setting the date and time" on page 54
- If you are using an NTP server and configured it in Chapter 5, "Configuring Server A," on page 39, do the procedure in "Setting the timezone" on page 48 only.
- If you are using an NTP server and did not configure it in Chapter 5, "Configuring Server A," on page 39, do the procedures in the following sections in order.
  1. "Setting the timezone" on page 48
  2. "Defining NTP servers" on page 51

Setting the timezone

About this task

Important: With Version 3.3.6 and later, you must apply each change you make to the timezone, date and time, and time server individually before proceeding to the next task.

Procedure

1. At the command line, type: `menu` and press Enter. The **ProtecTIER Service** menu appears:

```
--------------------------------------------------------------------------
  ProtecTIER Service Menu running on rasddx
--------------------------------------------------------------------------
   1) ProtecTIER Configuration (...)
   2) Manage ProtecTIER services (...)
   3) Health Monitoring (...)
   4) Problem Alerting (...)
   5) Version Information (...)
   6) Generate a service report
   7) Generate a system view
   8) Update ProtecTIER code

   E) Exit
--------------------------------------------------------------------------
>>> Your choice?
```

2. Type the numeral corresponding to `ProtecTIER Configuration` and press Enter. The **ProtecTIER Configuration** menu displays.

```
--------------------------------------------------------------------------
  ProtecTIER Service Menu running on rasddx
  ProtecTIER Configuration (...)
--------------------------------------------------------------------------
   1) Configure ProtecTIER node
   2) Recover Configuration for a replaced server
   3) Configure machine serial number for a replaced server
   4) Configure RAS
   5) Update Time, Date, Timezone & Timeserver(s)
   6) Scan storage interconnections
   7) File Systems Management (...)
   8) Configure replication (...)
   9) IP Network configuration (...)
   10) Update Firmware
   11) Update the System's name
   12) Validate configuration
   13) Single node - code upgrade (for Support Use Only)

   B) Back
   E) Exit
--------------------------------------------------------------------------
>>> Your choice?
```

3. Type the numeral corresponding to `Update Time, Date, Timezone & Timeserver(s)` and press Enter. The system displays the **Date, Time, Timezone & Timeserver(s) configuration** menu:

```
Date, Time, Timezone & Timeserver(s) configuration
==================================================
1. Set date & time
2. Set Timezone
3. Set Timeserver(s)

c. Commit changes and exit
q. Exit without committing changes

Please Choose:
```

4. To synchronize the local timezone, type the numeral corresponding to `Set Timezone` and press Enter. The system displays the following prompt:

```
Please Choose:2
Enter a 2 letter country code (or type 'm' to enter the timezone manually):
```

5. If you know the two-letter country code for the timezone, type it and press Enter, or type `m` to enter the full name of the timezone. The system displays all of the timezones within the country you chose. For example, if you typed `US`, the system displays the **Time zones under US** menu.

```
Time zones under US:
====================
1. America/New_York
2. America/Detroit
3. America/Kentucky/Louisville
4. America/Kentucky/Monticello
5. America/Indiana/Indianapolis
6. America/Indiana/Vincennes
7. America/Indiana/Knox
8. America/Indiana/Winamac
9. America/Indiana/Marengo
10. America/Indiana/Vevay
11. America/Chicago
12. America/Indiana/Tell_City
13. America/Indiana/Petersburg
14. America/Menominee
15. America/North_Dakota/Center
16. America/North_Dakota/New_Salem
17. America/Denver
18. America/Boise
19. America/Shiprock
20. America/Phoenix
21. America/Los_Angeles
22. America/Anchorage
23. America/Juneau
24. America/Yakutat
25. America/Nome
26. America/Adak
27. Pacific/Honolulu

Please choose a timezone:
```

Note: If you typed `m` to enter the full name of the timezone, enter the name of the timezone (for example `Italy`) at the prompt. The following message is displayed:

```
Enter the time zone (case sensitive):
```

Refer to Using the GUI to check the ProtecTIER version for a list of timezone codes for countries other than the United States.

6. Type the numeral corresponding to the timezone you want to synchronize (from the Appendix D, "Worldwide time zone codes," on page 117) under the country code entered. The system displays the **Date, Time, Timezone & Timeserver(s) configuration** menu.

   Note: If you typed in new information, an asterisk (*) is visible at the end of the `c. Commit changes and exit` option to show that there are modifications to be saved.

```
Date, Time, Timezone & Timeserver(s) configuration
==================================================
1. Set date & time
2. Set Timezone
3. Set Timeserver(s)

c. Commit changes and exit *
q. Exit without commiting changes

Please Choose:
```

7. Type the numeral corresponding to `Commit changes and exit *` and press Enter to save the changes and exit. A list of the configuration changes is displayed for review, and the system prompts for your confirmation of the changes.
8. Type `y` and press Enter to apply the new time zone setting.
9. Perform one of the following choices.
   - If you are not using an NTP server, go to "Setting the date and time" on page 54.
   - If you are using an NTP server and already configured it in Chapter 5, "Configuring Server A," on page 39, do the following steps:
     a. Replace any cables that you removed in step Chapter 5, "Configuring Server A," on page 39.
     b. Go to Chapter 6, "Installing ProtecTIER Manager on workstations," on page 55.
   - If you are using an NTP server and it is not yet configured, go to "Defining the date and time" on page 47.

Defining NTP servers

About this task

This procedure applies only if you have NTP servers.

Important: With Version 3.3.6 and later, you must apply each change you make to the timezone, date and time, and time server individually before proceeding to the next task.

Procedure

1. From the prompt on the **Date, Time, Timezone & Timeserver(s) configuration** menu, type the numeral that corresponds to the `Set Timeserver(s)` option and press Enter to add a time server to the system. The system displays the following prompt:

```
Please specify the timeserver's IP Address:
```

2. Enter the IP address of the NTP server. (For example, type *`192.168.10.15`* and press Enter.) The system displays the following prompt:

```
Would you like to set a secondary timeserver? (yes|no)
```

3. Type `y` and press Enter to set a secondary NTP server. The system displays the following prompt:

```
Please specify the secondary timeserver's IP Address:
```

4. Enter the IP address of the secondary NTP server. For example, type *192.168.12.15* and press Enter. The system displays the **Date, Time, Timezone & Timeserver(s) configuration** menu.
5. Type the character corresponding to `Commit changes and exit *` and press Enter. A list of the configuration changes is displayed for review, and the system prompts for your confirmation of the changes.
6. Type `y` to save and apply the changes. The system displays the following prompt:

```
Note: the cluster & VTFD services on all nodes must be stopped in order to continue.
Do you wish to continue? (yes|no)
```

7. Type y to stop and restart the cluster and VTFD services on all the nodes.

```
Stopping Cluster Services                          [ Done ]
Stopping NTPD                                      [ Done ]
Setting Time Zone                                  [ Done ]
Setting Timeserver                                 [ Done ]
Setting Date & Time                                [ Done ]
Starting NTPD                                      [ Done ]
Starting cluster                                   [ Done ]
Cluster Started
```

8. Replace any cables that you removed in step Chapter 5, "Configuring Server A," on page 39.
9. Go to Chapter 6, "Installing ProtecTIER Manager on workstations," on page 55.

Setting the date and time

About this task

Important: With Version 3.3.6 and later, you must apply each change you make to the timezone, date and time, and time server individually before proceeding to the next task.

Procedure

1. From the prompt on the **Date, Time, Timezone & Timeserver(s) configuration** menu, type the numeral that corresponds to the `Set date & time` option and press Enter. The system displays the following prompt:

```
Please Choose:1
Please specify the date in DD/MM/YYYY format [09/11/2009]:
```

2. Type the date in the specified format and press Enter. The system now prompts you to specify the time:

```
Please specify the date in DD/MM/YYYY format [07/03/2011]: DD/MM/YYYY
Please specify the time in HH:MM:SS format [11:56:16]:
```

3. Type the time in the specified format and press Enter. The system returns to the **Date, Time, Timezone & Timeserver(s) configuration** menu:

```
Date, Time, Timezone & Timeserver(s) configuration
================================================
1. Set date & time
2. Set Timezone
3. Set Timeserver(s)

c. Commit changes and exit *
q. Exit without committing changes

Please Choose:
```

4. Type the character corresponding to `Commit changes and exit *` and press Enter. A list of the configuration changes is displayed for review, and the system prompts for your confirmation of the changes.
5. Replace any cables that you removed in step Chapter 5, “Configuring Server A,” on page 39.

   Configuration of Server A is complete. If you are installing a clustered configuration, you must now install ProtecTIER Manager and create a repository on Server A before you configure Server B.
6. Go to Chapter 6, “Installing ProtecTIER Manager on workstations,” on page 55.

Chapter 6. Installing ProtecTIER Manager on workstations

Prerequisites for the ProtecTIER Manager workstation

The ProtecTIER Manager workstation must meet the prerequisites to install and effectively run ProtecTIER Manager:

- One of the following operating systems must be installed. See the *IBM TS7650 ProtecTIER Software Upgrade Guide, SC27-3643* for further information.)
  - Windows 32 or 64 bit (XP Professional, 2003, Windows 7, Windows 10)
  - Linux Red Hat 32 or 64 bit
- At least 1.2 GB of available disk space
- At least 256 MB of RAM
- The workstation can access the ProtecTIER service nodes IP addresses (ports 3501 and 3503 are open on the firewall).

Display requirements for viewing the ProtecTIER Manager:

- Optimum resolution: 1280 × 1024 pixels
- Minimum supported resolution: 1024 × 768 pixels
- 24-bit color or higher

Note: If you plan to run ProtecTIER Manager on a *UNIX* system, configure your graphics card and X Window System. This configuration is done either manually or with the **`Xconfigurator`** utility. For instructions, see the appropriate Linux documentation.

Installing ProtecTIER Manager on a Windows workstation

Procedure

1. Set the resolution of the workstation to 1280 × 1024, which is the optimal resolution for viewing the ProtecTIER Manager GUI.
2. Insert the CD that contains the ProtecTIER Manager software into the CD drive of the designated ProtecTIER Manager workstation. If the ProtecTIER Manager installation function starts and starts the installation, go to step 3. If the ProtecTIER Manager installation function does not start automatically, manually start and run the function:
   a. On the Windows task bar, click **Start** > **Run**. The Run window opens.
   b. In the **Open** field, type <*the letter of the CD drive of the server*> followed by **:** and click **Ok**. The contents of the CD display.
   c. From the list of files, locate the ProtecTIER Manager for Windows installation file `install.exe` and double-click the file to start the installation.
3. Read the contents of the **Introduction** window, and click **Next**. Two License Agreement windows open sequentially.

4. Read and accept the terms of each license agreement, and click **Next**. The Choose Install Folder window opens (Figure 22).

Figure 22. Choose Install Folder window

5. Specify the folder where the ProtecTIER Manager program files are to be installed, and click **Next**. The Choose Shortcut Folder window opens (Figure 23).

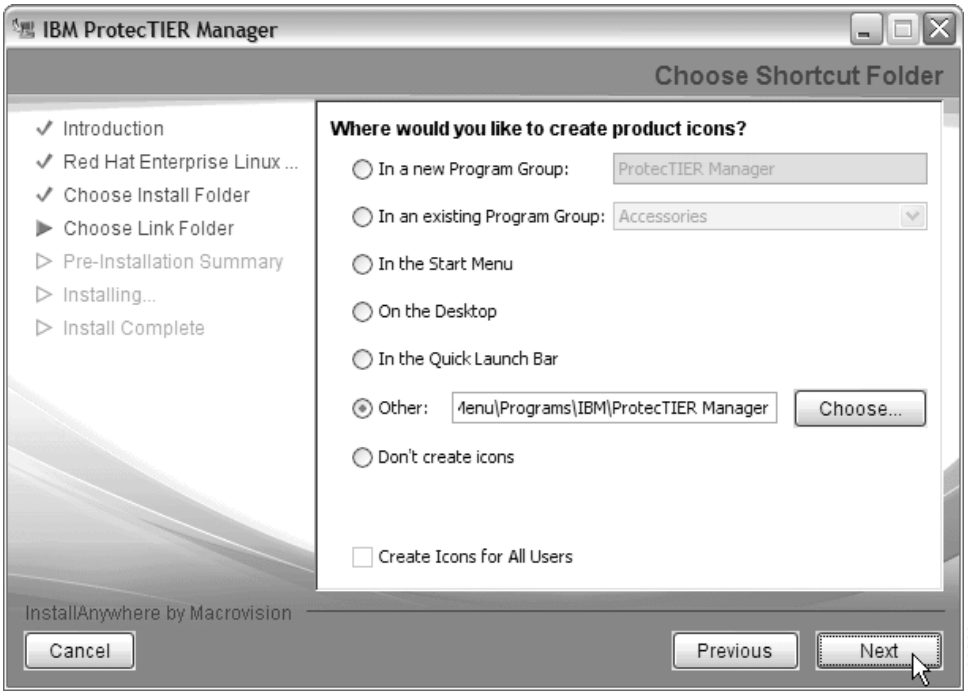


Figure 23. Choose Shortcut Folder window

6. Select the location where the program icons are to be created.

Option	Description
In a new Program Group	Creates a program group in the Program list of the **Start** menu.
In an existing Program Group	Creates a program group in the Program list of the **Start** menu.
In the Start Menu	
On the Desktop	
In the Quick Launch Bar	
Other	Opens a field into which you can enter a path location for the shortcut, or to browse for a location by clicking **Choose**.
Don't create icons	No shortcuts are created.
Create Icons for All Users	When appropriate, select this check box to create a shortcut in the defined location for all user accounts on the workstation.

7. Click **Next**. The Pre-Installation Summary window opens.
8. Review the Pre-Installation Summary window and then click **Install** to start the installation. The Installing ProtecTIER Manager window opens. When the installation is complete and ProtecTIER Manager is successfully installed, the Install Complete window opens.
9. Click **Done**. The ProtecTIER Manager Installation wizard closes and the installation process is complete.

Installing ProtecTIER Manager on a Linux workstation

Before you begin

The installation procedure assumes that the workstation on which ProtecTIER Manager is being installed has a Linux GUI. A GUI is required for ProtecTIER Manager operation on Linux.

Procedure

1. Insert the CD that contains the ProtecTIER Manager Enterprise Edition software into the CD drive of the designated ProtecTIER Manager workstation.
2. Run the ProtecTIER Manager installer:
   a. On the Linux desktop, double-click the **CD icon**. Double-click the installation folder for the version of Linux you have (Linux for version 64 or Linux32 for version 32).
   b. From the installation folder, select the `InstallLinuxXX.bin` file (where *XX* is either 64 or 32) and drag the file onto the desktop.
   c. Close any open windows.
   d. Right-click any open area of the desktop. From the menu that opens, click **Open Terminal**. The Terminal window opens.
   e. Change to the `Desktop` directory. At the command prompt, type `cd Desktop` and press Enter. (The command is case-sensitive. Type the word *"Desktop"* with an uppercase *"D"*.)
   f. From the desktop directory, run the ProtecTIER Manager installer. Type:

```
./InstallLinuxXX.bin
```

and press Enter. If the message: `Permission Denied` appears, type:

`chmod +x InstallLinuxXX.bin` and press Enter *(where "XX" is XX is 64 or 32)*.

`./InstallLinuxXX.bin` and press Enter *(where "XX" is XX is 64 or 32)*.

3. At the ProtecTIER Manager wizard Introduction window, click **Next**. Two separate Software License Agreement screens appear.
4. Read the terms for each license agreement, indicate your acceptance, and then click **Next**. The Choose Install Folder window appearss.
5. Specify the location to install the ProtecTIER Manager program files:
   - Enter the path to the location where the ProtecTIER Manager program files are to be installed.

     Click **Choose** to browse for a location, or

     Click **Restore Default Folder** to revert to the default installation path.
6. Click **Next**.
7. Select the location where the program links are to be created:

Option	Description
In your Home folder	Creates the links in the directory where the user files are typically stored. For example, `/home/bill`.
Other	Creates the links in the default location (`/opt/IBM/PTManager`). To specify a different location, click **Choose** and select a directory.
Don't create links	No links are created.

8. Click **Next**. The Pre-Installation Summary window displays.
9. Click **Install**. The Installing ProtecTIER Manager window displays and ProtecTIER Manager is installed. When the installation finishes, the Install Complete window displays.
10. Click **Done** to close the ProtecTIER Manager wizard, and return to the command prompt.
11. Close the window by typing `Exit` and pressing Enter.

Chapter 7. Creating repositories

Each ProtecTIER installation has one repository on which data is stored. In clustered installations, a repository for common use is a prerequisite for adding a second cluster member. Use the ProtecTIER Manager software for repository management tasks:

- Planning the repository (see "Planning the repository")
- Creating file systems (see "Creating file systems" on page 62)
- Creating the repository (see "Creating the repository" on page 65)

For the procedures for common tasks within ProtecTIER Manager, see Appendix E, "ProtecTIER Manager common tasks," on page 129.

Planning the repository

Procedure

1. On the ProtecTIER Manager workstation, start ProtecTIER Manager.
2. Click **Repository > Create repository planning**. The "Create repository planning" wizard opens. See Figure 24.

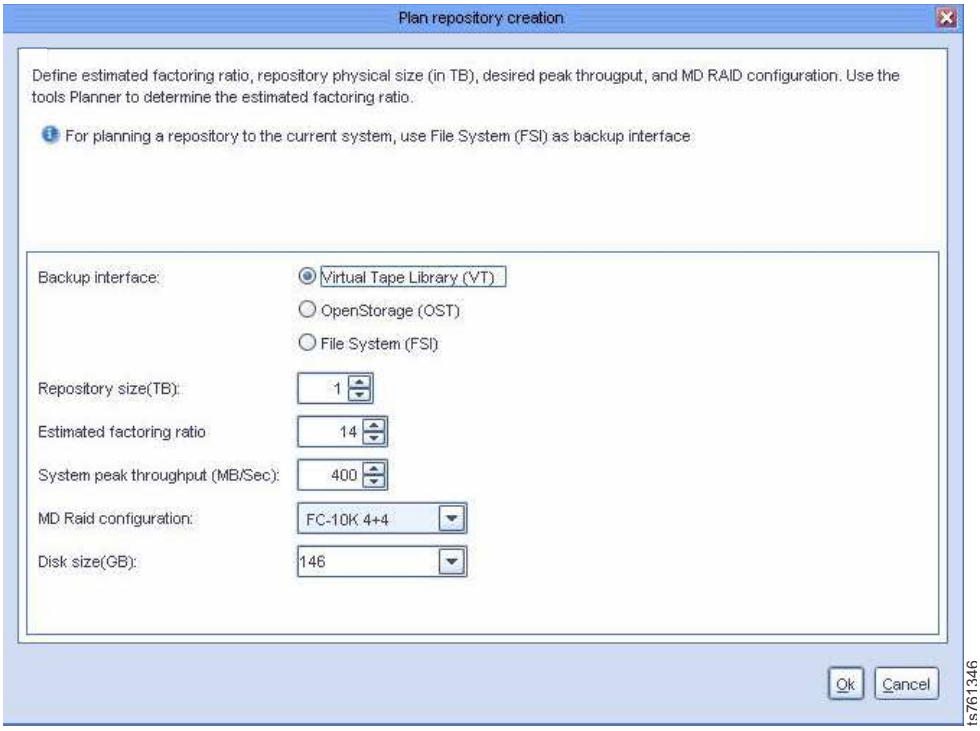


Figure 24. "Create repository planning" wizard

3. In the **Backup interface** area, click the radio button for your installation:
   - **Virtual Tape Library (VT)**
4. In the **Repository size** field, enter the value in terabytes of the size of the repository that you want to create.

Note: The maximum repository physical size is one petabyte (1 PB).

5. In the **Estimated factoring ratio** field, enter the value that was estimated for the customer environment. The estimate is based on the data change rate, backup policies, and retention period.
6. In the **System peak throughput** field, enter the rate of system peak throughput in megabytes per second that the metadata file systems can support.
7. From the **MD Raid configuration** list, select the RAID configuration of the logical volumes on which the repository metadata file systems are to be created. For example, select **FC-10K 4+4** for a configuration of RAID 10 4+4 with Fibre Channel 10 K RPM (revolutions per minute) disks.
8. In the **Disk size** field, enter the value in gigabytes of the size of the physical disk of the server where you want to create the repository.
9. Click **Ok**. The "Repository metadata storage requirements" window displays a list of file system arrangement options. See Figure 25.

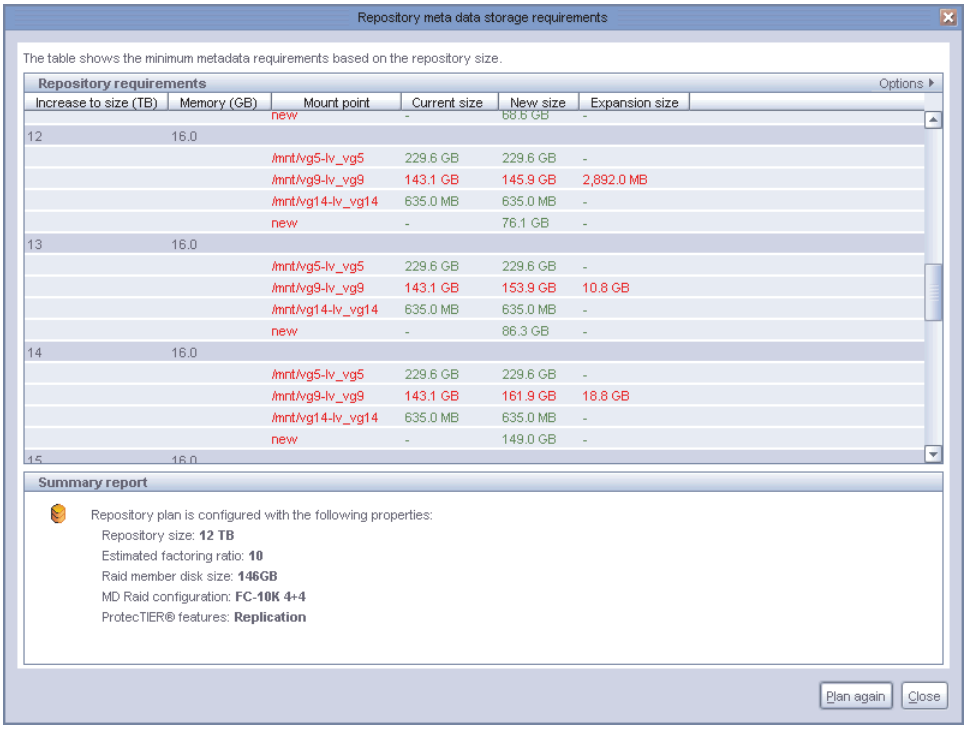


Figure 25. "Repository metadata storage requirements" window

10. To print the information in the "Repository metadata storage requirements" window, or to save the information as a `.csv` file, click **Options**.
11. Click **Ok**. The "Repository metadata storage requirements" window closes.

    Choose the metadata file system arrangement that most closely matches the arrangement of your disk array. Base your choice on the information that is shown in the "Repository metadata storage requirements" window.

Creating file systems

About this task

You need to create file systems during initial installation.

Creating file systems through the File Systems Management menu

About this task

You can create file systems for the repository through the ProtecTIER File Systems Management menu. When you select an option, an interactive dialog starts. Select components and values and confirm your final choices through the dialog.

