SDM Basics

Functional description

The SuperNode Data Manager (SDM) is a fault-tolerant UNIX-based processing platform that uses Motorola technology, and runs operations, administration, maintenance, and provisioning (OAM&P) software applications. It is a high-performance computing platform connected to the operating company's DMS switch.

The SDM and its applications allow the operating company to off-load its OAM&P processes from the switch. The SDM is connected to the operating company's network through an Ethernet connection to its operations intranet.

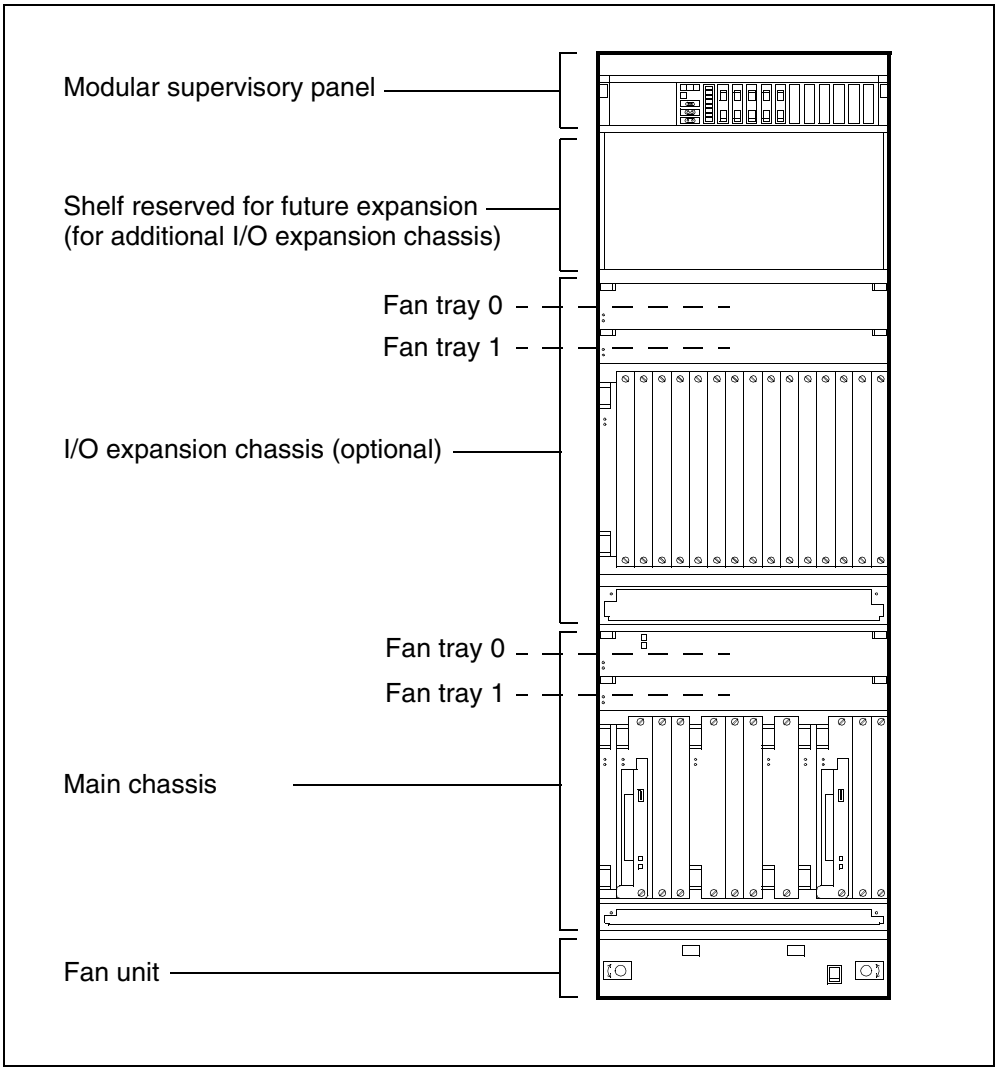
SuperNode Data Manager hardware overview

This module provides an overview of the SuperNode Data Manager (SDM) hardware. For gating hardware for a particular release, refer to “Hardware baseline” in the Upgrades document.