Procedure

1. Log in to Server A. See steps 2 on page 42 through 3 on page 43 of Chapter 5, "Configuring Server A," on page 39 for the login procedure.
2. At the command line, type `menu` and then press Enter. The ProtecTIER Service menu displays.

```
------------------------------------------------------------------------
  ProtecTIER Service Menu running on rasddx
------------------------------------------------------------------------
   1) ProtecTIER Configuration (...)
   2) Manage ProtecTIER services (...)
   3) Health Monitoring (...)
   4) Problem Alerting (...)
   5) Version Information (...)
   6) Generate a service report
   7) Generate a system view
   8) Update ProtecTIER code

   E) Exit
------------------------------------------------------------------------
>>> Your choice?
```

3. Type the numeral corresponding to `ProtecTIER Configuration` and press Enter. The ProtecTIER Configuration menu displays.

```
------------------------------------------------------------------------
  ProtecTIER Service Menu running on rasddx
  ProtecTIER Configuration (...)
------------------------------------------------------------------------
   1) Configure ProtecTIER node
   2) Recover Configuration for a replaced server
   3) Configure machine serial number for a replaced server
   4) Configure RAS
   5) Update Time, Date, Timezone & Timeserver(s)
   6) Scan storage interconnections
   7) File Systems Management (...)
   8) Configure replication (...)
   9) IP Network configuration (...)
   10) Update Firmware
   11) Update the System's name
   12) Validate configuration
   13) Single node - code upgrade (for Support Use Only)

   B) Back
   E) Exit
------------------------------------------------------------------------
>>> Your choice?
```

4. Type the numeral corresponding to `File Systems Management` and press Enter. The File Systems Management menu displays.

```
------------------------------------------------------------------------
 ProtecTIER Service Menu running on rasddx
 ProtecTIER Configuration (...)
 File Systems Management (...)
------------------------------------------------------------------------
  1) Configure file systems on all available devices
  2) Create file system(s) on a single unused device
  3) Extend a file system with a new unused device
  4) Update /etc/fstab
  5) Display configured devices
  6) Display unused devices
  7) Display GFS repository file systems
  8) Display unused GFS file systems
  9) Increase capacity completion (applicable for a second cluster node)

  B) Back
  E) Exit
------------------------------------------------------------------------
>>> Your choice?
```

5. Create the file systems for the repository by typing the numeral corresponding to `Configure file systems on all available devices` and pressing Enter. You must confirm your choice to continue. An example follows.

```
Device:         Size:           Status
mpath0          2048.00M        Unused
mpath1          2285200.00M     Unused
mpath2          2287248.00M     Unused
mpath3          2287248.00M     Unused

Please confirm:? (yes|no)
```

Creating the repository

After the necessary file systems are created, use the information that was generated during the repository planning process to create the repository.

About this task

A repository can be created only on a one-node cluster (creating a repository is a prerequisite for adding a second node to a cluster). You must create the repository on Server A before Server B is added to a cluster.

Procedure

1. On the ProtecTIER Manager workstation, if it is not already running, start ProtecTIER Manager.
2. In the **Nodes** panel, select the node on which to create the repository.
3. Click **Create new repository**. The "Create repository" wizard starts the data collection process. When data collection is complete, the Welcome window opens.
4. Read the information that is presented in the Welcome window, then click **Next**. The Create Repository Name window opens. See Figure 26.

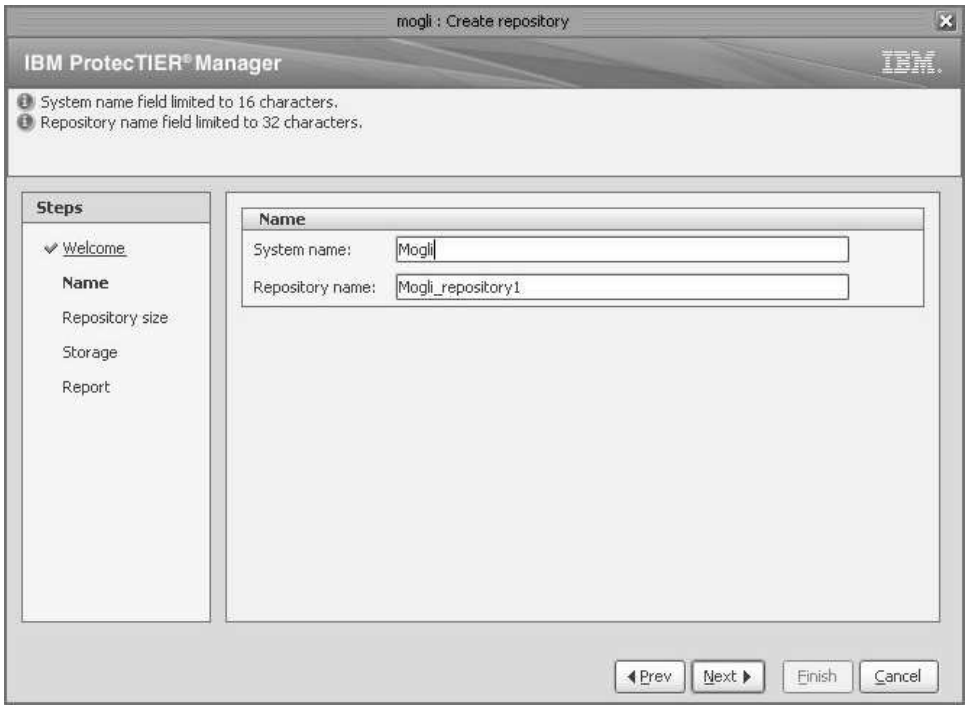


Figure 26. Create Repository Name window

5. In the Create Repository Name window, provide the following information:
   a. In the **System name** field, enter the name of the server on which the repository is being created.
   b. In the **Repository name** field, enter the name of the repository that you are creating.

6. Click **Next**. The “Repository size” window opens. See Figure 27.

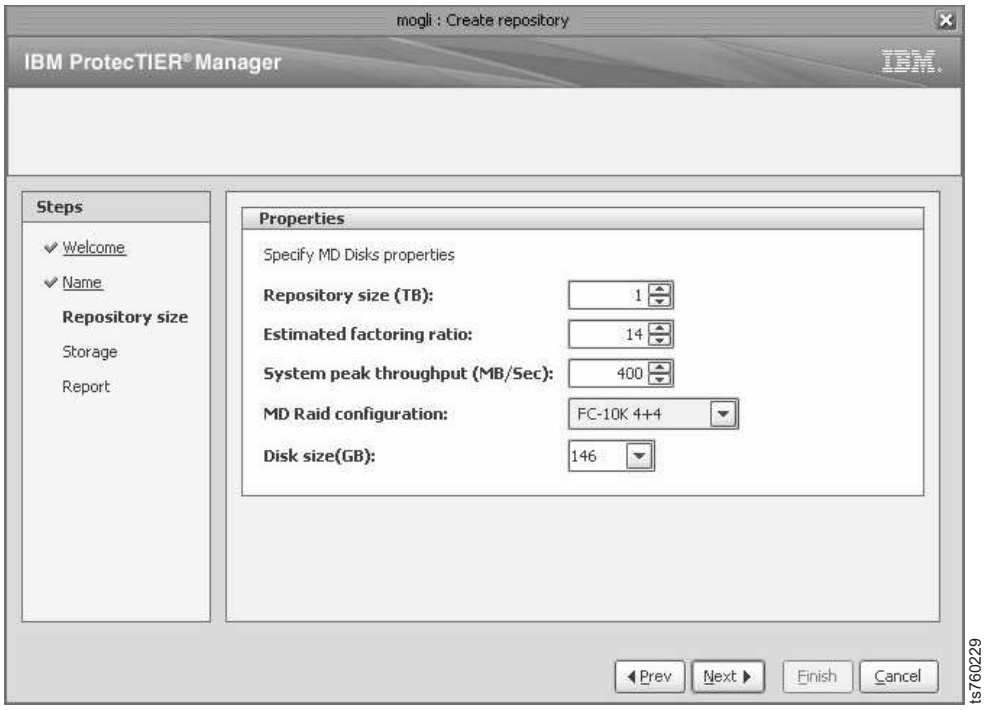


Figure 27. "Repository size" window

7. In the “Repository size” window, provide the following information:
   a. In the **Repository size (TB)** field, enter the repository size (in terabytes) that you determined with the “Create repository” wizard.
   b. In the **Estimated factoring ratio** field, enter the estimated factoring ratio value that was determined with the assistance of support personnel.
   c. In the **System peak throughput (MB/Sec)** field, enter the rate of system peak throughput that the metadata file systems can support.
   d. From the **MD Raid configuration** list, select the RAID configuration of the logical volumes on which the repository metadata file systems are to be created. For example, select **FC-10K 4+4** for a configuration of RAID 10 4+4 with Fibre Channel 10K RPM disks.
   e. From the **Disk Size (GB)** list, select the disk size that is used in the RAID array for metadata. If an exact match is not available, select the closest smaller value.

8. Click **Next**. The Storage window opens. See Figure 28.

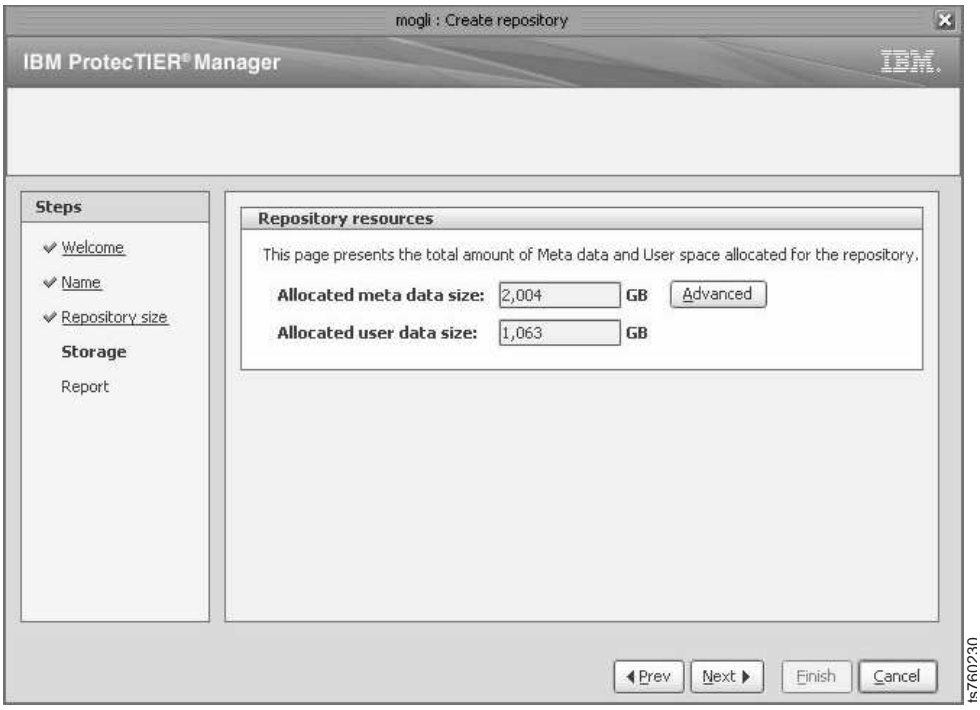


Figure 28. Storage window

In the Storage window, the **Allocated meta data size** field displays the amount of disk space in gigabytes that is allocated for metadata. The **Allocated user data size** field displays the amount of disk space in gigabytes allocated for user data. This allocation is based on the estimated factoring ratio and the set of existing file systems.

9. Click **Next**. The “Repository resources” window opens. See Figure 29.

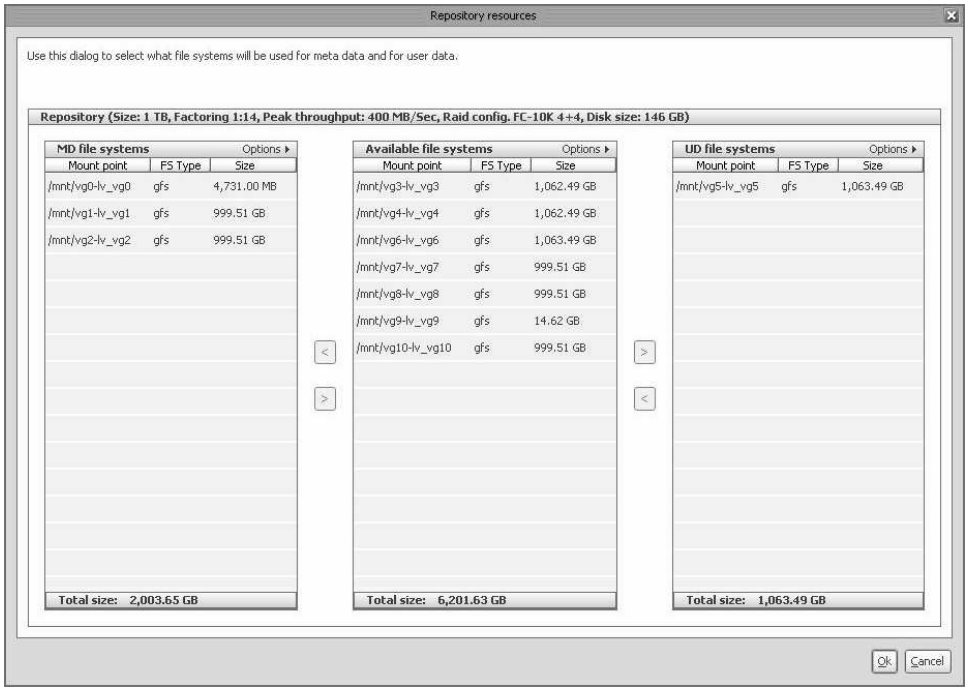


Figure 29. "Repository resources" window

10. Verify that the correct file systems are selected for metadata and user data. Consult the metadata file system sizes that are indicated in the repository planning process.

    Note: By default, the ProtecTIER system generally selects the smallest available file systems for use as metadata file systems. The remaining file systems are available for user data. Storage space for user data cannot exceed the repository size that is defined in the Repository Size window.
11. If the file systems that are selected by ProtecTIER for metadata and user data do not match the file systems that were created for those purposes, change the assignment. To do so:
    a. In the “Repository resources” window, from the **Available file systems** list, select **File Systems**.
    b. Click the left and right arrows to move file systems to and from the **MD file systems** (metadata) and **UD file systems** (user data) lists.
12. When the assignments are correct, click **Ok**. The Report window opens.
13. Review the summary report information and then click **Finish**. The “Create repository” wizard closes and the ProtecTIER system temporarily goes offline to create the repository. This process might take several hours to complete, depending upon the size of the repository.
14. Click **Next** and then click **Finish**.
15. Choose one of the following options:
    - If you are installing a stand-alone installation, go to Chapter 10, “Applying updates and fixes to the ProtecTIER software for version 3.4.3 and higher,” on page 89.
    - If you are installing a clustered installation, go to Chapter 8, “Configuring Server B,” on page 69.

Chapter 8. Configuring Server B

Before you begin

Note: If you are working with new servers (directly from the factory), the most current versions of Red Hat Linux and ProtecTIER software are preinstalled.

If you are not working with new servers (direct from the factory), you must install the most current versions of Red Hat Linux and ProtecTIER software code before you configure ProtecTIER on Server B.

Attention: If you are working with a clustered configuration, before you configure Server B, you must first:

- Configure Server A (Chapter 5, "Configuring Server A," on page 39)
- Install ProtecTIER Manager (Chapter 6, "Installing ProtecTIER Manager on workstations," on page 55)
- Create a repository and file systems on Server A (Chapter 7, "Creating repositories," on page 61)

Procedure

1. IP address conflicts in installations with multiple servers can cause configuration failure. To prevent IP address conflicts, disconnect any cables from replication (VTL) and customer host network Ethernet (FSI only) ports. Choose one of the following options, depending upon your installation.

   Option 1: VTL

   Remove replication cables from Server B ports that are labeled **26** and **27** in Figure 30.

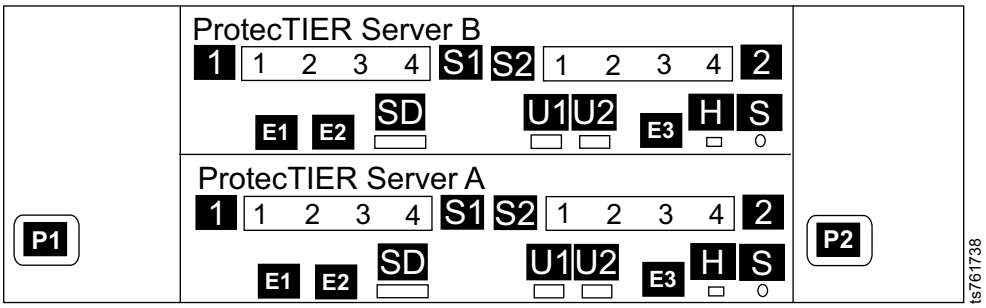


Figure 30. Server B replication ports for VTL configuration

Option 2: 1 Gb OpenStorage (FC 3456)

a. Remove replication cables from Server B ports that are labeled **17** and **18** in Figure 31.

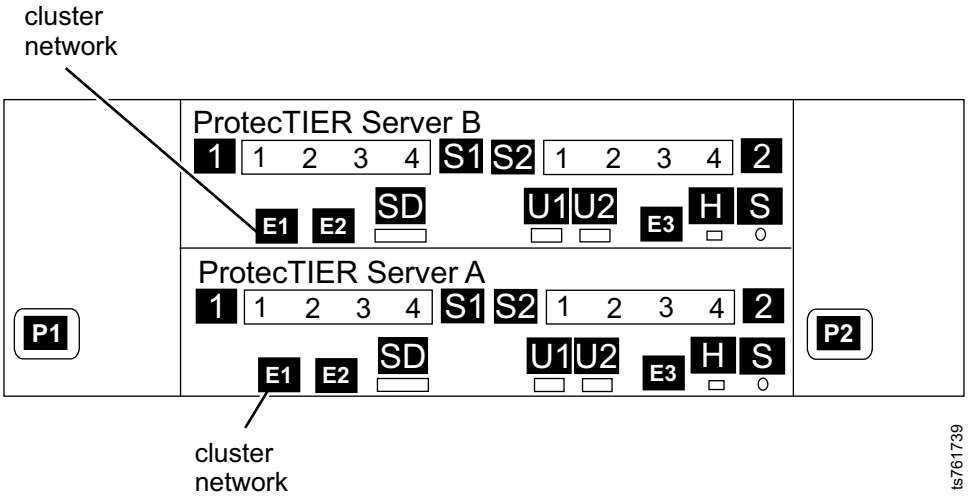


Figure 31. Server B replication ports for OpenStorage configuration, FC 3456

b. Remove customer host network Ethernet cables from Server B ports that are labeled **7 - 12**, **15**, and **16** in Figure 32. Not all of these connections might exist, depending upon the customer.

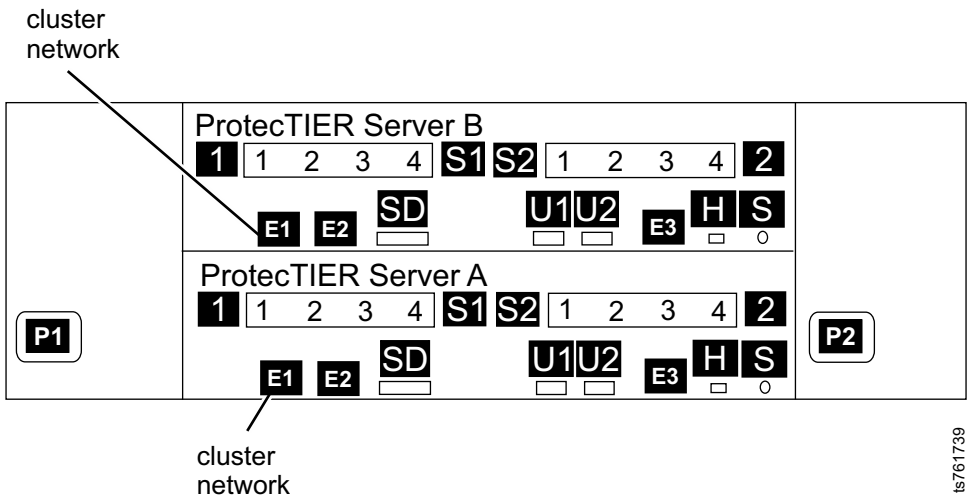


Figure 32. Server B customer host network Ethernet ports for 1 Gb OpenStorage configuration, FC 3456

Option 3: 10 Gb OpenStorage (FC 3457)

a. Remove replication cables from Server B ports that are labeled **17** and **18**.

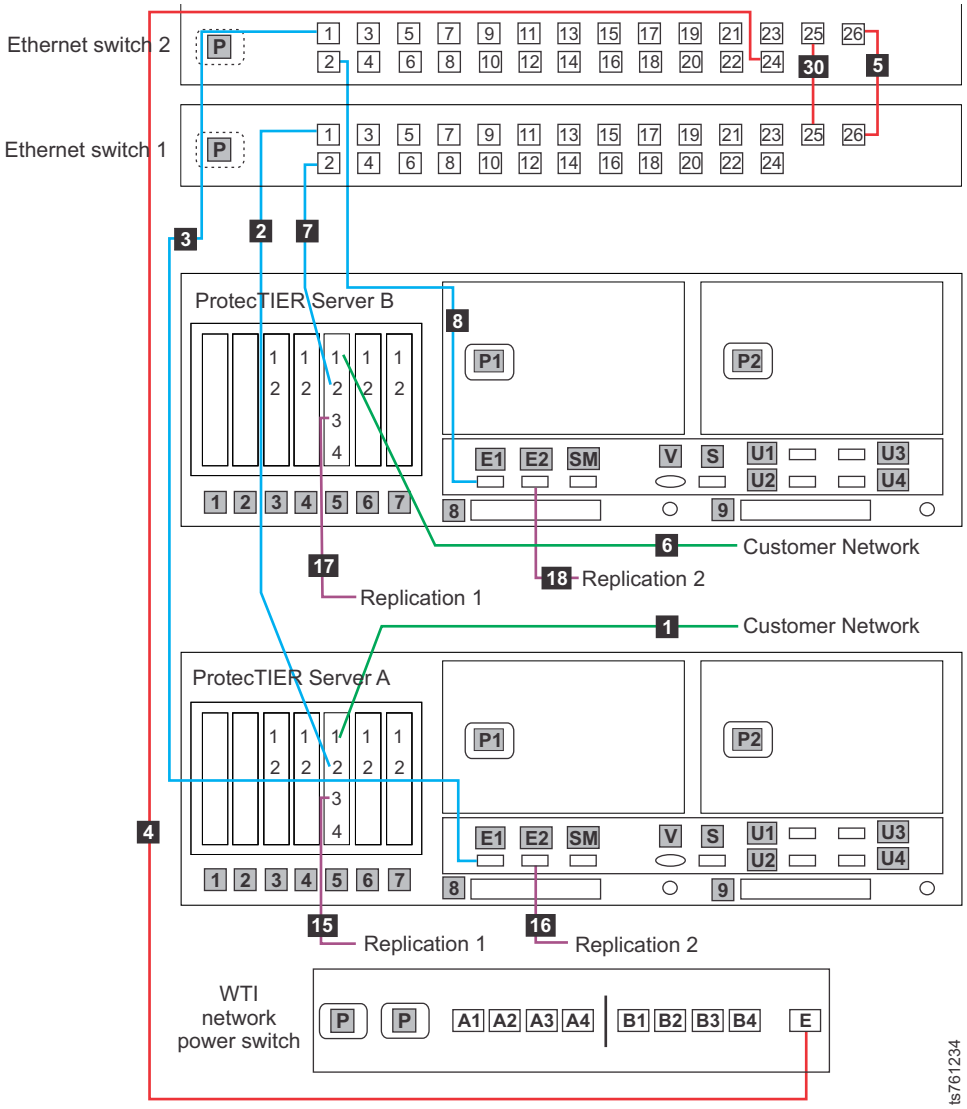


Figure 33. Server B replication ports for OpenStorage configuration, FC 3457

b. Remove customer host network Ethernet cables from Server B ports that are labeled **5 - 8** in Figure 34. Not all of these connections might exist, depending upon the customer.

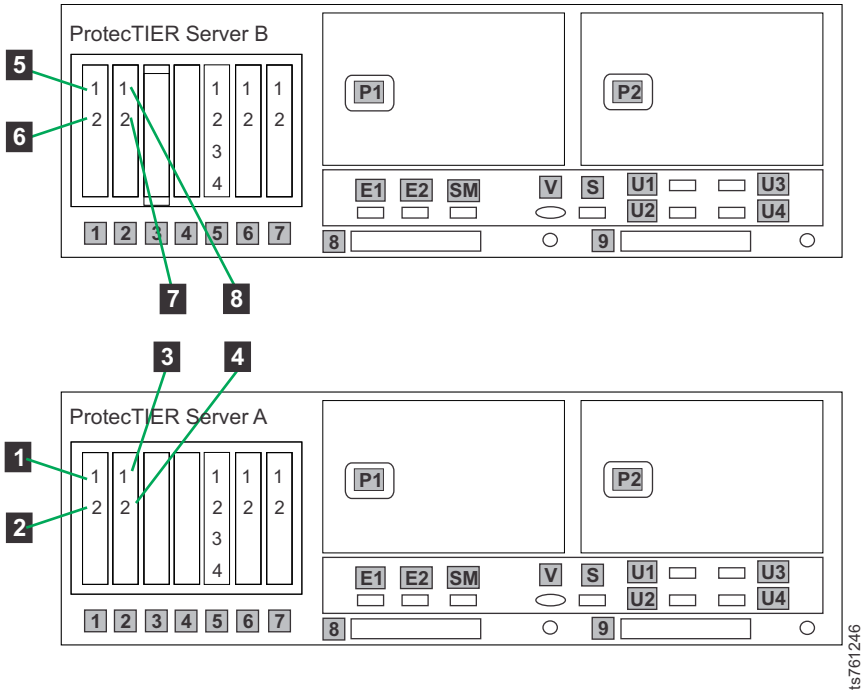


Figure 34. Server B customer host network Ethernet ports for 10 Gb OpenStorage configuration, FC 3457

2. Cycle power to the two 1-Gb Ethernet switches. This action helps ensure that Server B detects the switches during the configuration process.
   a. Remove power cables **1** and **2** from the AC power sockets on the rear of the switches. See Figure 35 on page 75 (for a single cluster) or Figure 36 on page 76 and Figure 37 on page 77 (for a dual cluster), whichever is applicable to your installation.

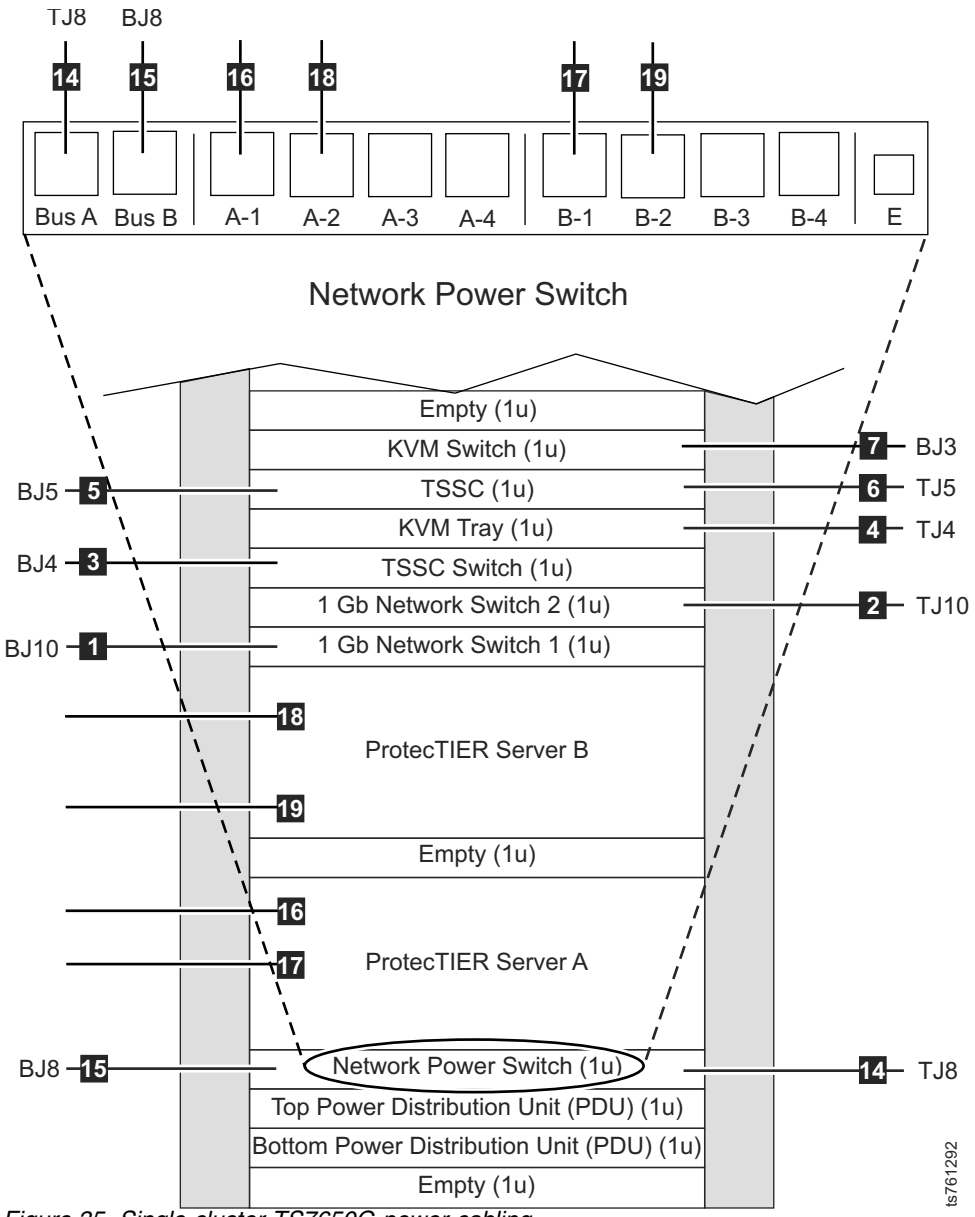


Figure 35. Single cluster TS7650G power cabling

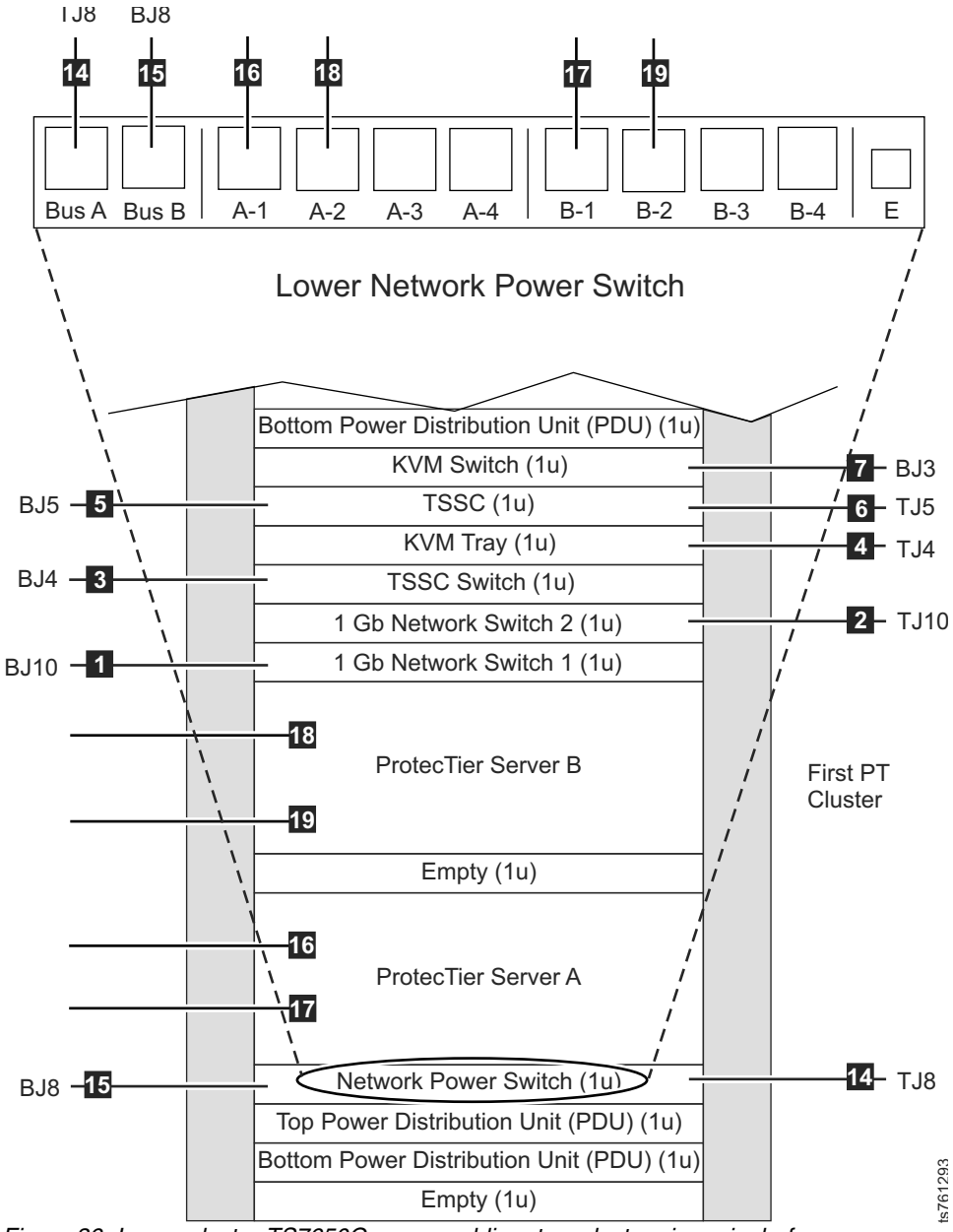


Figure 36. Lower cluster TS7650G power cabling, two clusters in a single frame

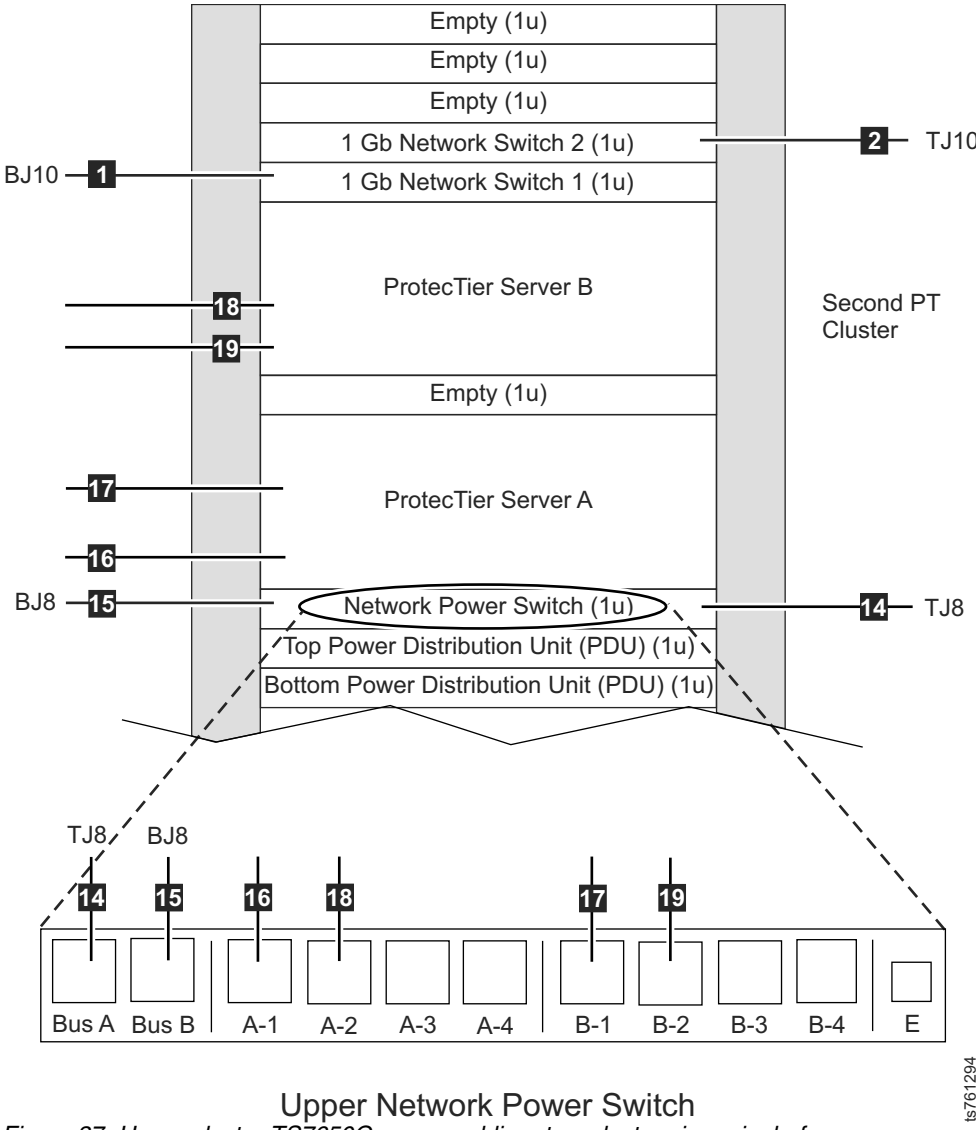


Figure 37. Upper cluster TS7650G power cabling, two clusters in a single frame

b. Wait 10 seconds.

c. Restore power to the 1 Gb Ethernet switches by replacing power cables **1** and **2** in the AC power sockets on the rear of the switches.

3. Power up Server B if it is not already powered up.

4. Log in to Server B with the user name `ptadmin` and password `ptadmin`.

5. At the command line, type **menu** and press Enter. The **ProtecTIER Service** menu displays.

```
--------------------------------------------------------------------------
  ProtecTIER Service Menu running on rasddx
--------------------------------------------------------------------------
   1) ProtecTIER Configuration (...)
   2) Manage ProtecTIER services (...)
   3) Health Monitoring (...)
   4) Problem Alerting (...)
   5) Version Information (...)
   6) Generate a service report
   7) Generate a system view
   8) Update ProtecTIER code

   E) Exit
--------------------------------------------------------------------------
>>> Your choice?
```

6. Type the numeral corresponding to ProtecTIER Configuration and press Enter. The **ProtecTIER Configuration** menu displays.

```
--------------------------------------------------------------------------
  ProtecTIER Service Menu running on rasddx
  ProtecTIER Configuration (...)
--------------------------------------------------------------------------
   1) Configure ProtecTIER node
   2) Recover Configuration for a replaced server
   3) Configure machine serial number for a replaced server
   4) Configure RAS
   5) Update Time, Date, Timezone & Timeserver(s)
   6) Scan storage interconnections
   7) File Systems Management (...)
   8) Configure replication (...)
   9) IP Network configuration (...)
   10) Update Firmware
   11) Update the System's name
   12) Validate configuration
   13) Single node - code upgrade (for Support Use Only)

   B) Back
   E) Exit
--------------------------------------------------------------------------
>>> Your choice?
```

7. Type the numeral corresponding to Configure ProtecTIER node and press Enter.

8. The system checks your hardware and presents one of two selection screens.
   Example (VTL)

```
1. VTL
```

   VTL is the only option
9. Type the numeral corresponding to your choice and press Enter.
10. When prompted to confirm the selection, enter y. The system automatically starts the configuration process, with output similar to the following example.

    Note: All examples are for an OpenStorage configuration with FC 3457 (dual-port 10 Gb Ethernet adapters).

```
Stopping services, please wait
Stopping Cluster Services                                    [ Done ]

Services stopped
Checking Fence Device                                        [ Done ]
Checking conditions...
Gathering information                                        [ Done ]
Checking BOM                                                 [ Done ]
Checking for existing nodes                                  [ Done ]
Configuring Probe Interface                                  [ Done ]
Collecting system information                                [ Done ]
Checking Switches Configuration                              [ Done ]
Stopping Cluster Services                                    [ Done ]
The following discovery may take up to 10 minutes
Discovering manageable switches                              [ Done ]
Assembling Switch Configuration                              [ Done ]
Configuring Switch                                           [ Done ]
Waiting for switch to boot                                   [ Done ]
Configuring Switch                                           [ Done ]
Waiting for switch to boot                                   [ Done ]
Saving Configuration                                         [ Done ]
Removing Probe Interface                                     [ Done ]
Comparing mapped devices                                     [ Done ]
Checking Application Interfaces                              [ Done ]
NOTICE: In order to continue the ProtecTIER Services must be stopped
on the other node.

Would you like To Stop the ProtecTIER services on the other node? (yes|no)
```

11. At the prompt to stop the other node (Server A), type y and press Enter. The configuration process continues, with output similar to the following example.

```
Stopping RAS Remotely                                          [ Done ]
Stopping VTFD Remotely                                         [ Done ]
Stopping the GFS Service Remotely                              [ Done ]
Checking repository                                            [ Done ]
Checking installed applications                                [ Done ]
Checking installed applications                                [ Done ]
Checking local raid                                            [ Done ]
Checking conditions done
```

12. The installation process prompts you to enter IP addresses for primary and secondary NTP servers and information for external application interfaces, as shown in the following example output. When prompted for the IP addresses of the NTP primary and secondary servers, choose one of the following options:
    - If you are not using NTP servers, press Enter when prompted without entering IP addresses.
    - If you are using NTP servers, enter the IP address for the primary and secondary NTP servers when prompted and press Enter after each.

    The following paragraphs deal with the external application interface IP addresses to be entered.

    ProtecTIER exposes virtual interfaces to the host, such as a media server with the plug-in installed. In version 3.4.3, the physical Ethernet ports are assigned to one virtual application interface. Currently, the physical ports are assigned to virtual interface eth0 or eth1, depending on the server configuration. This assignment option is used to group several physical interfaces into a single virtual interface, and create a bond configuration of several physical interfaces. Each virtual interface used must be configured with a corresponding IP address.

    Attention: Each configured IP address on the same server needs to be on a different subnet, and each subnet needs to be on a different VLAN. If separate subnets and VLAN's are not used, in certain environments and networks, network packets can move to other subnets, which can harm network performance and potentially reduce the network's quality of service.

    In addition, each virtual interface containing more than one physical interface (configured as a bond) needs to be configured with a load balancing method. For a server with 10 Gb interfaces, where bonding is implemented, the recommended load balancing method is Link Aggregation Control Protocol (LACP) with L3L4.

    For more information about bonding, the different load balancing methods, and whether to configure bonds at all, refer to the *IBM ProtecTIER Implementation and Best Practices*, Redbooks publication SG24-8025, available at: http://www.redbooks.ibm.com/Redbooks.nsf/RedpieceAbstracts/sg248025.html?Open or the *IBM ProtecTIER Implementation and Best Practices*, Redbooks publication SG24-8025, available at: http://www.redbooks.ibm.com/Redbooks.nsf/RedpieceAbstracts/sg248025.html?Open.

```
Please provide the following information:
----------------------------------------
NTP server timeserver, IP Address (optional):
NTP server secondary_timeserver, IP Address (optional):
ApplicationInterface external, IP Address [192.168.10.162]: 9.148.220.203
ApplicationInterface external, Netmask [255.255.255.0]: 255.255.252.0
ApplicationInterface external, Default Gateway [192.168.10.1]: 9.148.220.4
ApplicationInterface external, Hostname [node2]: annapolis
```

13. When prompted to confirm your choices as shown in the following example, verify that they are correct, type y and press Enter.

```
Please check the following values:
---------------------------------
NTP server timeserver, IP Address:
NTP server secondary_timeserver, IP Address:

ApplicationInterface external, IP Address: 9.148.220.203
ApplicationInterface external, Netmask: 255.255.252.0
ApplicationInterface external, Default Gateway: 9.148.220.4
ApplicationInterface external, Hostname: annapolis

Are you sure you want to submit these values? (yes|no|quit) y
```

14. The configuration process continues, with output similar to the following example.

```
Configuring network                                          [ Done ]
Restarting Network Service                                   [ Done ]
Configuring Application Interfaces                           [ Done ]
Stopping Remote VTFD                                         [ Done ]
Stopping Remote RAS                                          [ Done ]
Stopping cluster                                             [ Done ]
Configuring Fence Device                                     [ Done ]
Configuring cluster                                          [ Done ]
Starting cluster                                             [ Done ]
Installing NTP                                               [ Done ]
Set interfaces addresses                                     [ Done ]
Adding records to /etc/fstab                                 [ Done ]
Starting VTFD locally                                        [ Done ]
Starting VTFD remotely                                       [ Done ]
Adding Node to PT Cluster                                    [ Done ]
Starting RAS                                                 [ Done ]
Starting RAS remotely                                        [ Done ]
Collecting RAS Persistent configuration                      [ Done ]
validation will start in 10 seconds
Testing customer network connectivity                        [ Done ]
Testing connectivity to the Default Gateway                  [ Done ]
Getting number of nodes                                      [ Done ]
Testing NTP configuration                                    [ Done ]
Testing cluster's network speed                              [ Done ]
Testing connectivity to other node in the cluster            [ Done ]
Testing fence ports                                          [ Done ]
Validation is about to execute a fence on 1 node in the cluster,
the node will be forcefully shutdown and rebooted
To Continue please type "fence test", or "q" to quit:
```

15. Because you run the fence test later, in Chapter 9, “Validating the servers,” on page 83, enter q at the prompt. The configuration process finishes with output similar to the following example.

```
User aborted
validation ended
install ended successfully
```

16. Replace any cables that you removed in step 1 on page 70.

What to do next

Go to Chapter 9, “Validating the servers,” on page 83.

Chapter 9. Validating the servers

Validating Server A

About this task

Perform the procedures only if you are installing a clustered installation. If you are installing a stand-alone installation and you completed the procedures in Chapter 7, "Creating repositories," on page 61, go to Chapter 10, "Applying updates and fixes to the ProtecTIER software for version 3.4.3 and higher," on page 89.

Procedure

1. Log in to Server A and access the ProtecTIER Service menu. See 2 on page 42 through 3 on page 43 of Chapter 5, "Configuring Server A," on page 39 for the login procedure. The **ProtecTIER Service** menu displays.

```
--------------------------------------------------------------------------
  ProtecTIER Service Menu running on rasddx
--------------------------------------------------------------------------
   1) ProtecTIER Configuration (...)
   2) Manage ProtecTIER services (...)
   3) Health Monitoring (...)
   4) Problem Alerting (...)
   5) Version Information (...)
   6) Generate a service report
   7) Generate a system view
   8) Update ProtecTIER code

   E) Exit
--------------------------------------------------------------------------
>>> Your choice?
```

2. Type the numeral corresponding to `ProtecTIER Configuration` and press Enter. The **ProtecTIER Configuration** menu displays.

```
--------------------------------------------------------------------------
  ProtecTIER Service Menu running on rasddx
  ProtecTIER Configuration (...)
--------------------------------------------------------------------------
   1) Configure ProtecTIER node
   2) Recover Configuration for a replaced server
   3) Configure machine serial number for a replaced server
   4) Configure RAS
   5) Update Time, Date, Timezone & Timeserver(s)
   6) Scan storage interconnections
   7) File Systems Management (...)
   8) Configure replication (...)
   9) IP Network configuration (...)
   10) Update Firmware
   11) Update the System's name
   12) Validate configuration
   13) Single node - code upgrade (for Support Use Only)

   B) Back
   E) Exit
--------------------------------------------------------------------------
>>> Your choice?
```

3. Type the numeral corresponding to `Validate configuration` and press Enter. The system displays the following messages:

```
Begin Processing Procedure

Testing customer network connectivity                          [ Done ]
Testing connectivity to the Default Gateway                    [ Done ]
Getting number of nodes                                        [ Done ]
Testing NTP configuration                                      [ Done ]
Testing cluster's network speed                                [ Done ]
Testing connectivity to other node in the cluster              [ Done ]
Testing fence ports                                            [ Done ]
Validation is about to execute a fence on 1 node in the cluster,
  the node will be forcefully shutdown and rebooted
To Continue please type "fence test", or "q" to quit:
```

Note: The fence test occurs only if there are two nodes in the cluster.

4. Type `fence test` and press Enter. The system displays the messages:

```
Testing connectivity to the fence device [ Done ]
Would you like to stop the VTFD service on both nodes? (yes|no)
```

5. Type: `yes` and press Enter. The system displays the message:

```
Stopping RAS                                                   [ Done ]
Stopping VTFD                                                  [ Done ]
Stopping RAS                                                   [ Done ]
Stopping VTFD locally                                          [ Done ]
Stopping RAS Remotely                                          [ Done ]
Stopping VTFD remotely                                         [ Done ]
Testing fencing                                                [ Done ]
Starting VTFD                                                  [ Done ]
Starting RAS                                                   [ Done ]
validation ended

End Processing Procedure Successfully

Press <Enter> to continue.
```

6. Press Enter to exit. If the test succeeds, go to “Validating Server B” on page 86. If the test fails on either node, contact your next level of support to resolve the failure conditions. You must have the customer number when you contact software support. To avoid entitlement delays, have the customer number available before you initiate the call.

Note: Alerts might be generated as the validation tests are running. You can view the ProtecTIER Manager Alerts Log on the ProtecTIER workstation to monitor the alerts as they occur. Click **Alerts** in the lower right corner of the ProtecTIER Manager pane to display the Alerts Log pane (Figure 38 on page 85).

Figure 38. Alerts Log

When you are finished reviewing alerts, click **Clear Alerts** in the lower right corner of the Alerts Log pane.

Validating Server B

Procedure

1. Connect the keyboard and monitor to Server B.
2. Log in to Server B, and access the ProtecTIER Service menu. See 2 on page 42 through 3 on page 43 of Chapter 5, “Configuring Server A,” on page 39 for the login procedure.
3. Type the numeral corresponding to `ProtecTIER Configuration` and press Enter. The **ProtecTIER Configuration** menu displays.

```
------------------------------------------------------------------------
  ProtecTIER Service Menu running on rasddx
  ProtecTIER Configuration (...)
------------------------------------------------------------------------
   1) Configure ProtecTIER node
   2) Recover Configuration for a replaced server
   3) Configure machine serial number for a replaced server
   4) Configure RAS
   5) Update Time, Date, Timezone & Timeserver(s)
   6) Scan storage interconnections
   7) File Systems Management (...)
   8) Configure replication (...)
   9) IP Network configuration (...)
   10) Update Firmware
   11) Update the System's name
   12) Validate configuration
   13) Single node - code upgrade (for Support Use Only)

   B) Back
   E) Exit
------------------------------------------------------------------------
>>> Your choice?
```

4. Type the numeral corresponding to `Validate configuration` and press Enter. The system displays the following messages:

```
Begin Processing Procedure

Testing customer network connectivity                          [ Done ]
Testing connectivity to the Default Gateway                    [ Done ]
Getting number of nodes                                        [ Done ]
Testing NTP configuration                                      [ Done ]
Testing cluster's network speed                                [ Done ]
Testing connectivity to other node in the cluster              [ Done ]
Testing fence ports                                            [ Done ]
Validation is about to execute a fence on 1 node in the cluster,
  the node will be forcefully shutdown and rebooted
To Continue please type "fence test", or "q" to quit:
```

5. Type `fence test` and press Enter. The system displays the messages:

```
Testing connectivity to the fence device [ Done ]
Would you like to stop the VTFD service on both nodes? (yes|no)
```

6. Type `yes` and press Enter. The system displays the message:

```
Stopping RAS                                                    [ Done ]
Stopping VTFD                                                   [ Done ]
Stopping RAS                                                    [ Done ]
Stopping VTFD locally                                           [ Done ]
Stopping RAS Remotely                                           [ Done ]
Stopping VTFD remotely                                          [ Done ]
Testing fencing                                                 [ Done ]
Starting VTFD                                                   [ Done ]
Starting RAS                                                    [ Done ]
validation ended

End Processing Procedure Successfully

Press <Enter> to continue.
```

7. Choose one of the following options:
   - If the test succeeds, system validation is complete. Go to Chapter 10, "Applying updates and fixes to the ProtecTIER software for version 3.4.3 and higher," on page 89.
   - If the test fails on either node, contact your next level of support to resolve the failure conditions. You must have the customer number when you contact software support. To avoid entitlement delays, have the customer number available before you initiate the call.

Chapter 10. Applying updates and fixes to the ProtecTIER software for version 3.4.3 and higher

After you validate the servers, you might need to install updates to ProtecTIER for fixes and other updates.

About this task

Important: These procedures are for concurrent fix updates. To understand if a specific fix update is concurrent or non-concurrent, consult the release notes for the update. Release notes are available on the ProtecTIER fix update (patch) page of the IBM website. Procedures for non-concurrent fixes are documented in the release notes for each fix package.

The ProtecTIER version 3.4.3 release includes the ability to apply the fix update to the server in three ways:

- Using a file
- Using a USB drive
- Creating a DVD

Table 10. Preparing the servers for the most current update

Tasks	Procedure
Check the version of ProtecTIER running on each server.	"Checking the ProtecTIER version for servers at ProtecTIER version 3.3.1 or higher" on page 90
Download the most current version of ProtecTIER (version 3.4.x) from Fix Central. Copy the downloaded files to either a DVD or a USB drive, or copy the files directly to the appropriate location on the server.	"Downloading the ProtecTIER version 3.4.x fix update" on page 91
If you are installing from a DVD or a file continue with the topic to the right.	"Applying the ProtecTIER 3.4.x updates using a DVD or a file" on page 93
If you are installing from a USB drive continue with the topic to the right.	"Applying the ProtecTIER 3.4.x updates using a DVD or a file" on page 93

Checking the ProtecTIER version for servers at ProtecTIER version 3.3.1 or higher

Check the ProtecTIER version on servers at ProtecTIER version 3.3.1 or later.

Procedure

Perform this procedure on each server for which you need version information. Make note of the ProtecTIER version for each server to verify that the fix update you are applying is a later version of ProtecTIER than the version currently installed.

1. Log in to server A. At the login prompt, log in with the ID `ptconfig` and the password `ptconfig`.
2. The ProtecTIER Service main menu is displayed.

```
--------------------------------------------------------------------------
  ProtecTIER Service Menu running on rasddx
--------------------------------------------------------------------------
   1) ProtecTIER Configuration (...)
   2) Manage ProtecTIER services (...)
   3) Health Monitoring (...)
   4) Problem Alerting (...)
   5) Version Information (...)
   6) Generate a service report
   7) Generate a system view
   8) Update ProtecTIER code

   E) Exit
--------------------------------------------------------------------------
>>> Your choice?
```

3. From the main ProtecTIER Service menu, select the **Version information** option. The **Version information** menu is displayed.

```
--------------------------------------------------------------------------
 ProtecTIER Service Menu running on rasddx
 Version Information (...)
--------------------------------------------------------------------------
  1) Display version information
  2) Display Machine Reported Product Data (MRPD)
  3) Display Firmware Versions

  B) Back
  E) Exit
--------------------------------------------------------------------------
>>> Your choice?
```

4. Select the option to **Display version information**. The ProtecTIER version is shown in the first line of output, in the first three digits after the colon. The version information looks similar to the following example message:

   ```
   PT version : 3.3.1
   ```

5. Record the ProtecTIER version. Verify that the fix update you are applying is a later version than the currently installed version.
6. If you are updating a clustered configuration, repeat steps 1 through 5 for server B.
7. Continue on to "Downloading the ProtecTIER version 3.4.x fix update" on page 91.

Downloading the ProtecTIER version 3.4.x fix update

Use these procedures to download ProtecTIER version 3.4.x fix update from the IBM website.

Before you begin

If you plan to copy the files to a USB drive, it must be formatted FAT32.

About this task

Important: These procedures are for concurrent fix updates. To determine whether a specific fix update is concurrent or non-concurrent, consult the release notes for the update. Release notes are available on the ProtecTIER fix update (patch) page of the IBM website. All package names and versions that are listed are examples only. The exact package file names can differ.

Procedure

Sign in to ibm.com®, find the correct fix package, and download the fix update.

1. Go to www.ibm.com.
2. Click the **Sign in** link in the masthead and log in using your IBM user ID. If you do not have an IBM user ID, follow the procedures to create one from any IBM web page.

   Note: If you need help with the login, go to the **Help and FAQ for authentication** website: https://www.ibm.com/account/profile/.
3. From the Home page, click: **Support & Downloads** > **Download** > **Fixes, updates & drivers**.
4. If the **IBM Support Portal - Quick start** page does not open automatically, click **Go to quick start** in the upper left corner of the web page. The **IBM Support Portal - Quick start** page opens.
5. Under **1. Choose your products**:
   a. Click **Search**.
   b. Type `ProtecTIER` in the empty field. As you type, search results that match your input appear in a list below the field.
   c. In the list of search results, select the check box for the product or products for which you want to download files.
6. Under **2. Choose your page**, click **Downloads** and then click **Continue**.
7. In the **Downloads and fixes** window, click the downloads link for the applicable ProtecTIER product, such as View TS7650G Deduplication Gateway (3958-DD5) ProtecTIER Gateway Edition downloads. You might need to hover the mouse over the link for the full text of the link to become visible. The **Select fixes** page opens.
8. From the **Results** list, click the most recent entry, such as v3.4.x for the product you specified, where *3.4.x* is the most current version of ProtecTIER 3.4 available for download. The **Download options** page is displayed.
9. In the **Download Options** box, click **Download using bulk FTP**. Select the check box to include prerequisites and co-requisite fixes. Click **Continue**. The **Terms and Conditions** page is displayed.
10. Read the information and then click **I agree**. The tar file window for the product that you selected opens.

Note: The specific file name depends on the fix package that you are downloading.

11. Select **Save file** and click **OK**.

    The ProtecTIER software fix update downloads to the local hard disk drive.

12. Copy the downloaded `PT_TS7650G_V3.4.x.x.x86_64.tar` file to either a DVD or USB drive and use this disk or drive to run the fix update. Alternatively, you can copy the file directly to the ProtecTIER server. If you choose to copy the file directly to the server, copy it to the `/install/new` directory on the ProtecTIER server. In the following example, commands and output have more line breaks to ensure that they fit on the page.

    ```
    cp /install/PT_TS7650G_V3.4.x.x.x86_64.tar /install/new
    ls -l /install/new -rwxr-xr-x 1 root root 873666560 Feb 28 15:11
    PT_TS7650G_V3.4.x.x.x86_64.tar
    ```

13. Go to "Applying the ProtecTIER 3.4.x updates using a DVD or a file" on page 93.

Applying the ProtecTIER 3.4.x updates using a DVD or a file

You update the ProtecTIER servers to the latest v3.4.x code level through the ProtecTIER Service menu.

Before you begin

You have completed "Downloading the ProtecTIER version 3.4.x fix update" on page 91 and saved the update package either to a DVD, a USB drive or copied it to the `/install/new` directory on Server A.

The terms *update file*, *update package*, and *software package* are used interchangeably in this procedure.

Important: These procedures are for concurrent fix updates. To understand if a specific fix update is concurrent or non-concurrent, you must consult the release notes for the update, available on the ProtecTIER fix update (patch) page of the IBM website. Procedures for non-concurrent fixes are documented in the release notes for each fix package. All update file names and versions that are listed are examples only. The exact update file names can differ.

Procedure

1. If you saved the update package to a DVD in step 12 on page 92, perform the following substeps:
   a. Insert the DVD into the disk drive tray of Server A.
   b. Close the disk drive tray.
2. On Server A, access the ProtecTIER Service menu.
3. At the **login** prompt, log in with user name `ptconfig` and password `ptconfig`.
4. At the command prompt, type `menu` and press Enter. The **ProtecTIER Service Menu** is displayed.

```
------------------------------------------------------------------------
  ProtecTIER Service Menu running on rasddx
------------------------------------------------------------------------
   1) ProtecTIER Configuration (...)
   2) Manage ProtecTIER services (...)
   3) Health Monitoring (...)
   4) Problem Alerting (...)
   5) Version Information (...)
   6) Generate a service report
   7) Generate a system view
   8) Update ProtecTIER code

   E) Exit
------------------------------------------------------------------------
>>> Your choice?
```

5. From the main menu, select the numeral corresponding to **Update ProtecTIER code** and press Enter. A message that is similar to the following example is displayed.

```
Begin Processing Procedure

Going to extract upgrade package

============================================================
            ptupgrade V3.4.89.0 package
            kernel    2.6.18-238.40.1.el5.x86_64
            PT Build  7133.089
============================================================
```

```
Extracting perl modules...
job 805 at 2016-02-24 20:34
job 806 at 2016-02-24 20:34
Going to start installation GUI process
Checking for available packages:                    [ Done ]
```

If older update packages are found, the system prompts you to delete them if desired.

If you are not prompted to delete older packages, or after you delete them, output similar to the following example displays.

```
Upgrade candidates:
1. /mnt/cdrom/PT_MD5_TS7650_Medium_V3.4.97.0-full.x86_64.tar (node 1)
Which Package do you want to install ? (press 'q' to quit) :
```

6. Type the numeral corresponding to the update package that you want to install and press Enter. Output similar to the following example displays.

```
Extracting new GUI package from upgrade package                 [ Done ]
Checking prerequisites conditions for package                   [ Done ]
Going to upgrade to package
  /mnt/cdrom/PT_MD5_TS7650_Medium_V3.4.97.0-full.x86_64.tar
  (build=7133.097, version=3, release=3, minor=97, fix=0)
Upgrade method = SEQUENTIAL
Do you want to continue ? (yes|no)
```

7. Enter yes to continue. Respond to any prompts as required.
8. When the update is complete, you are prompted to restart the server. Press Enter.

9. When the restart cycle completes, the login prompt is shown. Check the status of the services on the server on which you updated the code.
   a. At the **login** prompt, log in with user name `ptconfig` and password `ptconfig`.
   b. At the command prompt, type `menu` and press Enter. The ProtecTIER Service main menu is displayed:

```
--------------------------------------------------------------------------
  ProtecTIER Service Menu running on rasddx
--------------------------------------------------------------------------
   1) ProtecTIER Configuration (...)
   2) Manage ProtecTIER services (...)
   3) Health Monitoring (...)
   4) Problem Alerting (...)
   5) Version Information (...)
   6) Generate a service report
   7) Generate a system view
   8) Update ProtecTIER code

   E) Exit
--------------------------------------------------------------------------
>>> Your choice?
```

   c. Select the option to **Manage ProtecTIER services**. The **Manage ProtecTIER services** menu is displayed.

```
--------------------------------------------------------------------------
  ProtecTIER Service Menu running on rasddx
             Manage ProtecTIER Services (...)
--------------------------------------------------------------------------
   1) Display services status
   2) Start all services
   3) Stop all services
   4) Stop ProtecTIER services only (including GFS)
   5) Stop VTFD service only

   B) Back
   E) Exit
--------------------------------------------------------------------------
>>> Your choice?
```

   d. Select the option to **Display services status**.
   e. The service status is expected to be `UP` for all services. If a service status is `STILL_LOADING`, wait and check the service status again until it changes to `UP`.

```
Service                  Status
=========================================
cman                     UP
clvmd                    UP
gfs                      UP
vtfd                     STILL_LOADING
ptrasd                   UP
ptconfigd                UP
```

10. Verify the ProtecTIER version on the server on which you updated the code. Use the ProtecTIER Service menu.
    a. From the main ProtecTIER Service menu, select the **Version information** option.
    b. The **Version information** menu is displayed.

```
------------------------------------------------------------------------
 ProtecTIER Service Menu running on rasddx
 Version Information (...)
------------------------------------------------------------------------
  1) Display version information
  2) Display Machine Reported Product Data (MRPD)
  3) Display Firmware Versions

  B) Back
  E) Exit
------------------------------------------------------------------------
>>> Your choice?
```

    c. Select the **Display version information** option. The ProtecTIER version is shown in the first line of output, in the first three digits after the colon. The version information looks similar to the following message:

```
PT version : 3.4.1.1
```

    If the ProtecTIER fix update version is correct, continue to the next step. If the ProtecTIER version is incorrect, the update failed. Contact IBM Support for assistance.
11. If in a clustered configuration, repeat steps 1 on page 93 through 10 for Server B.
12. The code update procedure is now complete. Go to Chapter 11, "Releasing the system to the customer," on page 99.

Applying the ProtecTIER 3.4.x updates using a USB drive

USB installation is an autorun process that upgrades the ProtecTIER software, reboots and configures the server.

Before you begin

You have completed "Downloading the ProtecTIER version 3.4.x fix update" on page 91 and saved the update package to a USB drive.

The terms *update file*, *update package*, and *software package* are used interchangeably in this procedure.

Important: These procedures are for concurrent fix updates. To understand if a specific fix update is concurrent or non-concurrent, you must consult the release notes for the update, available on the ProtecTIER fix update (patch) page of the IBM website. Procedures for non-concurrent fixes are documented in the release notes for each fix package. All update file names and versions that are listed are examples only. The exact update file names can differ.

Procedure

1. Insert the USB drive into the far right USB port on the rear of the server.
2. From a command prompt, use the following command to mount the USB drive. `#/bin/mount /dev/usbStgDevice /media`

3. Access the ProtecTIER Service menu on the server into which you plugged the USB drive.

```
------------------------------------------------------------------------
  ProtecTIER Service Menu running on rasddx
------------------------------------------------------------------------
   1) ProtecTIER Configuration (...)
   2) Manage ProtecTIER services (...)
   3) Health Monitoring (...)
   4) Problem Alerting (...)
   5) Version Information (...)
   6) Generate a service report
   7) Generate a system view
   8) Update ProtecTIER code
   9) ProtecTIER Analysis (...)
  10) USB Installation (...)

   E) Exit
------------------------------------------------------------------------
>>> Your choice?
```

4. From the main menu, select the numeral corresponding to **USB Installation (...)** and press Enter. The following menu appears.

```
------------------------------------------------------------------------
  ProtecTIER Service Menu running on rasddx
  USB Installation (...)
------------------------------------------------------------------------
   1) Monitor istallation progress
   2) Generate USB files

   B) Back
   E) Exit
------------------------------------------------------------------------
>>> Your choice?
```

5. Select the numeral corresponding to **Generate USB files** and press Enter. The RAS services begin to create the USB configuration files.
6. Answer the following questions.

```
Begin Processing Procedure [May 10 04:28:02]

Please provide the following information: ('q' to quit)
-------------------------------------------------------
1)  Configure ProtecTIER.
2)  Upgrade ProtecTIER code.
3)  Upgrade ProtecTIER code and Configure system.
Choose: 1
```

Note: In case of an upgrade, the guided menu asks for the package to install.

```
Please provide the following information:
-----------------------------------------
1)  Single node.
2)  Cluster node.
Choose: 1

Please provide the following information for node 1:
---------------------------------------------------
Serial number:
Is this the ProtecTIER system to install? (yes|no) no
Serial number for the ProtecTIER system to install (7 alphanumeric string): 78IBM00
NTP server timeserver, IP Address (optional):
NTP server secondary_timeserver, IP Address (optional):
ApplicationInterface external, IP address: 192.178.0.10
ApplicationInterface external, Netmask [255.255.255.0]:
ApplicationInterface external, Default Gateway: 192.178.0.1
ApplicationInterface external, Hostname: test
```

```
ApplicationInterface bmc, IP Address [192.168.10.163]:
ApplicationInterface bmc, Netmask [255.255.255.0]:
ApplicationInterface bmc, Default Gateway: [192.168.10.1]:
```

Note: In a cluster environment, most of the questions will be repeated for the second node.

```
Please provide the following RAS information:
---------------------------------------------
Customer SMTP server IP address (optional):
Customer number (7 alphanumeric): IBM0000
Country code (3 alphanumeric):052
Business company name, e.g. IBM, (optional):
Machine location, e.g. Server room, (optional):

Configuration files were copied successfully to the USB.

End Processing Procedure Successfully [May 10 04:28:02]

Press <ENTER> to continue
```

7. You can verify the files created under /media/.

```
[root@Ronaldo ~]# ls /media/
pt_command.txt  pt_serial_number.txt  pt_user_values.xml
[root@Ronaldo ~]#
```

Note: In case of a configuration operation, you may see files similar to these. If you selected to upgrade, the files also include the PT installation package and another file called `package_md5.txt`.

8. Use the following command to unmount the USB drive. `#unmount /media/`
9. Remove the USB drive and put it into the right-most USB port on the rear of Server A. The PT-USB deamon detects the USB device and starts the upgrade automatically. When autorun completes, the PT-USB daemon restarts the server. If you selected the upgrade and configure option, the configuration process then begins automatically. If you selected to configure only, the server is not rebooted when the process completes.
10. On the USB Installation menu, select the option to **Monitor installation progress**. See the menu in step "Applying the ProtecTIER 3.4.x updates using a USB drive" on page 96. When the configuration is complete, the following message appears.

```
Install ended successfully
```

11. If you are in a clustered environment, use the USB drive to complete the installation on Server B.

Chapter 11. Releasing the system to the customer

After you complete installation of the TS7650G (Gateway), ProtecTIER V3.4.3, you must turn the system over to the customer.

About this task

The installation and configuration process for the TS7650G is complete.

Follow the standard IBM procedures for releasing the system to the customer. Refer the customer to the *IBM ProtecTIER User's Guide for VTL Systems*, GA32-0922 for information about managing and operating the ProtecTIER system, such as the procedure for enabling ProtecTIER Replication Manager in clustered installations.

Appendix A. Company information worksheet

IBM service representatives use the information that is provided on the company information worksheet to customize your IBM storage complex. When you use any of the remote support features, the TSSC sends this information to IBM so an IBM service representative can contact you.

Table 11. Company information worksheet

Required information	Description	Your information
Business company name	The full name of your company. IBM service representatives use this information to identify your company when they receive Call Home reports from your IBM storage system. Ensure that the company name provided is consistent with all other machines that correspond to your IBM customer account.	
Customer number	The IBM-assigned customer number for your company. This is provided by the customer.	
Country code	The two-character code that must be used in order to reach your country by phone or fax, from another country. This is **not** the three-digit RETAIN country code. See Table 12 on page 102.	
SMTP Server ID / IP address		
SMTP email address	The email address of the administrator who receives failure alerts for the server. This may or may not be the administrator listed below.	
System administrator information Provide information about your storage system administrator in the following section.		
Administrator name	The name of the individual at your site who IBM service representatives should contact about IBM storage system service matters.	
Administrator email address	The storage system administrator's email address.	
Voice phone number	The primary telephone number that IBM service representatives should use to contact the storage system administrator. Include the area code and the country code, if appropriate.	
Fax number	The primary fax number that IBM service representatives should use to fax documents to the storage system administrator. Include the area code and the country code, if appropriate.	

Table 11. Company information worksheet (continued)

Required information	Description	Your information
Alternate fax number	An alternate fax number that IBM service representatives can use to fax documents to the storage system administrator. Include the area code and the country code, if appropriate.	
Administrator mailing address	The postal mailing address for the storage system administrator. provide the full street address, building (if appropriate), city or locality, state or province, and postal or zip code.	
Storage system information Provide basic information about your storage system and the TSSC in the following section.		
Machine location	The address of the facility where the TS7650 server(s) reside. If different from the administrator mailing address above, provide the full street address, building (if appropriate), city or locality, state or province, and postal or zip code.	
Call back phone number	The phone number of the modem being used for Call Home. Include the area code and the country code, if appropriate.	
Disk array machine type(s) and model number(s)	The machine type(s) and model number(s) for the attached disk array storage subsystem(s). For non-IBM equipment, also provide vendor name(s). Use an additional sheet if necessary.	
Disk array serial number(s)	The serial number(s) for the attached disk array storage subsystem(s).	

Use the information in the following table to convert a country to a code, and use that code as an entry in the **Country code** field of the Table 11 on page 101.

Table 12. Country codes

Country	Code	Country	Code	Country	Code	Country	Code	Country	Code
Afghanistan	af	Cook Islands	ck	Iceland	is	Nauru	nr	Solomon Islands	sb
Albania	al	Costa Rica	cr	India	in	Nepal	np	Somalia	so
Algeria	dz	Croatia	hr	Indonesia	id	Netherlands	nl	South Africa	za
American Samoa	as	Cuba	cu	Iran	ir	Netherlands Antilles	an	South Korea	kr
Andorra	ad	Cyprus	cy	Iraq	iq	Neutral Zone	nt	Spain	es
Angola	ao	Czech Republic	cz	Ireland	ie	New Caledonia (French)	nc	Sri Lanka	lk
Anguilla	ai	Denmark	dk	Israel	il	New Zealand	nz	Sudan	sd
Antarctica	aq	Djibouti	dj	Italy	it	Nicaragua	ni	Suriname	sr
Antigua and Barbuda	ag	Dominica	dm	Ivory Coast (Cote D'Ivoire)	ci	Niger	ne	Svalbard and Jan Mayen Islands	sj

Table 12. Country codes (continued)

Country	Code	Country	Code	Country	Code	Country	Code	Country	Code
Argentina	ar	Dominican Republic	do	Jamaica	jm	Nigeria	ng	Swaziland	sz
Armenia	am	East Timor	tp	Japan	jp	Niue	nu	Sweden	se
Aruba	aw	Ecuador	ec	Jordan	jo	Norfolk Island	nf	Switzerland	ch
Australia	au	Egypt	eg	Kazakhstan	kz	North Korea	kp	Syria	sy
Austria	at	El Salvador	sv	Kenya	ke	Northern Mariana Islands	mp	Tadjikistan	tj
Azerbaidjan	az	Equatorial Guinea	gq	Kiribati	ki	Norway	no	Taiwan	tw
Bahamas	bs	Eritrea	er	Kuwait	kw	Oman	om	Tanzania	tz
Bahrain	bh	Estonia	ee	Kyrgyzstan	kg	Pakistan	pk	Thailand	th
Bangladesh	bd	Ethiopia	et	Laos	la	Palau	pw	Togo	tg
Barbados	bb	Falkland Islands	fk	Latvia	lv	Panama	pa	Tokelau	tk
Belarus	by	Faroe Islands	fo	Lebanon	lb	Papua New Guinea	pg	Tonga	to
Belgium	be	Fiji	fj	Lesotho	ls	Paraguay	py	Trinidad and Tobago	tt
Belize	bz	Finland	fi	Liberia	lr	Peru	pe	Tunisia	tn
Benin	bj	Former Czechoslovakia	cs	Libya	ly	Philippines	ph	Turkey	tr
Bermuda	bm	Former USSR	su	Liechtenstein	li	Pitcairn Island	pn	Turkmenistan	tm
Bhutan	bt	France	fr	Lithuania	lt	Poland	pl	Turks and Caicos Islands	tc
Bolivia	bo	France (European Territory)	fx	Luxembourg	lu	Polynesia (French)	pf	Tuvalu	tv
Bosnia-Herzegovina	ba	French Guyana	gf	Macau	mo	Portugal	pt	Uganda	ug
Botswana	bw	French Southern Territories	tf	Macedonia	mk	Puerto Rico	pr	Ukraine	ua
Bouvet Island	bv	Gabon	ga	Madagascar	mg	Qatar	qa	United Arab Emirates	ae
Brazil	br	Gambia	gm	Malawi	mw	Reunion (French)	re	United Kingdom	uk
British Indian Ocean Territory	io	Georgia	ge	Malaysia	my	Romania	ro	United States of America	us
Brunei Darussalam	bn	Germany	de	Maldives	mv	Russian Federation	ru	Uruguay	uy
Bulgaria	bg	Ghana	gh	Mali	ml	Rwanda	rw	USA Minor Outlying Islands	um
Burkina Faso	bf	Gibraltar	gi	Malta	mt	S. Georgia & S. Sandwich Isls.	gs	Uzbekistan	uz
Burundi	bi	Great Britain	gb	Marshall Islands	mh	Saint Helena	sh	Vanuatu	vu
Cambodia	kh	Greece	gr	Martinique (French)	mq	Saint Kitts & Nevis Anguilla	kn	Vatican City State	va

Table 12. Country codes (continued)

Country	Code	Country	Code	Country	Code	Country	Code	Country	Code
Cameroon	cm	Greenland	gl	Mauritania	mr	Saint Lucia	lc	Venezuela	ve
Canada	ca	Grenada	gd	Mauritius	mu	Saint Pierre and Miquelon	pm	Vietnam	vn
Cape Verde	cv	Guadeloupe (French)	gp	Mayotte	yt	Saint Tome (Sao Tome) and Principe	st	Virgin Islands (British)	vg
Cayman Islands	ky	Guam (USA)	gu	Mexico	mx	Saint Vincent & Grenadines	vc	Virgin Islands (USA)	vi
Central African Republic	cf	Guatemala	gt	Micronesia	fm	Samoa	ws	Wallis and Futuna Islands	wf
Chad	td	Guinea	gn	Moldavia	md	San Marino	sm	Western Sahara	eh
Chile	cl	Guinea Bissau	gw	Monaco	mc	Saudi Arabia	sa	Yemen	ye
China	cn	Guyana	gy	Mongoliar	mn	Senegal	sn	Yugoslavia	yu
Christmas Island	cx	Haiti	ht	Montserrat	ms	Seychelles	sc	Zaire	zr
Cocos (Keeling) Islands	cc	Heard and McDonald Islands	hm	Morocco	ma	Sierra Leon	sl	Zambia	zm
Colombia	co	Honduras	hn	Mozambique	mz	Singapore	sg	Zimbabwe	zw
Comoros	km	Hong Kong	hk	Myanmar	mm	Slovak Republic	sk		
Congo	cg	Hungary	hy	Namibia	na	Slovenia	si		

Appendix B. IP address worksheet

Use this worksheet to specify the IP addresses assigned to the TS7650G components. IBM service representatives use the information provided to define the IP addresses of components supported by the TSSC and ECC. When Call Home information is sent to IBM through VPN or modem, or sends you notices about serviceable events, these settings will be included in the information to identify and provide important information about the service request.

Table 14 on page 106 and Table 18 on page 108 show the default IP addresses for the TS7650G servers with VTL configurations.

Table 16 on page 107 shows the default IP addresses for the TS7650G servers with FSI configurations.

Table 20 on page 109 shows the IP address, network mask, DNS and VLAN settings for the source and destination servers for replication. This information is needed to configure the individual ports to communicate and transfer data over the replication network. Write this information in the spaces provided for future reference. Table 21 on page 110 shows the host names and other settings needed for replication. Write the appropriate information in the spaces provided for future reference.

Table 23 on page 112 shows the default IP addresses for the Baseboard Management Controller.

Note: TSSC is not supported on 3958 DD6 servers.

Table 24 on page 112 shows the default IP addresses for the Electronic Customer Care.

Attention:

1. All components use subnet mask **255.255.255.0**.
2. Do not configure the replication ports on the same subnet as the external LAN port Eth2. Doing so may cause replication errors.

ProtecTIER exposes virtual interfaces to the host, such as a media server with the plug-in installed. In version 3.4.3, the physical Ethernet ports are assigned to one virtual application interface. Currently, the physical ports are assigned to virtual interface fsi1. This assignment option is used to group several physical interfaces into a single virtual interface, and create a bond configuration of several physical interfaces. Each virtual interface used must be configured with a corresponding IP address.

Attention: Each configured IP address on the same server needs to be on a different subnet, and each subnet needs to be on a different VLAN. If separate subnets and VLAN's are not used, in certain environments and networks, network packets can move to other subnets, which can harm network performance and potentially reduce the network's quality of service.

In addition, each virtual interface containing more than one physical interface (configured as a bond) needs to be configured with a load balancing method. For a

server with 10 Gb interfaces, where bonding is implemented, the recommended load balancing method is LACP with L3L4.

For more information about bonding, the different load balancing methods, and whether to configure bonds at all, refer to the *IBM ProtecTIER Implementation and Best Practices*, Redbooks publication SG24-8025, available at: http://www.redbooks.ibm.com/Redbooks.nsf/RedpieceAbstracts/sg248025.html?Open.

Factory-default IP addresses for a stand-alone VTL configuration for a TS7650G 3958 DD6

Table 13. Factory-default server IP addresses for a stand-alone VTL ProtecTIER server (3958 DD6)

Stand-alone TS7650 VTL configuration	Component	Port	Function	Factory Default IP Address
	Server A	eth2	Customer Local LAN	192.168.10.161
	Server A	eth0	Replication Network 1	192.168.20.1
	Server A	eth1	Replication Network 2	192.168.21.1
	Server A	bmc	BMC Network	192.168.10.163

Factory-default IP addresses for a stand-alone VTL configuration for a TS7650G 3958 DD5

Table 14. Factory-default server IP addresses for a stand-alone VTL ProtecTIER server (3958 DD5)

Stand-alone TS7650 VTL configuration	Component	Port	Function	Factory Default IP Address
Node A (the server located in the lower part of the rack)	Server A	eth0	Customer local LAN	192.168.10.161
	Server A	eth1	Cluster network 1	N/A
	Server A	eth2	Replication network 1	192.168.20.1
	Server A	eth3	RAS	172.31.1.xx
	Server A	eth4	Cluster network 2	N/A
	Server A	eth5	Replication network 2	192.168.21.1

Factory-default IP addresses for a single node FSI configuration for a TS7650G 3958 DD6

Table 15. Factory-default server IP addresses for a single node FSI ProtecTIER server (3958 DD6

Stand-alone TS7650G FSI configuration	Component	Physical Port (virtual port)	Function	Factory IP Address
Node A - 1 Gb/s ethernet card (the control unit on the bottom of the enclosure chassis)	Server A	E1 (eth0)	Replication network 1	192.168.10.161
		E2 (eth1)	Replication network 2	192.169.21.1
		E3 (eth 3)	Customer local LAN	192.168.10.161
			BMC (A 1Gb/s port that you can connect to the x86 subsystem or directly to the baseboard management controller (BMC). Supports the Intelligent Platform Management Interface (IPMI)	192.168.10.163

Factory-default IP addresses for a single node FSI configuration for a TS7650G 3958 DD5

Table 16. Factory-default server IP addresses for a single node FSI ProtecTIER server (3958 DD5)

Stand-alone TS7650 FSI configuration	Component	Port	Function	Factory Default IP Address
Node A (the server located in the lower part of the rack)	Server A	eth0	Customer local LAN	192.168.10.161
	Server A	eth1	Cluster network 1	N/A
	Server A	eth2	Replication network 1 (1 Gb or 10 Gb)	1 Gb : 192.168.20.1 10 Gb : 192.168.153.1[1]
	Server A	eth3	RAS	172.31.1.xx
	Server A	eth4	FSI	1 Gb or 10 Gb : 192.168.150.1[1]
	Server A	eth5	FSI	192.168.151.1
	Server A	eth6	FSI	1 Gb or 10 Gb : 192.168.152.1[1]
	Server A	eth7	FSI	1 Gb or 10 Gb : 192.168.152.1[1]
	Server A	eth8	FSI	192.168.153.1
	Server A	eth9	Replication network 2 (10 Gb only)	192.168.154.1
	Server A	eth10	FSI	192.168.155.1
	Server A	eth11	FSI	192.168.156.1
	Server A	eth12	Cluster network 2	N/A
	Server A	eth13	Replication network 2 (1 Gb only)	192.168.21.1
Note: [1] 1 Gb Ethernet adapters use ports eth4-eth7 (Slot 3, Ports 1-4) and eth8-eth11 (Slot 4, Ports 1-4). 10 Gb Ethernet adapters use ports eth4-eth5 (Slot 3, Ports 1-2) and eth6-eth7 (Slot 4, Ports 1-2).				

Factory-default server IP addresses for a clustered VTL TS7650G 3958 DD6

Table 17. Factory-default server IP addresses for a clustered VTL ProtecTIER system (3958 DD6)

TS7650 clustered VTL system	Component	Port	Function	Factory Default IP Address
Node A (the server located in the lower part of the rack)	Server A	eth2	Customer Local LAN	192.168.10.161
		eth0	Replication Network	192.168.20.1
		bmc	BMC Network	192.168.10.163
		eth1	Cluster Network	10.0.0.51
Node B (the server located in the lower part of the rack)	Server B	eth2	Customer Local LAN	192.168.10.162
		eth0	Replication Network	192.168.20.2
		bmc	BMC Network	192.168.10.164
		Note: The correct IP address for the BMC in Server B is 192.168.10.164.		
		eth1	Cluster Network	10.0.0.52

Factory-default server IP addresses for a clustered VTL TS7650G 3958 DD5

Table 18. Factory-default server IP addresses for a clustered VTL ProtecTIER system (3958 DD5)

TS7650 clustered VTL system	Component	Port	Function	Factory Default IP Address
Node A (the server located in the lower part of the rack)	Server A	eth0	Customer local LAN	192.168.10.161
	Note: By default, the TS7650 servers use the IP address range 10.0.0.50 through 10.0.0.59 for the power control network. The server IP addresses do not change from frame to frame.			
	Server A	eth1	Cluster network 1	10.0.0.51
	Server A	eth2	Replication network 1	192.168.20.1
	Server A	eth3	RAS	172.31.1.xx
	Server A	eth4	Cluster network 2	10.0.0.51
	Server A	eth5	Replication network 2	192.168.21.1
	Network Power Switch	N/A		10.0.0.50

Table 18. Factory-default server IP addresses for a clustered VTL ProtecTIER system (3958 DD5) (continued)

TS7650 clustered VTL system	Component	Port	Function	Factory Default IP Address
Node B (the server located in the upper part of the rack)	Server B	eth0	Customer local LAN	192.168.10.162
	Note: By default, the TS7650 servers use the IP address range 10.0.0.50 through 10.0.0.59, for the power control network. The server IP addresses do not change from frame to frame.			
	Server B	eth1	Cluster network 1	10.0.0.52
	Server B	eth2	Replication network 1	192.168.20.2
	Server B	eth3	RAS	172.31.1.xx
	Server B	eth4	Cluster network 2	10.0.0.52
	Server B	eth5	Replication network 2	192.168.21.2
	Network Power Switch	N/A		10.0.0.50

Customer IP addresses

Table 19. Customer IP addresses

Node A (the server located in the lower part of the rack)	**Port**	**Host Name**	**IP Address**	**Network Mask**	**Default Gateway**
	eth0				
Node B (the server located in the upper part of the rack)	**Port**		**IP Address**	**Network Mask**	**Default Gateway**
	eth0				

Customer and Replication IP addresses

Table 20. Customer and Replication IP addresses for VTL

Default gateways for eth2 and eth5 for VTL systems, eth2 and eth13 for 1 Gb FSI systems, or eth2 and eth 9 for 10 Gb FSI systems should be different, otherwise the vlans are meaningless. For VTL systems, provide a routing path from the IP address on eth2-site1 to the IP address of eth2-site2, and a routing path from the IP address on eth5-site1 to the IP address of eth5-site2. For FSI systems, provide a routing path from the IP address on eth2-site1 to the IP address of eth2-site2, and a routing path from the IP address on eth9-site1 to the IP address of eth9-site2.					
Source Site					
Node A (the server located in the lower part of the rack)	**Port**	**IP Address**	**Network Mask**	**Default Gateway**	**Dedicated VLAN**
	eth2 for VTL systems and FSI systems				
	eth5 for VTL systems, eth13 for 1 GB FSI systems, or eth9 for 10 GB FSI systems				

Table 20. Customer and Replication IP addresses for VTL (continued)

Node B (the server located in the upper part of the rack)	**Port**	**IP Address**	**Network Mask**	**Default Gateway**	**Dedicated VLAN**
	eth2 for VTL systems and FSI systems				
	eth5 for VTL systems				
Destination or Target Site					
Node A (the server located in the lower part of the rack)	**Port**	**IP Address**	**Network Mask**	**Default Gateway**	**Dedicated VLAN**
	eth2 for VTL systems and FSI systems				
	eth5 for VTL systems, eth13 for 1 GB FSI systems, or eth9 for 10 GB FSI systems				
Node B (the server located in the upper part of the rack)	**Port**	**IP Address**	**Network Mask**	**Default Gateway**	**Dedicated VLAN**
	eth2 for VTL systems				
	eth5 for VTL systems				

Host names and DNS settings for setting up the TSSC with the TS7650G

Note: TSSC is not supported on 3958 DD6 servers.

Table 21. Host names and DNS settings for setting up the TSSC with the TS7650G

Item or setting	Instructions	eth0	eth1 (if applicable)
Source host name _____	Record the console or host name that you want to assign to the management console workstation (for example, **dsve1**). The console name and the domain are used to identify the TS7650G to the network.	IP address (client) #1: _____	IP address #1 (client): _____
		IP address #2 (service): _____	IP address #2 (service): _____
Domain name	Provide the domain name that you are assigning to the TSSC (for example, **medina.xyz.it**).		
Ethernet settings Complete the LAN Adapter Details section when the TSSC connects to your LAN.			

Table 21. Host names and DNS settings for setting up the TSSC with the TS7650G (continued)

Item or setting	Instructions	eth0	eth1 (if applicable)
Media speed (Ethernet)	Check **Autodetection** or the media speed of the Ethernet adapter.	_ **Autodetection** _ 10Mpbs Half Duplex _ 10Mpbs Full Duplex _ 100Mpbs Half Duplx _ 100Mpbs Full Duplx _ 1000Mpbs Half Duplx _ 1000Mpbs Full Duplx	_ **Autodetection** _ 10Mpbs Half Duplex _ 10Mpbs Full Duplex _ 100Mpbs Half Duplx _ 100Mpbs Full Duplx _ 1000Mpbs Half Duplx _ 1000Mpbs Full Duplx
TCP/IP interface network mask	Record the dotted decimal network mask that you want to apply to the TCP/IP address (for example, **127.123.546.0**).		
DNS settings: Complete this section if you plan to use a domain name server (DNS) to resolve network names.			
Name server (DNS) internet address 1	Provide the dotted decimal address of the name server that the TSSC will access (for example, **5.127.42.250**).		
Name server domain name 1	Provide the domain name of the name server (for example, **medina.xyz.it**).		
Name server (DNS) internet address 2 (Optional)	Provide the dotted decimal address of the second name server that this workstation can access (for example, **5.127.42.252**). Although this is optional, you can specify a second name server when you configure a backup or secondary server.		
Name server domain name 2	If you have a second name server, provide the domain name of the second name server (for example, **medina2.xyz.it**).		
Routing settings: Complete the following section if you want to specify a default gateway for routing.			
Gateway address	Confirm and record the dotted decimal or symbolic name address of the gateway (for example, **8.127.155.254** or londongate).		

BMC IP addresses

Note: BMC is only supported on 3958 DD6 servers.

Table 22. BMC IP addresses

Node	Ethernet Port	Default IP Address	Customer Assigned IP Address
Node A (the server located in the lower part of the rack)	eth2	192.168.10.163	
Node B (the server located in the upper part of the rack)	eth2	192.168.10.64	

TSSC IP addresses

Note: TSSC is not supported on 3958 DD6 servers.

Table 23. TSSC IP addresses

TSSC	Ethernet Port	Default IP Address	Customer Assigned IP Address
TSSC	External	N/A	
TSSC	Internal	172.31.1.1 (fixed, do not change)	N/A

Electronic Customer Care (ECC) IP addresses

Table 24. ECC IP addresses

Host name	IP address	Port	Description
Edge	• 129.42.56.189 • 129.42.60.189 • 129.42.54.189	80	Edge replaces IP addresses needed for Service Providers, Download Servers, Upload Servers and CCF, but not FTP.
esupport.ibm.com	• 2620:0:6c0:200:129:42:56:189 • 2620:0:6c2:200:129:42:60:189 • 2620:0:6c4:200:129:42:54:189	443, 80 (optional)	We recommend customers open 129.42.0.0/18 (EI IPv4 address range) and 2620:0:6c0::/45 (EI IPv6 address range) for the least amount of hassle going forward.

Appendix C. Connect to BMC using a web-browser

This topic provides instructions for connecting to Baseboard Management Controller with a web-browser.

Procedure

1. Connect your computer to the ProtecTIER canister using the Ethernet cable from the ProtecTIER canister to the computer with the fixed IP setup (192.168.10.160).

   Note: The BMC port is the port on the far right of the ProtecTIER canister.
2. Start BMC in a Web Browser (Mozilla Firefox or Microsoft Internet Explorer) using the IP address configured in the BMC interface, in this case the default BMC IP address is 192.168.10.163 for the lower node and 192.168.10.164 for the upper node in case you have a clustered environment.

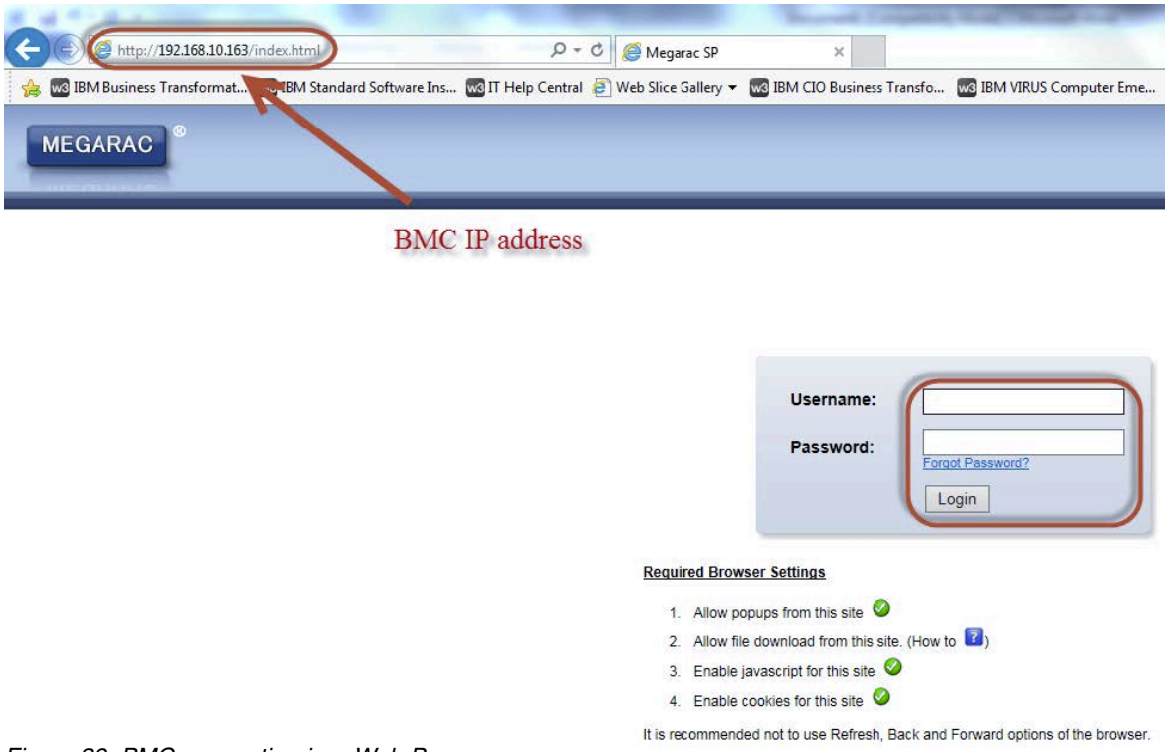


Figure 39. BMC connection in a Web Browser

3. Log in to the BMC interface. At the login prompt, log in with the ID `admin` and the password `admin`.
4. Select **Remote Control** > **Console Redirection**.
   The Console Redirection Page is displayed.

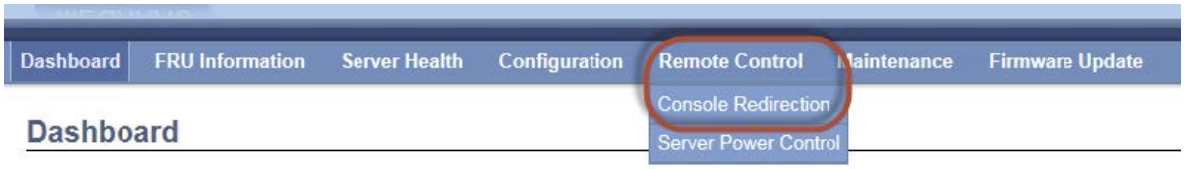


Figure 40. Console redirect menu

5. Click **Java Console** to launch the redirection console.

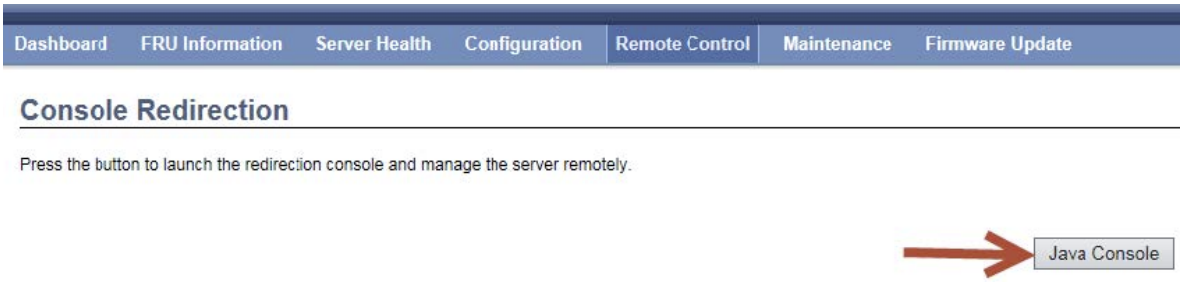
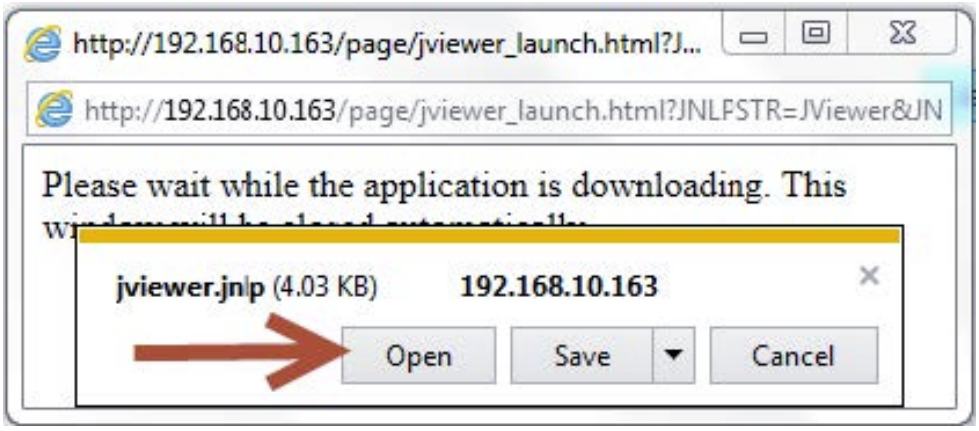


Figure 41. Console Redirection page

6. Click **Open** in the dialog-box displayed.



7. If a security warning is displayed, click **Allow** to continue.

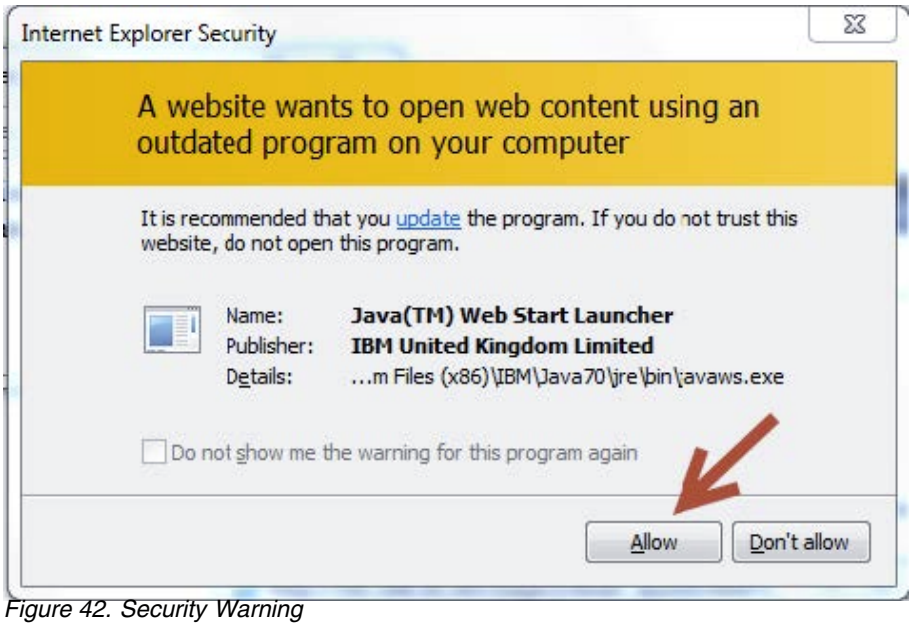


Figure 42. Security Warning

8. Another security warning will appear, click the checkbox to accept the security risk and then click **Execute** to continue.

9. You are connected to the system. If a blank screen is displayed, press **Enter** to refresh the view and obtain a video signal from the system.

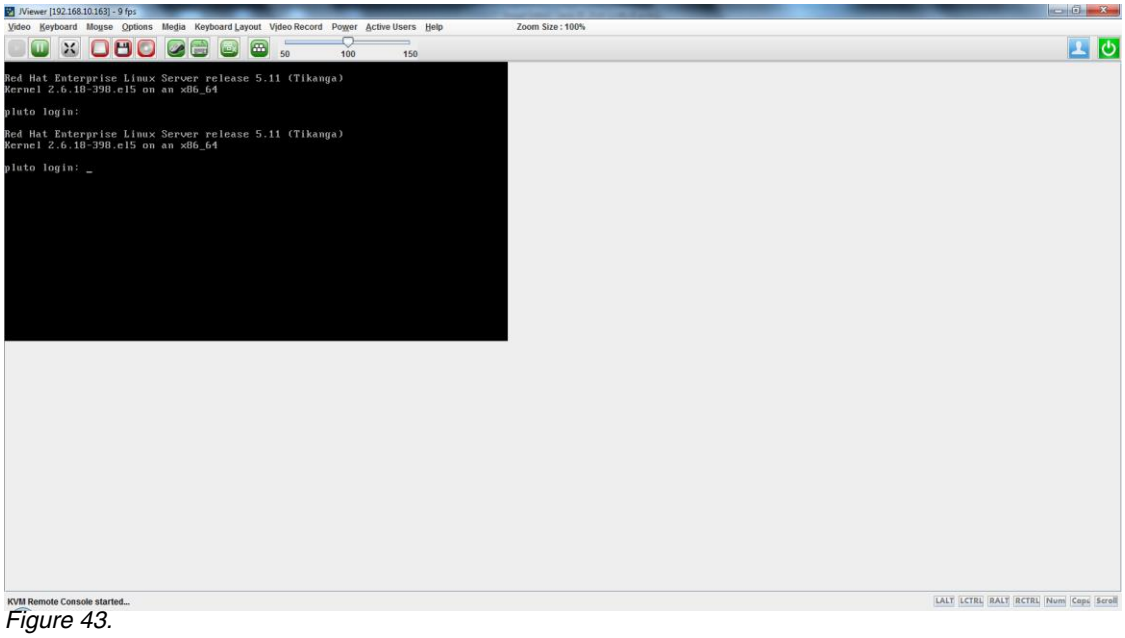


Figure 43.

10. Select Option in the pop-up message bar to allow pop-up windows in the browser.
11. Select **Allow pop-ups for 9.11.243.44**.

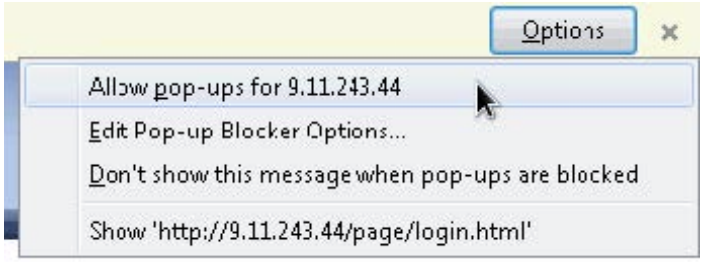


Figure 44. Firefox Options menu

Results

You are now connected to the BMC interface through your Web Browser.

Direct connection with a USB keyboard and monitor

Procedure

1. Connect a USB keyboard and graphics-capable monitor to Server B.
2. Log in to the server. See steps 2 on page 42 through 3 on page 43 of Chapter 5, “Configuring Server A,” on page 39 for the login procedure.
3. At the command prompt, type `reboot` and press Enter.
4. When the IBM logo displays, press `F1` to enter **Setup** mode.
5. Select **System Settings** > **Integrated Management Module** > **Network Configuration**.
6. Locate the current IMM IP address.

7. Change the last octet of the static IP address to a value that is lower than the default of 254. For example: `172.31.1.253`.
8. In the **Netmask** field, enter `255.255.255.0`.
9. Leave the **Gateway** field blank.
10. Ensure that use of the **static IP address** is specified.
11. Select **Save the Network Changes** and then press Enter.
12. Press Esc.
13. Select **Save Settings**.
14. Select **Exit Setup**. Server B restarts with the value that you specified for the IMM IP address.

Appendix D. Worldwide time zone codes

Use the information in the following table to help you set the system's time zone.

Time zone codes

The following table lists all of the worldwide time zone codes and the associated time zone descriptions. Additional information about the time zone is located in the Comments column.

Code	Time zone	Comments
AD	Europe/Andorra	
AE	Asia/Dubai	
AF	Asia/Kabul	
AG	America/Antigua	
AI	America/Anguilla	
AL	Europe/Tirane	
AM	Asia/Yerevan	
AN	America/Curacao	
AO	Africa/Luanda	
AQ	Antarctica/McMurdo	McMurdo Station, Ross Island
AQ	Antarctica/South_Pole	Amundsen-Scott Station, South Pole
AQ	Antarctica/Rothera	Rothera Station, Adelaide Island
AQ	Antarctica/Palmer	Palmer Station, Anvers Island
AQ	Antarctica/Mawson	Mawson Station, Holme Bay
AQ	Antarctica/Davis	Davis Station, Vestfold Hills
AQ	Antarctica/Casey	Casey Station, Bailey Peninsula
AQ	Antarctica/Vostok	Vostok Station, S Magnetic Pole
AQ	Antarctica/DumontDUrville	Dumont-d'Urville Station, Terre Adelie
AQ	Antarctica/Syowa	Syowa Station, E Ongul I
AR	America/Argentina/Buenos_Aires	Buenos Aires (BA, CF)
AR	America/Argentina/Cordoba	most locations (CB, CC, CN, ER, FM, LP, MN, NQ, RN, SA, SE, SF, SL)
AR	America/Argentina/Jujuy	Jujuy (JY)
AR	America/Argentina/Tucuman	Tucuman (TM)
AR	America/Argentina/Catamarca	Catamarca (CT), Chubut (CH)
AR	America/Argentina/La_Rioja	La Rioja (LR)
AR	America/Argentina/San_Juan	San Juan (SJ)
AR	America/Argentina/Mendoza	Mendoza (MZ)
AR	America/Argentina/Rio_Gallegos	Santa Cruz (SC)
AR	America/Argentina/Ushuaia	Tierra del Fuego (TF)
AS	Pacific/Pago_Pago	

Code	Time zone	Comments
AT	Europe/Vienna	
AU	Australia/Lord_Howe	Lord Howe Island
AU	Australia/Hobart	Tasmania - most locations
AU	Australia/Currie	Tasmania - King Island
AU	Australia/Melbourne	Victoria
AU	Australia/Sydney	New South Wales - most locations
AU	Australia/Broken_Hill	New South Wales - Yancowinna
AU	Australia/Brisbane	Queensland - most locations
AU	Australia/Lindeman	Queensland - Holiday Islands
AU	Australia/Adelaide	South Australia
AU	Australia/Darwin	Northern Territory
AU	Australia/Perth	Western Australia - most locations
AU	Australia/Eucla	Western Australia - Eucla area
AW	America/Aruba	
AX	Europe/Mariehamn	
AZ	Asia/Baku	
BA	Europe/Sarajevo	
BB	America/Barbados	
BD	Asia/Dhaka	
BE	Europe/Brussels	
BF	Africa/Ouagadougou	
BG	Europe/Sofia	
BH	Asia/Bahrain	
BI	Africa/Bujumbura	
BJ	Africa/Porto-Novo	
BL	America/St_Barthelemy	
BM	Atlantic/Bermuda	
BN	Asia/Brunei	
BO	America/La_Paz	
BR	America/Noronha	Atlantic islands
BR	America/Belem	Amapa, E Para
BR	America/Fortaleza	NE Brazil (MA, PI, CE, RN, PB)
BR	America/Recife	Pernambuco
BR	America/Araguaina	Tocantins
BR	America/Maceio	Alagoas, Sergipe
BR	America/Bahia	Bahia
BR	America/Sao_Paulo	S & SE Brazil (GO, DF, MG, ES, RJ, SP, PR, SC, RS)
BR	America/Campo_Grande	Mato Grosso do Sul
BR	America/Cuiaba	Mato Grosso
BR	America/Porto_Velho	W Para, Rondonia
BR	America/Boa_Vista	Roraima

Code	Time zone	Comments
BR	America/Manaus	E Amazonas
BR	America/Eirunepe	W Amazonas
BR	America/Rio_Branco	Acre
BS	America/Nassau	
BT	Asia/Thimphu	
BW	Africa/Gaborone	
BY	Europe/Minsk	
BZ	America/Belize	
CA	America/St_Johns	Newfoundland Time, including SE Labrador
CA	America/Halifax	Atlantic Time - Nova Scotia (most places), PEI
CA	America/Glace_Bay	Atlantic Time - Nova Scotia - places that did not observe DST 1966-1971
CA	America/Moncton	Atlantic Time - New Brunswick
CA	America/Goose_Bay	Atlantic Time - Labrador - most locations
CA	America/Blanc-Sablon	Atlantic Standard Time - Quebec - Lower North Shore
CA	America/Montreal	Eastern Time - Quebec - most locations
CA	America/Toronto	Eastern Time - Ontario - most locations
CA	America/Nipigon	Eastern Time - Ontario & Quebec - places that did not observe DST 1967-1973
CA	America/Thunder_Bay	Eastern Time - Thunder Bay, Ontario
CA	America/Iqaluit	Eastern Time - east Nunavut - most locations
CA	America/Pangnirtung	Eastern Time - Pangnirtung, Nunavut
CA	America/Resolute	Eastern Time - Resolute, Nunavut
CA	America/Atikokan	Eastern Standard Time - Atikokan, Ontario and Southampton I, Nunavut
CA	America/Rankin_Inlet	Central Time - central Nunavut
CA	America/Winnipeg	Central Time - Manitoba & west Ontario
CA	America/Rainy_River	Central Time - Rainy River & Fort Frances, Ontario
CA	America/Regina	Central Standard Time - Saskatchewan - most locations
CA	America/Swift_Current	Central Standard Time - Saskatchewan - midwest
CA	America/Edmonton	Mountain Time - Alberta, east British Columbia & west Saskatchewan
CA	America/Cambridge_Bay	Mountain Time - west Nunavut
CA	America/Yellowknife	Mountain Time - central Northwest Territories
CA	America/Inuvik	Mountain Time - west Northwest Territories
CA	America/Dawson_Creek	Mountain Standard Time - Dawson Creek & Fort Saint John, British Columbia
CA	America/Vancouver	Pacific Time - west British Columbia
CA	America/Whitehorse	Pacific Time - south Yukon
CA	America/Dawson	Pacific Time - north Yukon
CC	Indian/Cocos	

Code	Time zone	Comments
CD	Africa/Kinshasa	west Dem. Rep. of Congo
CD	Africa/Lubumbashi	east Dem. Rep. of Congo
CF	Africa/Bangui	
CG	Africa/Brazzaville	
CH	Europe/Zurich	
CI	Africa/Abidjan	
CK	Pacific/Rarotonga	
CL	America/Santiago	most locations
CL	Pacific/Easter	Easter Island & Sala y Gomez
CM	Africa/Douala	
CN	Asia/Shanghai	east China - Beijing, Guangdong, Shanghai, etc.
CN	Asia/Harbin	Heilongjiang (except Mohe), Jilin
CN	Asia/Chongqing	central China - Sichuan, Yunnan, Guangxi, Shaanxi, Guizhou, etc.
CN	Asia/Urumqi	most of Tibet & Xinjiang
CN	Asia/Kashgar	west Tibet & Xinjiang
CO	America/Bogota	
CR	America/Costa_Rica	
CU	America/Havana	
CV	Atlantic/Cape_Verde	
CX	Indian/Christmas	
CY	Asia/Nicosia	
CZ	Europe/Prague	
DE	Europe/Berlin	
DJ	Africa/Djibouti	
DK	Europe/Copenhagen	
DM	America/Dominica	
DO	America/Santo_Domingo	
DZ	Africa/Algiers	
EC	America/Guayaquil	mainland
EC	Pacific/Galapagos	Galapagos Islands
EE	Europe/Tallinn	
EG	Africa/Cairo	
EH	Africa/El_Aaiun	
ER	Africa/Asmara	
ES	Europe/Madrid	mainland
ES	Africa/Ceuta	Ceuta & Melilla
ES	Atlantic/Canary	Canary Islands
ET	Africa/Addis_Ababa	
FI	Europe/Helsinki	
FJ	Pacific/Fiji	

Code	Time zone	Comments
FK	Atlantic/Stanley	
FM	Pacific/Truk	Truk (Chuuk) and Yap
FM	Pacific/Ponape	Ponape (Pohnpei)
FM	Pacific/Kosrae	Kosrae
FO	Atlantic/Faroe	
FR	Europe/Paris	
GA	Africa/Libreville	
GB	Europe/London	
GD	America/Grenada	
GE	Asia/Tbilisi	
GF	America/Cayenne	
GG	Europe/Guernsey	
GH	Africa/Accra	
GI	Europe/Gibraltar	
GL	America/Godthab	most locations
GL	America/Danmarkshavn	east coast, north of Scoresbysund
GL	America/Scoresbysund	Scoresbysund / Ittoqqortoormiit
GL	America/Thule	Thule / Pituffik
GM	Africa/Banjul	
GN	Africa/Conakry	
GP	America/Guadeloupe	
GQ	Africa/Malabo	
GR	Europe/Athens	
GS	Atlantic/South_Georgia	
GT	America/Guatemala	
GU	Pacific/Guam	
GW	Africa/Bissau	
GY	America/Guyana	
HK	Asia/Hong_Kong	
HN	America/Tegucigalpa	
HR	Europe/Zagreb	
HT	America/Port-au-Prince	
HU	Europe/Budapest	
ID	Asia/Jakarta	Java & Sumatra
ID	Asia/Pontianak	west & central Borneo
ID	Asia/Makassar	east & south Borneo, Celebes, Bali, Nusa Tengarra, west Timor
ID	Asia/Jayapura	Irian Jaya & the Moluccas
IE	Europe/Dublin	
IL	Asia/Jerusalem	
IM	Europe/Isle_of_Man	

Code	Time zone	Comments
IN	Asia/Calcutta	
IO	Indian/Chagos	
IQ	Asia/Baghdad	
IR	Asia/Tehran	
IS	Atlantic/Reykjavik	
IT	Europe/Rome	
JE	Europe/Jersey	
JM	America/Jamaica	
JO	Asia/Amman	
JP	Asia/Tokyo	
KE	Africa/Nairobi	
KG	Asia/Bishkek	
KH	Asia/Phnom_Penh	
KI	Pacific/Tarawa	Gilbert Islands
KI	Pacific/Enderbury	Phoenix Islands
KI	Pacific/Kiritimati	Line Islands
KM	Indian/Comoro	
KN	America/St_Kitts	
KP	Asia/Pyongyang	
KR	Asia/Seoul	
KW	Asia/Kuwait	
KY	America/Cayman	
KZ	Asia/Almaty	most locations
KZ	Asia/Qyzylorda	Qyzylorda (Kyzylorda, Kzyl-Orda)
KZ	Asia/Aqtobe	Aqtobe (Aktobe)
KZ	Asia/Aqtau	Atyrau (Atirau, Gur'yev), Mangghystau (Mankistau)
KZ	Asia/Oral	West Kazakhstan
LA	Asia/Vientiane	
LB	Asia/Beirut	
LC	America/St_Lucia	
LI	Europe/Vaduz	
LK	Asia/Colombo	
LR	Africa/Monrovia	
LS	Africa/Maseru	
LT	Europe/Vilnius	
LU	Europe/Luxembourg	
LV	Europe/Riga	
LY	Africa/Tripoli	
MA	Africa/Casablanca	
MC	Europe/Monaco	
MD	Europe/Chisinau	

Code	Time zone	Comments
ME	Europe/Podgorica	
MF	America/Marigot	
MG	Indian/Antananarivo	
MH	Pacific/Majuro	most locations
MH	Pacific/Kwajalein	Kwajalein
MK	Europe/Skopje	
ML	Africa/Bamako	
MM	Asia/Rangoon	
MN	Asia/Ulaanbaatar	most locations
MN	Asia/Hovd	Bayan-Olgiy, Govi-Altai, Hovd, Uvs, Zavkhan
MN	Asia/Choibalsan	Dornod, Sukhbaatar
MO	Asia/Macau	
MP	Pacific/Saipan	
MQ	America/Martinique	
MR	Africa/Nouakchott	
MS	America/Montserrat	
MT	Europe/Malta	
MU	Indian/Mauritius	
MV	Indian/Maldives	
MW	Africa/Blantyre	
MX	America/Mexico_City	Central Time - most locations
MX	America/Cancun	Central Time - Quintana Roo
MX	America/Merida	Central Time - Campeche, Yucatan
MX	America/Monterrey	Central Time - Coahuila, Durango, Nuevo Leon, Tamaulipas
MX	America/Mazatlan	Mountain Time - S Baja, Nayarit, Sinaloa
MX	America/Chihuahua	Mountain Time - Chihuahua
MX	America/Hermosillo	Mountain Standard Time - Sonora
MX	America/Tijuana	Pacific Time
MY	Asia/Kuala_Lumpur	peninsular Malaysia
MY	Asia/Kuching	Sabah & Sarawak
MZ	Africa/Maputo	
NA	Africa/Windhoek	
NC	Pacific/Noumea	
NE	Africa/Niamey	
NF	Pacific/Norfolk	
NG	Africa/Lagos	
NI	America/Managua	
NL	Europe/Amsterdam	
NO	Europe/Oslo	
NP	Asia/Katmandu	

Code	Time zone	Comments
NR	Pacific/Nauru	
NU	Pacific/Niue	
NZ	Pacific/Auckland	most locations
NZ	Pacific/Chatham	Chatham Islands
OM	Asia/Muscat	
PA	America/Panama	
PE	America/Lima	
PF	Pacific/Tahiti	Society Islands
PF	Pacific/Marquesas	Marquesas Islands
PF	Pacific/Gambier	Gambier Islands
PG	Pacific/Port_Moresby	
PH	Asia/Manila	
PK	Asia/Karachi	
PL	Europe/Warsaw	
PM	America/Miquelon	
PN	Pacific/Pitcairn	
PR	America/Puerto_Rico	
PS	Asia/Gaza	
PT	Europe/Lisbon	mainland
PT	Atlantic/Madeira	Madeira Islands
PT	Atlantic/Azores	Azores
PW	Pacific/Palau	
PY	America/Asuncion	
QA	Asia/Qatar	
RE	Indian/Reunion	
RO	Europe/Bucharest	
RS	Europe/Belgrade	
RU	Europe/Kaliningrad	Moscow-01 - Kaliningrad
RU	Europe/Moscow	Moscow+00 - west Russia
RU	Europe/Volgograd	Moscow+00 - Caspian Sea
RU	Europe/Samara	Moscow+01 - Samara, Udmurtia
RU	Asia/Yekaterinburg	Moscow+02 - Urals
RU	Asia/Omsk	Moscow+03 - west Siberia
RU	Asia/Novosibirsk	Moscow+03 - Novosibirsk
RU	Asia/Krasnoyarsk	Moscow+04 - Yenisei River
RU	Asia/Irkutsk	Moscow+05 - Lake Baikal
RU	Asia/Yakutsk	Moscow+06 - Lena River
RU	Asia/Vladivostok	Moscow+07 - Amur River
RU	Asia/Sakhalin	Moscow+07 - Sakhalin Island
RU	Asia/Magadan	Moscow+08 - Magadan
RU	Asia/Kamchatka	Moscow+09 - Kamchatka

Code	Time zone	Comments
RU	Asia/Anadyr	Moscow+10 - Bering Sea
RW	Africa/Kigali	
SA	Asia/Riyadh	
SB	Pacific/Guadalcanal	
SC	Indian/Mahe	
SD	Africa/Khartoum	
SE	Europe/Stockholm	
SG	Asia/Singapore	
SH	Atlantic/St_Helena	
SI	Europe/Ljubljana	
SJ	Arctic/Longyearbyen	
SK	Europe/Bratislava	
SL	Africa/Freetown	
SM	Europe/San_Marino	
SN	Africa/Dakar	
SO	Africa/Mogadishu	
SR	America/Paramaribo	
ST	Africa/Sao_Tome	
SV	America/El_Salvador	
SY	Asia/Damascus	
SZ	Africa/Mbabane	
TC	America/Grand_Turk	
TD	Africa/Ndjamena	
TF	Indian/Kerguelen	
TG	Africa/Lome	
TH	Asia/Bangkok	
TJ	Asia/Dushanbe	
TK	Pacific/Fakaofo	
TL	Asia/Dili	
TM	Asia/Ashgabat	
TN	Africa/Tunis	
TO	Pacific/Tongatapu	
TR	Europe/Istanbul	
TT	America/Port_of_Spain	
TV	Pacific/Funafuti	
TW	Asia/Taipei	
TZ	Africa/Dar_es_Salaam	
UA	Europe/Kiev	most locations
UA	Europe/Uzhgorod	Ruthenia
UA	Europe/Zaporozhye	Zaporozh'ye, E Lugansk / Zaporizhia, E Luhansk
UA	Europe/Simferopol	central Crimea

Code	Time zone	Comments
UG	Africa/Kampala	
UM	Pacific/Johnston	Johnston Atoll
UM	Pacific/Midway	Midway Islands
UM	Pacific/Wake	Wake Island
US	America/New_York	Eastern Time
US	America/Detroit	Eastern Time - Michigan - most locations
US	America/Kentucky/Louisville	Eastern Time - Kentucky - Louisville area
US	America/Kentucky/Monticello	Eastern Time - Kentucky - Wayne County
US	America/Indiana/Indianapolis	Eastern Time - Indiana - most locations
US	America/Indiana/Vincennes	Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties
US	America/Indiana/Knox	Eastern Time - Indiana - Starke County
US	America/Indiana/Winamac	Eastern Time - Indiana - Pulaski County
US	America/Indiana/Marengo	Eastern Time - Indiana - Crawford County
US	America/Indiana/Vevay	Eastern Time - Indiana - Switzerland County
US	America/Chicago	Central Time
US	America/Indiana/Tell_City	Central Time - Indiana - Perry County
US	America/Indiana/Petersburg	Central Time - Indiana - Pike County
US	America/Menominee	Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties
US	America/North_Dakota/Center	Central Time - North Dakota - Oliver County
US	America/North_Dakota/New_Salem	Central Time - North Dakota - Morton County (except Mandan area)
US	America/Denver	Mountain Time
US	America/Boise	Mountain Time - south Idaho & east Oregon
US	America/Shiprock	Mountain Time - Navajo
US	America/Phoenix	Mountain Standard Time - Arizona
US	America/Los_Angeles	Pacific Time
US	America/Anchorage	Alaska Time
US	America/Juneau	Alaska Time - Alaska panhandle
US	America/Yakutat	Alaska Time - Alaska panhandle neck
US	America/Nome	Alaska Time - west Alaska
US	America/Adak	Aleutian Islands
US	Pacific/Honolulu	Hawaii
UY	America/Montevideo	
UZ	Asia/Samarkand	west Uzbekistan
UZ	Asia/Tashkent	east Uzbekistan
VA	Europe/Vatican	
VC	America/St_Vincent	
VE	America/Caracas	
VG	America/Tortola	
VI	America/St_Thomas	

Code	Time zone	Comments
VN	Asia/Saigon	
VU	Pacific/Efate	
WF	Pacific/Wallis	
WS	Pacific/Apia	
YE	Asia/Aden	
YT	Indian/Mayotte	
ZA	Africa/Johannesburg	
ZM	Africa/Lusaka	
ZW	Africa/Harare	

Appendix E. ProtecTIER Manager common tasks

Running the ProtecTIER Manager application TS7600 ProtecTIER Deduplication Solutions, V3.4.3

This task describes how to run the ProtecTIER Manager software on the ProtecTIER Manager workstation.

About this task

The ProtecTIER Manager GUI can be run from either a Windows based, or a Linux based ProtecTIER Manager workstation.

Procedure

1. Run the ProtecTIER Manager application:
   - On a Windows-based ProtecTIER Manager workstation, run the ProtecTIER Manager application:

     Click **Start > Programs > IBM > ProtecTIER Manager > IBM ProtecTIER Manager**.
   - On a Linux-based ProtecTIER Manager workstation:
     a. Navigate to the directory where you installed ProtecTIER Manager. The default installation directory is: **/opt/IBM/PTManager**.
     b. Double-click the ProtecTIER Manager icon.

   The **ProtecTIER Manager** window is displayed.
2. Go on to .
3. Go on to "Managing nodes and clusters."

Managing nodes and clusters

The ProtecTIER system supports both one-node systems (stand-alone) and two-node (clustered) configurations. A clustered configuration enables higher throughput and provides higher availability in the event of node failure. When ProtecTIER Manager restarts, it automatically detects all nodes on the added subnetworks of the Internet Protocol network. Removing a node stops ProtecTIER Manager from registering the node and being able to manage it. The node and the associated cluster are unaffected by removing a node in this way. If you remove a node that is associated with a two-node cluster, the second node is also removed.

Adding and removing nodes from ProtecTIER Manager

The topics in this section describe how to add a node, a subnetwork node, and remove a node from the ProtecTIER system using the ProtecTIER Manager.

Note: This section provides instructions for adding and removing nodes when using the TS7650G.

Adding a node registers the node IP address and port number with the instance of ProtecTIER Manager at your workstation. Similarly, removing a node removes the node registration from ProtecTIER Manager at that workstation.

Adding nodes

Complete this task to add a node to your ProtecTIER system with ProtecTIER Manager.

About this task

Adding a node registers the node IP address and port number with the instance of ProtecTIER Manager at your workstation.

To add a node to your ProtecTIER system:

Procedure

1. Run the ProtecTIER Manager application:
   - For a Windows-based ProtecTIER Manager workstation, run the ProtecTIER Manager application:

     Click **Start > Programs > IBM > ProtecTIER Manager > IBM ProtecTIER Manager**.
   - For a Linux-based ProtecTIER Manager workstation, click the icon for ProtecTIER Manager on the Desktop or the location of the shortcut specified during the installation.

   The **ProtecTIER Manager** window is displayed.
2. From the Systems Management view, click the **Add new node** button on the toolbar located at the top of the **ProtecTIER Manager** window. The **Add new node** dialog box is displayed, prompting you for the IP address and Port number of the node that you want to add.
3. Enter the IP address of the node and click **Ok**. The node is displayed in the **Navigation** pane and the **Login** button is displayed in the **View** pane.

   Note: Do not change the port number of the node unless directed to do so by trained ProtecTIER specialist.

Adding node subnetworks

This topic describes how to add a node subnetwork to your ProtecTIER system with the ProtecTIER Manager.

About this task

In addition to adding individual nodes to ProtecTIER Manager, you can add addresses for subnetworks to which nodes are connected. When ProtecTIER Manager restarts, it automatically detects all nodes on the added subnetworks of the TCP/IP network.

Procedure

1. Click on the **Auto discovery** tab.
2. For each subnetwork you want to add, click a **Sub network** check box and enter the subnetwork address in the corresponding field.
3. Click **Ok**. The **Preferences** dialog box closes and the subnetwork address is added to the ProtecTIER Manager. When you restart the ProtecTIER Manager, all nodes on the defined subnetwork addresses are automatically added to the ProtecTIER Manager.

Removing nodes

This topic describes how to remove a node from your ProtecTIER system using the ProtecTIER Manager.

About this task

Removing a node stops the instance of ProtecTIER Manager at your workstation from registering the node and being able to manage it. The node itself is unaffected by removing a node in this way.

Perform the following steps to remove a node from ProtecTIER Manager:

Note: Do not log in to the node you want to remove or you will be unable to perform this operation.

Procedure

1. From the**Select a system** dropdown list in the Systems Management view, choose the system from which you want to disconnect.
2. Select **Node** > **Remove node**. A confirmation message box is displayed to remove the connection.
3. Click **Yes**. The node is removed.

Customizing the network configuration of a node

This topic describes how to use the Network Configuration window in ProtecTIER Manager to customize the IP communication interfaces on a node.

About this task

The Network Configuration window lets you reassign the IP communication interfaces to group several physical interfaces into a single virtual interface, and create a bond configuration of several physical interfaces. The IP communication interfaces can also be reassigned using the ProtecTIER Service menu. See Chapter 5, “Configuring Server A,” on page 39.

Procedure

1. From the Systems Management view, select **Node** > **Network configuration**. The **Network configuration** window is displayed:

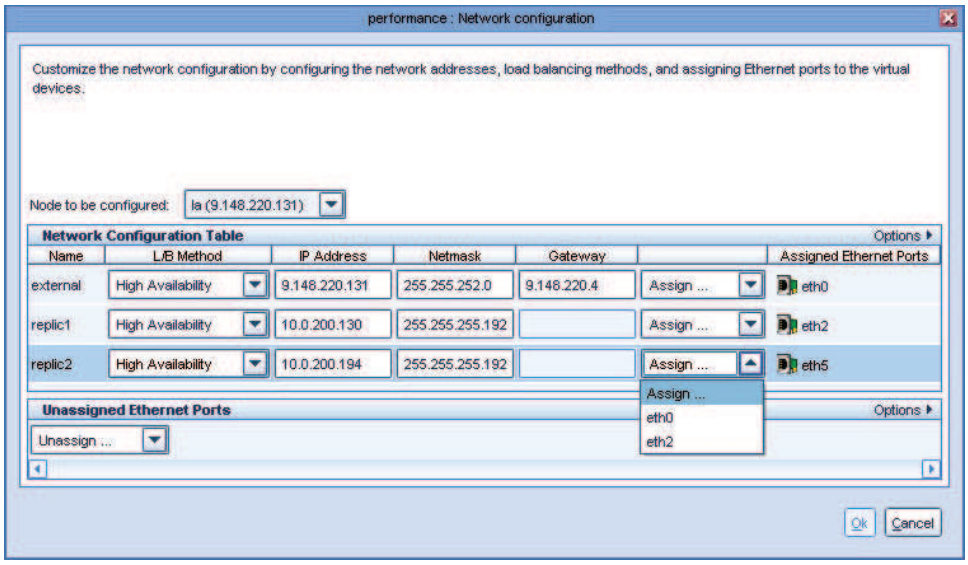


Figure 45. Configure IP interfaces window

2. Select a node from the **Node to be configured** field.
3. Highlight the virtual interface you wish to edit.
4. Click on the dropdown in the **L/B Method** column to select the load balancing method. The available load balancing methods are displayed:

   RR (Round-robin)
   Outgoing traffic is spread evenly across all of the adapter ports in the bond

   L2 Outgoing traffic is spread using a default transmit hash policy of layer 2

   L2L3
   Outgoing traffic is spread using a transmit hash policy of MAC addresses and IP addresses of the source and the destination

   L3L4
   Outgoing traffic is spread using a transmit hash policy of IP addresses and ports of the source and the destination

   HA Active-backup policy: only one slave in the bond is active. A different slave becomes active if, and only if, the active slave fails.
5. Edit the **IP Address**, **Netmask** and **Gateway** addresses, as desired.
6. If you want to reassign a physical interface, select an Ethernet port from the ports available in the **Assign** field.
7. If you want to unassign a port, select the port to unassign from the **Unassigned Ethernet Ports** dropdown.
8. Click **Ok** to save the changes and exit the Network Configuration window.

Logging in and out of the ProtecTIER Manager application

Complete this task to log in to and log out of the ProtecTIER Manager application.

About this task

ProtecTIER Manager has default user accounts corresponding to three user permission levels: Administrator, Operator, and User. For more information, see “Permission levels” on page 133. The default username and password for each of these accounts are as follows:

Table 25. Default usernames and passwords

Permission Level	Default Username	Default Password
Administrator	ptadmin	ptadmin
Operator	ptoper	ptoper
User	ptuser	ptuser

Procedure

1. Click the **Login** button. The **Login** dialog box is displayed.
2. Enter your username and password.
3. Click **Ok**. The **Login** dialog box closes and ProtecTIER Manager displays the information for that node.

Results

IBM recommends that you change or replace these default user accounts. For more information, see "Managing users."

If you log in with Administrator level permission while another Administrator is already logged in, a message box is displayed with the following message:

```
Administrator is already logged in from host <host name>, at IP address:
<IP address>.
Would you like to login anyway?
```

Clicking **Yes** forces the other Administrator to logout.

Managing users

The topics in this section describe how to manage users of the ProtecTIER Manager system.

ProtecTIER Manager enables you to create user accounts with different permission levels for accessing and configuring your ProtecTIER system.

Permission levels

This topic describes the various user permission levels in the ProtecTIER Manager system.

The ProtecTIER system supports the following permission levels:

- **Administrator** has full access to the ProtecTIER system.

  Note: Only one Administrator can be logged in to the ProtecTIER system at a time. If you log in as an administrator while another administrator is already logged in, the system displays a notification pane. The notification pane lists the other administrator who is logged in, and offers to force that administrator to log out.
- **Operator** can access ProtecTIER Manager monitoring screens and perform limited tasks.
- **User** can access only ProtecTIER Manager monitoring screens.

Adding user accounts

This topic describes how to add a user account to ProtecTIER Manager.

About this task

Complete this task to add a new user account to the ProtecTIER Manager system.

Procedure

1. Log in to the ProtecTIER Manager system and choose **System > Manage Users**. The **Manage Users** dialog is displayed:

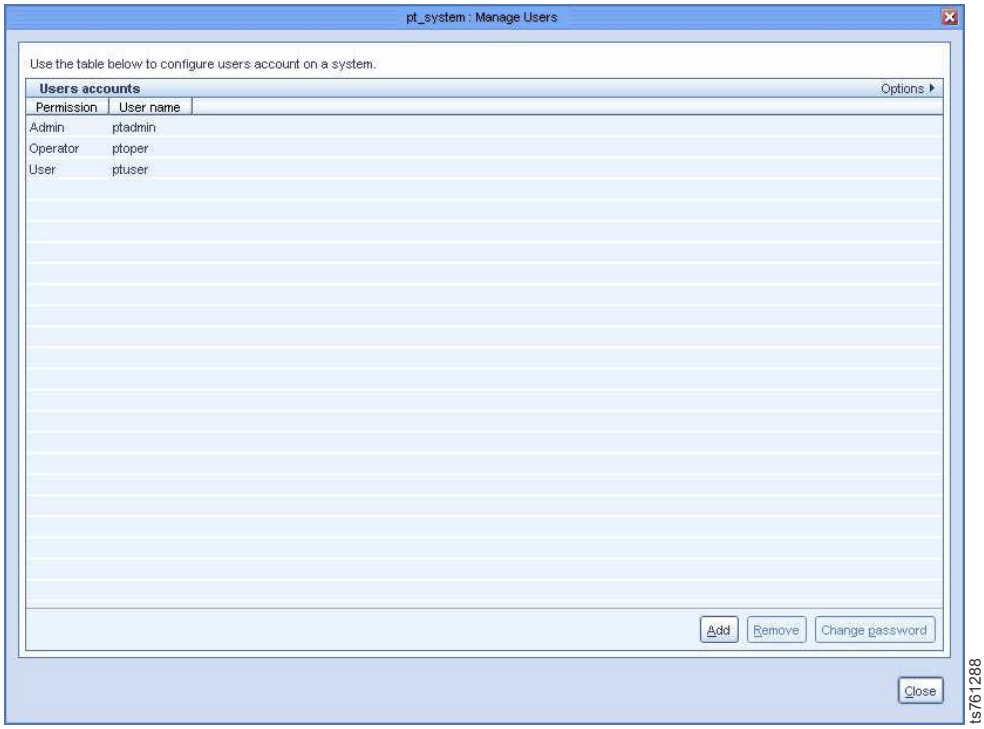


Figure 46. Manage Users dialog

2. Click **Add**. The **Add account** dialog is displayed.
3. In the **User name** field, enter a username for the account.
4. In the **New password** field, enter a password for the account.
5. In the **Verify password** field, reenter the password that you entered in the **New password** field.
6. In the **Permission** field, select a permission level (Administrator, Operator, or User) you want to assign to the user account.

   Note: Before processing, record this information in a manner that allows you to notify the new user. Remind the new user to record the password because you nor the system stores the passwords for later use.
7. Click **Ok**. The **Add account** dialog closes and the account is added to the ProtecTIER Manager system.
8. Click **Close** to exit the **Manage Users** window.

Changing the user account password

This topic describes how to change the password of a user account on the ProtecTIER Manager system.

About this task

Complete this task to change the user password in the ProtecTIER Manager system.

Procedure

1. Choose **System > Manage Users**. The **Manage Users** dialog is displayed.
2. Select a user account from the list and click **Change password**. The **Change password** dialog is displayed.
3. Type the current password in the **Password** field.
4. Type the new password in the **New password** field.
5. Type the new password again in the **Verify password** field.
6. Click **Ok**. The password for the selected user account is changed.
7. Click **Close** to exit the **Manage Users** window.

Changing the Support System settings

This topic explains how to change the support system settings.

About this task

The ProtecTIER Manager installation wizard and the ProtecTIER Manager application are fully compatible with the JAWS screen-reader software. ProtecTIER Manager also allows you to change other accessibility settings, such as the contrast resolution mode and color palette. Instructions for installing JAWS and the Java-based accessibility tools, and for setting the contrast resolution mode and color palette are available in "Accessibility for publications and ProtecTIER Manager" on page 137.

Saving and printing data

This task describes how to save or print the data displayed in informational ProtecTIER Manager windows.

About this task

Follow these steps to save or print data in ProtecTIER Manager informational windows and panes:

Procedure

1. Select **Options** in the upper right-hand corner of the window.

   Note: The **Options** menu may not be available on all windows.
2. Select **Save** to save the information or **Print** to print the information. Use the standard saving or printing procedures for your operating system.

Refreshing ProtecTIER Manager

This task describes how to refresh windows, screens, and panes in the ProtecTIER Manager application.

Many windows, screens, and panes of ProtecTIER Manager automatically refresh to display the most current information. However, you need to refresh some

windows manually. Because you can have multiple ProtecTIER Manager workstations on the same system, changes made on another workstation are not automatically reflected on your workstation. To ensure that you have the most up to date information, you should periodically refresh the ProtecTIER Manager Navigation pane and View pane.

Figure 47. ProtecTIER Manager

Select the **Refresh navigation pane** button to refresh the Navigation pane.

Select the **Refresh current view** button to refresh the View pane.

Running operations in the background

This topic describes enabling operations to run in the background while you are run another operation.

You can use the same instance of ProtecTIER Manager to work with multiple ProtecTIER systems while a specific ProtecTIER Manager operation runs in the background. You cannot, however, run multiple operations in the same ProtecTIER system.

For instance, if you are running a **Delete library** operation, the wizard prompts you to wait while the system goes offline to run the required operation. That system will be busy until it completes, thereby not allowing further administration of other operations.

By selecting **Run in background**, you return control to the user. If additional systems are configured in ProtecTIER Manager, those systems are accessible and can be worked on, even while the required operation is running.

Accessibility for publications and ProtecTIER Manager

The publications for this product are in Adobe Portable Document Format (PDF) and should be compliant with accessibility standards. Use these procedures to enable screen-reader compatibility, change the Windows contrast setting, and customize the color palette used in ProtecTIER Manager.

About this task

If you experience difficulties when you use the PDF files and want to request a Web-based format for a publication, send your request to the following address:

International Business Machines Corporation
Information Development
Department GZW
9000 South Rita Road
Tucson, Arizona 85744-001 U.S.A

In the request, be sure to include the publication number and title. When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

About the Windows-based accessibility features

About this task

The accessibility features in ProtecTIER Manager help persons with limited vision use the ProtecTIER Manager installation wizard and software. After preparing the ProtecTIER Manager workstation for accessibility, you can use Windows-based screen-reader software and a digital voice synthesizer to hear what is displayed on the screen.

The installation, configuration, and instructional screens in the Windows versions of the ProtecTIER Manager installation wizard and the ProtecTIER Manager software have been tested with Job Access with Speech (JAWS). However, the associated diagrams and graphs in ProtecTIER Manager and ProtecTIER Replication Manager, do not currently support keyboard navigation or screen-reader use. You can obtain full system statistics (typically provided in the diagrams and graphs) by going to the ProtecTIER Manager toolbar and clicking: **Reports** > **Create long term statistics report**, and downloading the results.

To enable screen-reader compatibility, you must prepare the ProtecTIER Manager workstation by completing these tasks. Instructions are provided in the topics that follow:

Before you install ProtecTIER Manager:

- Download and install the Java Runtime Environment (JRE).
- Download and install the Java Access Bridge (JAB).

After you install ProtecTIER Manager:

- Change the ProtecTIER Manager preferences to enable support of the Windows system settings *(required)*.
- Select a high-contrast color scheme in Windows *(optional)*.
- Customize the color palette used in the ProtecTIER Manager display *(optional)*.

About the Java-based tools

About this task

Complete the following procedures to download and install the Java-based tools that are required to enable full screen-reader compatibility on the ProtecTIER Manager workstation.

Install the Java™ Runtime Environment (JRE) first, and then install the Java Access Bridge (JAB). Both of these tools must be installed before you install the ProtecTIER Manager software.

For simplicity, download the Java-based tools by using the ProtecTIER Manager workstation on which you are installing the JRE and JAB. If this is not possible, try to use another computer that is running Windows.

Installing the Java Runtime Environment

About this task

The JRE includes the Java Virtual Machine (JVM). These tools are necessary for your computer to run Java-based applications.

Procedure

1. Go to http://www.java.com. The Java website opens.

   The java.com website auto-detects the operating system and Internet browser of the computer you use when you access the site.
2. Click **Free Java Download**, and proceed as appropriate:
   - If the **Download Java for Windows** page opens, go on to step 3
   - If the **Download Java for...** page title contains the name of an operating system other than Windows, do the following:
     a. Click the **See all downloads here** link.

        The list of available downloads, categorized by operating system, displays.
     b. In the Windows section, click **Windows 7/XP/Vista/2000/2003/2008 Online**.
3. Review the information provided, and then click **Agree and Start Free Download**.

   The download dialog box opens.
4. Follow the on-screen instructions to save the executable (.exe) installer file to the hard disk drive.
5. After the download is complete, find the installer file on the hard disk drive and write down the full path to the location of the file. For example: *C:\Program Files\Java\jre6\bin\java.exe*. This path is needed during ProtecTIER Manager installation.
6. Proceed as appropriate:

- If you downloaded the installer on the ProtecTIER Manager workstation on which you are installing the JRE, go on to step 7.
- If you downloaded the installer on a PC other than the applicable ProtecTIER Manager workstation, do the following:
  a. Copy the installer file onto a CD, flash memory drive, or other form of removable media.
  b. Copy the installer file from the removable media to the hard disk drive of the ProtecTIER Manager workstation.
  c. Go on to step 7.

7. Double-click the installer file to start the **Java installation wizard**.

   The **Java Setup – Welcome** window opens.
8. Click **Install** and follow the on-screen instructions to complete the installation process.
9. When you have successfully installed the JRE, go on to "Installing the Java Access Bridge."

Installing the Java Access Bridge

About this task

The Java Access Bridge (JAB) makes it possible for you to use Java-based screen readers with the ProtecTIER Manager installation wizard and software.

Procedure

1. Go to: http://www.oracle.com/technetwork/java/javase/tech/index-jsp-136191.html.

   The **Java SE Desktop Accessibility** page of the Oracle website opens.
2. Read the information provided, then click **Access Bridge**.
3. Scroll down to the **Java Access Bridge for Microsoft Windows Operating System x.x.x** (where *x.x.x* is the most recent version listed) section. Click the **Download Java Access Bridge x.x.x** link.

   The **Software License Agreement** page opens.
4. Read the license agreement, and then select the **I agree to the Software License Agreement** check box.

   The **Download Java Access Bridge for Windows Operating System x.x.x** page opens.
5. In the **Required Files** list, click the link to download the **Access Bridge x.x.x, accessbridge-x.x.x.exe** file.

   The download dialog box opens.
6. Follow the on-screen instructions to save the executable (.exe) installer file to the hard disk drive.
7. When the download is complete, locate the installer file on the hard disk drive and proceed as appropriate:
   - If you downloaded the installer by using the ProtecTIER Manager workstation on which you are installing the JAB, go on to step 8 on page 140.
   - If you downloaded the installer by using a PC other than the applicable ProtecTIER Manager workstation, do the following:
     a. Copy the installer file onto a CD, flash memory drive, or other removable media device.

b. Copy the installer file from the removable media device to the hard disk drive of the ProtecTIER Manager workstation.
c. Go on to step 8.

8. On the ProtecTIER Manager workstation, double-click the **accessbridge-x.x.x.exe** installer file.

   A security warning dialog box displays.

9. Click **Run**.

   The **Java Access Bridge – InstallShield Wizard** opens.

10. Read the welcome information, then click **Next** and follow the on-screen instructions to complete the installation.
11. When the installation is complete, restart the workstation as directed.

    You now have the necessary Java tools for compatibility between the ProtecTIER Manager installation wizard and screen reader software.

12. Follow the instructions in "Using a screen reader to install ProtecTIER Manager" to start the ProtecTIER Manager installation wizard by using a screen reader.

Using a screen reader to install ProtecTIER Manager

About this task

Install ProtecTIER Manager according to the following command line-based instructions.

When entering the commands, type them exactly as shown, including any spaces or quotation marks. Any deviation in the procedure can cause the installation to start in the non-accessible mode, or fail completely.

Procedure

1. If your workstation is configured to automatically open DVDs, temporarily disable the Windows **AutoPlay** feature for the CD/DVD device. Use the Windows Help or other Windows documentation for instructions, and then go on to step 2.
2. Insert the *IBM ProtecTIER Manager DVD* into the CD/DVD drive of the ProtecTIER Manager workstation.
3. Access the command prompt on the ProtecTIER Manager workstation:
   a. Click **Start** > **Run...**.

      The **Run** dialog box opens.

4. In the **Open** field, type: **cmd** and click **Ok**.

   The command window opens.

5. Browse to the ProtecTIER Manager installation directory on the DVD. To do so:
   a. At the command prompt, type: **D:** (where D: is the letter assigned to the CD/DVD drive of the workstation) and press **<enter>**.
   b. At the command prompt, list the contents of the DVD. Type: **dir** and press **<enter>**.
   c. Locate the name of the ProtecTIER Manager directory on the DVD. For example: *PT_Manager_V3.3*.
   d. At the command prompt, change to the **ProtecTIER Manager** directory. Type: **cd <directory name>** and press **<enter>**. For example: `cd PT_Manager_V3.3` **<enter>.**

e. At the command prompt, change to the **Windows** directory. Type: **cd windows** and press **<enter>**.

f. At the command prompt, type: **Install.exe LAX_VM "C:\Program Files\Java60\jre\bin\java.exe"** and press **<enter>**, where the path contained within the quotation marks is the same as the path that you noted in step 5 on page 138.

The screen-reader-enabled ProtecTIER Manager installation wizard starts.

g. Follow the spoken prompts to compete the installation.

6. When the installation completes, proceed as appropriate:
   - If you **do not** want to enable the Windows High Contrast option or customize the color palette, resume your regular use of ProtecTIER Manager.
   - To change the contrast mode for ProtecTIER Manager, go to "Enabling the Windows High Contrast option." To customize the color palette, go to "Customizing the color palette" on page 145.

Enabling the Windows High Contrast option

About this task

To make it possible for ProtecTIER Manager to display in high contrast, you must first enable the **Use High Contrast** option in Windows.

Procedure

1. On the ProtecTIER Manager workstation, go to **Windows** > **Control Panel** > **Accessibility Options**.

   The **Accessibility Options** dialog box opens.

2. Select the **Display** tab.
3. In the **High Contrast** area of the **Display** tab, select the **Use High Contrast** check box, as shown in Figure 48 on page 142:

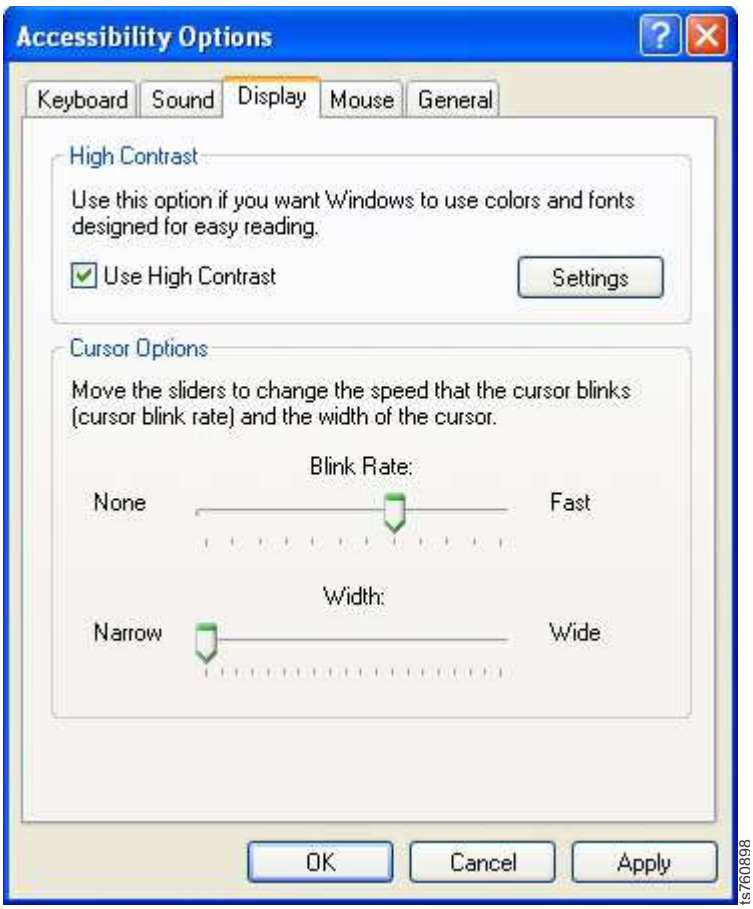


Figure 48. Display tab

4. Click **Settings**.

   The **Settings for High Contrast** dialog box displays, as shown in Figure 49 on page 143:

Figure 49. Settings for High Contrast

By default, the **High Contrast Black (large)** scheme is selected.

5. Do one of the following:
   - To use the default, **High Contrast Black (large)**, scheme:
     a. Click **Ok** to close the **Settings for High Contrast** dialog box.
     b. Click **Ok** to close the **Accessibility Options** dialog box.
        After a few moments, the display changes to the new color scheme.
     c. Go on to "Using the Windows high contrast scheme with ProtecTIER Manager."
   - To use a different high contrast scheme:
     a. Click the arrow to show the list of available color schemes.
     b. Select the high contrast scheme that you want to use.
     c. Click **Ok** to close the **Settings for High Contrast** dialog box.
     d. Click **Ok** to close the **Accessibility Options** dialog box.
        After a few moments, the display changes to the new color scheme.
     e. Go on to "Using the Windows high contrast scheme with ProtecTIER Manager."

Using the Windows high contrast scheme with ProtecTIER Manager

About this task

Now that you have changed the contrast scheme in Windows, you must enable the **Support system settings** option in ProtecTIER Manager.

Procedure

1. Launch **ProtecTIER Manager**:

a. Click: **Start** > **All Programs** > **IBM** > **ProtecTIER Manager** > **IBM ProtecTIER Manager**.

The ProtecTIER Manager window opens, as shown in: Figure 50.

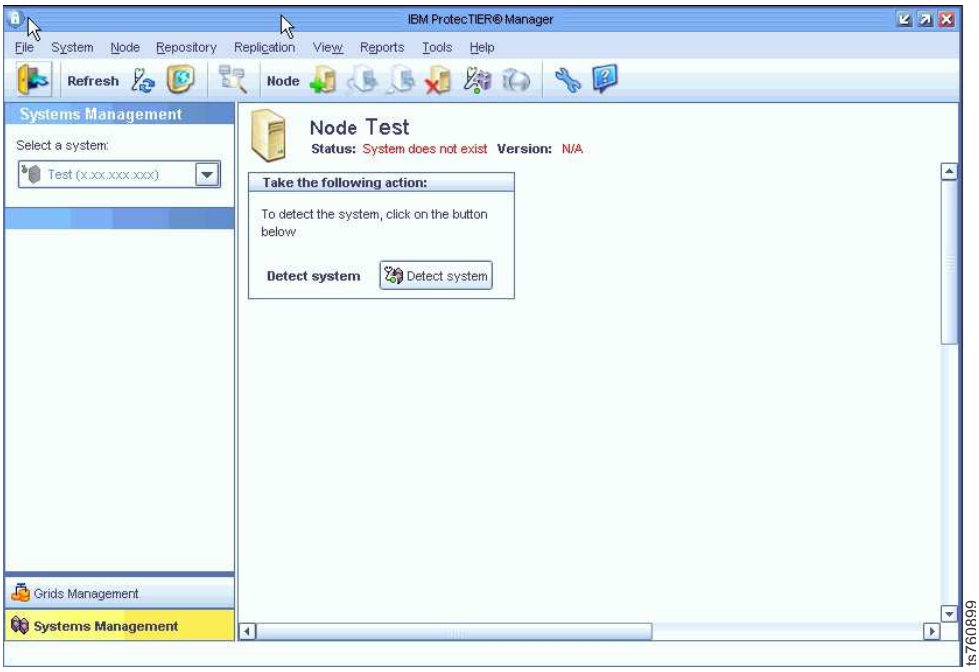


Figure 50. ProtecTIER Manager window

2. On the toolbar, click: **Tools** > **Preferences**.

   The **Preferences** dialog box opens with the **Appearance** tab selected, as shown in Figure 51:

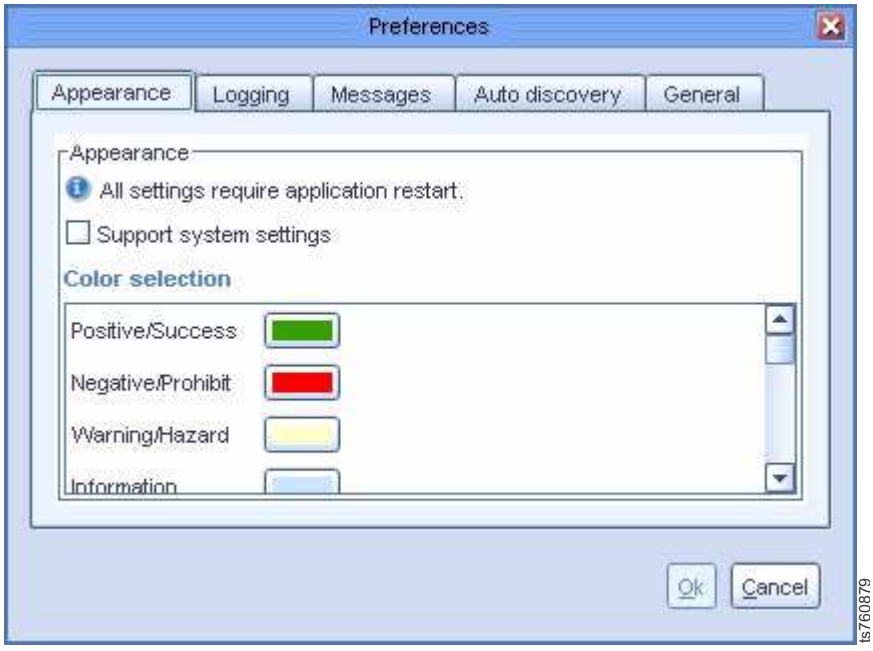


Figure 51. Preferences dialog box

3. On the **Appearance** tab, select the **Support system settings** check box.
   You are returned to the **ProtecTIER Manager** window.
4. Exit and restart ProtecTIER Manager so the contrast settings take effect:
   a. On the **ProtecTIER Manager** toolbar, click: **File** > **Exit**.
      The **ProtecTIER Manager** window closes.
   b. Click: **Start** > **All Programs** > **IBM** > **ProtecTIER Manager** > **IBM ProtecTIER Manager**.
      When the ProtecTIER Manager window opens, the display reflects the contrast change, as shown in: Figure 52.

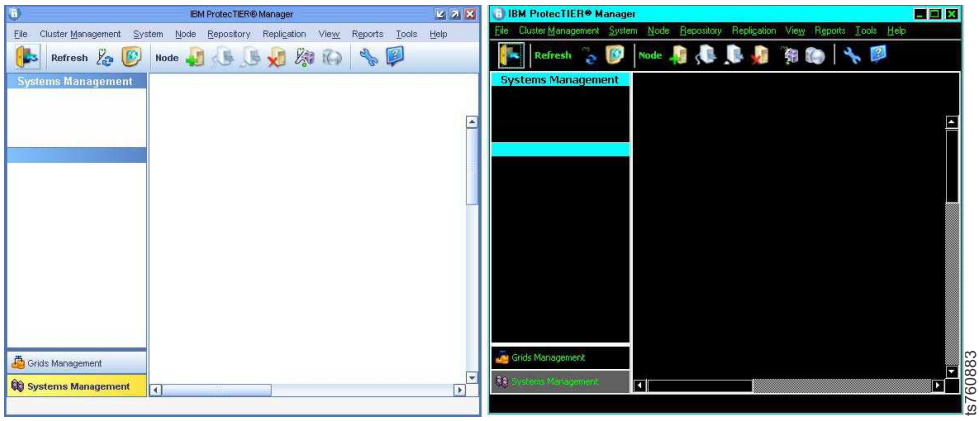


Figure 52. Normal contrast versus high contrast

5. Proceed as appropriate:
   - If you want to change one or more of the colors used in the ProtecTIER Manager display, continue to "Customizing the color palette."
   - If you **do not** want to customize the color palette, resume your regular use of ProtecTIER Manager.

Customizing the color palette

About this task

Use this procedure to customize the color palette for ProtecTIER Manager to improve visibility in the display, or to suit your personal preferences.

Procedure

1. If necessary, start ProtecTIER Manager as described in step 1 on page 143.
2. Open the **Preferences** dialog box, as described in 2 on page 144.
3. Scroll down (if necessary) to see the entire **Color selection** list, and then select the color you want to change.
   The **Color selection** dialog box opens, with the **Swatches** tab selected, as shown in Figure 53 on page 146:

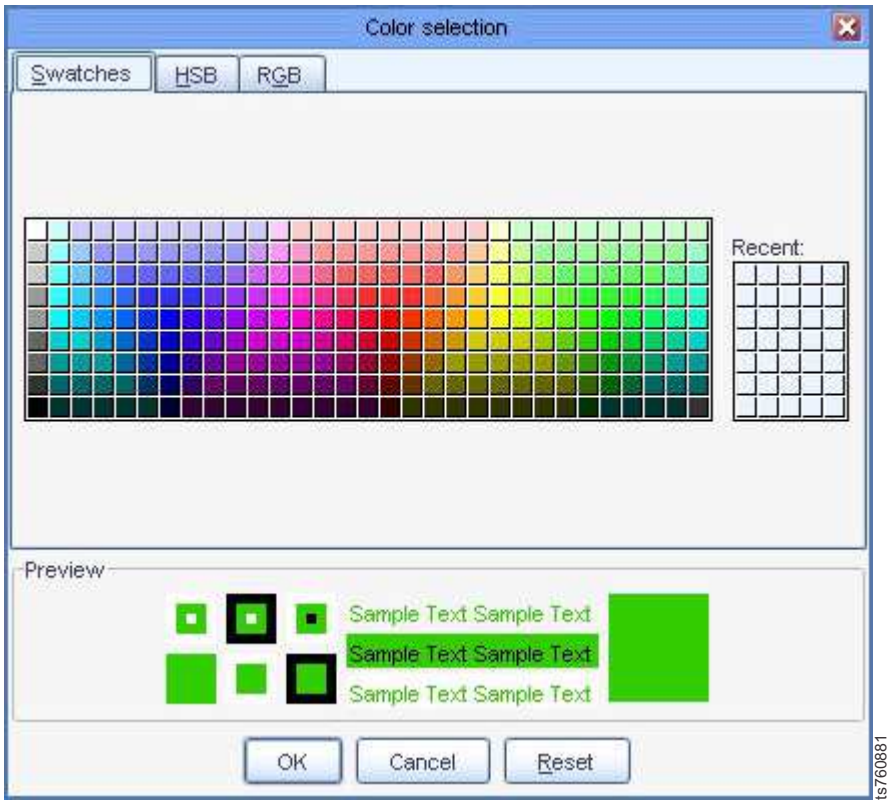


Figure 53. Color selection, Swatches tab

The color that is currently defined for your selection is shown in the **Preview** pane.

4. Select a new color from the color palette.

   You can also specify a new color by using the Hue/Saturation/Brightness (HSB) or Red/Green/Blue (RGB) color models. To do so, click the tab for the model you want to use and enter the required values.

5. When you have finished selecting or specifying the new color, click **Ok**.

   You are returned to the **Appearance** tab.

6. To change another color, repeat steps 3 on page 145 through 5.

7. When you are finished making changes in the **Appearance** tab, click **Ok**.

   You are returned to the ProtecTIER Manager window.

8. Exit and restart ProtecTIER Manager (as described in step 4 on page 145) so the color palette changes take effect.

   After you log in to ProtecTIER Manager and add a node, the display reflects your custom color selections.

   An example of the default color versus a custom color for **Allocable** resources, is shown in: Figure 54 on page 147

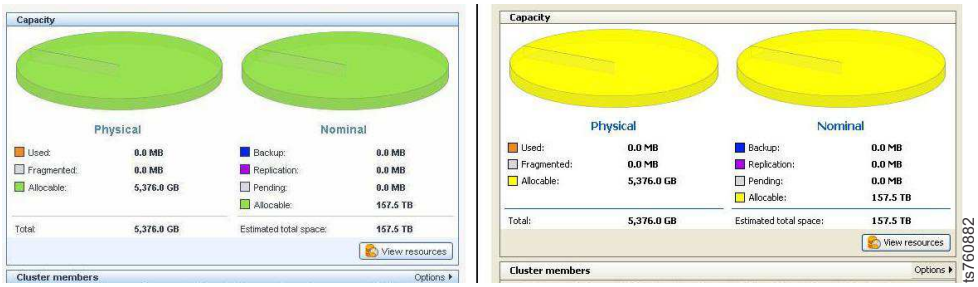


Figure 54. Default color versus custom color

9. Proceed as appropriate. Return to the task from which you were sent to these instructions or resume your regular use of ProtecTIER Manager.

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 give 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.

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 PUBLICATIONS "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.

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 measurement may have been

estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

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

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Red Hat Notice

IBM delivers patches (including security fixes) for Red Hat Enterprise Linux (RHEL) based on the Red Hat Enterprise Linux Life Cycle policy. As stated in the Red Hat policy, fixes are not provided for all vulnerabilities on all RHEL versions, which means that IBM cannot deliver security fixes for some RHEL issues.

When security and other related updates are available from Red Hat, IBM delivers those updates in software packages that can be downloaded and applied to ProtecTIER. IBM may also publish Security Bulletins with additional information for security related updates. Customers should subscribe to My Notifications to be notified of important ProtecTIER support alerts.

Trademarks

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

- AIX®
- DS4000®
- Enterprise Storage Server®
- ESCON
- FICON®
- i5/OS™
- iSeries
- IBM
- ProtecTIER
- pSeries
- S/390®
- ServeRAID
- System x

- System Storage
- TotalStorage
- Wake on LAN
- z/OS®
- zSeries

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol ((R) or (TM)), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Java and all Java-based trademarks are trademarks of Oracle, Inc. in the United States, other countries, or both.

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

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

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

Red Hat is a registered trademark of Red Hat, Inc. in the United States, other countries, or both.

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

Electronic emission notices

This section contains the electronic emission notices or statements for the United States and other regions.

Federal Communications Commission statement

This explains the Federal Communications Commission's (FCC) statement.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is

operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, might cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors, or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device might not cause harmful interference, and (2) this device must accept any interference received, including interference that might cause undesired operation.

Industry Canada compliance statement

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conform à la norme NMB-003 du Canada.

European Union Electromagnetic Compatibility Directive

This product is in conformity with the protection requirements of European Union (EU) Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

Attention: This is an EN 55022 Class A product. In a domestic environment this product might cause radio interference in which case the user might be required to take adequate measures.

Responsible Manufacturer:

International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
914-499-1900

European community contact:

IBM Deutschland GmbH
Technical Regulations, Department M372
IBM-Allee 1, 71139 Ehningen, Germany
Tele: +49 7032 15 2941
e-mail: lugi@de.ibm.com

Australia and New Zealand Class A Statement

Attention: This is a Class A product. In a domestic environment this product might cause radio interference in which case the user might be required to take adequate measures.

Germany Electromagnetic compatibility directive

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der IBM gesteckt/eingebaut werden.

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden:

"Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Mabnahmen zu ergreifen und dafür aufzukommen."

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem "Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)." Dies ist die Umsetzung der EU-Richtlinie 2004/108/EG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2004/108/EG) für Geräte der Klasse A

Dieses Gerät ist berechtigt, in übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:

International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:

IBM Deutschland GmbH
Technical Regulations, Abteilung M372

IBM-Allee 1, 71139 Ehningen, Germany
Tele: +49 7032 15 2941
e-mail: lugi@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

People's Republic of China Class A Electronic Emission statement

中华人民共和国“A类”警告声明

声 明
此为A级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。

Taiwan Class A Statement

警告使用者:
這是甲類的資訊產品，在
居住的環境中使用時，可
能會造成射頻干擾，在這
種情況下，使用者會被要
求採取某些適當的對策。 taiemi

Taiwan contact information

This topic contains the product service contact information for Taiwan.

IBM Taiwan Product Service Contact Information:
IBM Taiwan Corporation
3F, No 7, Song Ren Rd., Taipei Taiwan
Tel: 0800-016-888

台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

f2c00790

Japan Voluntary Control Council for Interference (VCCI) Class A Statement

この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI-A

Japan Electronics and Information Technology Industries Association (JEITA) Statement (less than or equal to 20 A per phase)

高調波ガイドライン適合品

jjieta1

Korean Electromagnetic Interference (EMI) Statement

This explains the Korean Electromagnetic Interference (EMI) statement.

이 기기는 업무용 환경에서 사용할 목적으로 적합성평가를 받은 기기로서

가정용 환경에서 사용하는 경우 전파간섭의 우려가 있습니다.

Russia Electromagnetic Interference (EMI) Class A Statement

ВНИМАНИЕ! Настоящее изделие относится к классу А.
В жилых помещениях оно может создавать
радиопомехи, для снижения которых необходимы
дополнительные меры

rusemi

Index

Numerics

A

C

D

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W

X

Printed in USA

SC27-8901-01