Cabinet

The SuperNode Data Manager uses the Nortel C28 Model B (C28B) Streamlined cabinet. The cabinet contains a modular supervisory panel (MSP), a shelf reserved for future expansion, an optional input/output (I/O) expansion chassis, a main chassis, and a fan unit. System modules are located at the front of the main chassis and the I/O expansion chassis. The following figure shows a front view of the cabinet.

Front view of the C28B cabinet



Modular supervisory panel

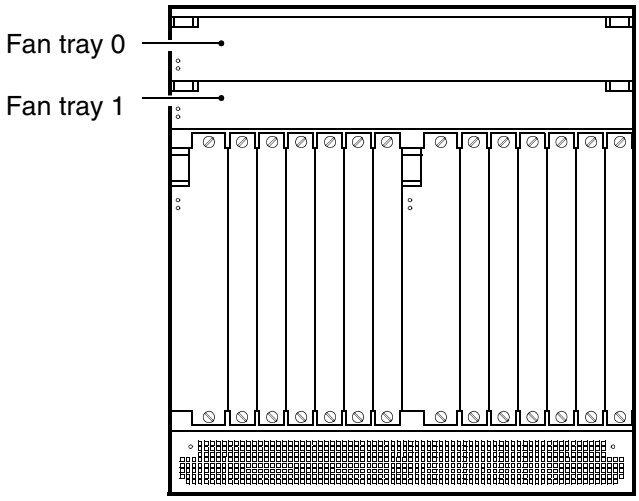
The modular supervisory panel (MSP) provides power and alarm monitoring for the C28B cabinet. The A and B battery feeds (-48V dc) supply power to the SDM platform. Each feed is supplied from a separate breaker in the MSP into interconnect modules (Dims) in the main and I/O expansion chassis.

Front-mounted I/O expansion chassis

The I/O expansion chassis is for optional system modules. The chassis has two removable fan trays (NTRX50KD and NTRX50FF) that provide horizontal (front-to-rear) cooling to the chassis. Each fan tray has three fans powered by separate battery feeds to ensure uninterrupted cooling

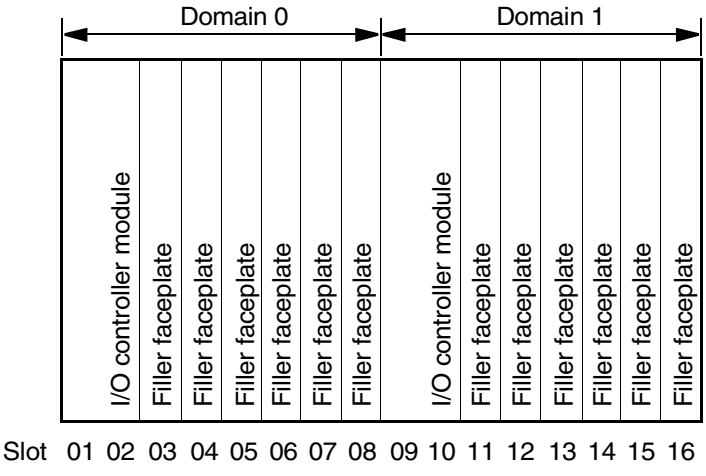
during fan tray servicing. The following figure shows a front view of the chassis. The fan trays do not have system status LEDs.

Front view of the I/O expansion chassis



Provisionable system modules in the I/O expansion chassis are not restricted to specific slot numbers. The I/O controller modules mount in any two slots, providing the slot numbers correspond in each domain (0 and 1). Personality modules are not required for the I/O controller modules. The following figure identifies the slot numbers in domains 0 and 1, and the I/O controller modules.

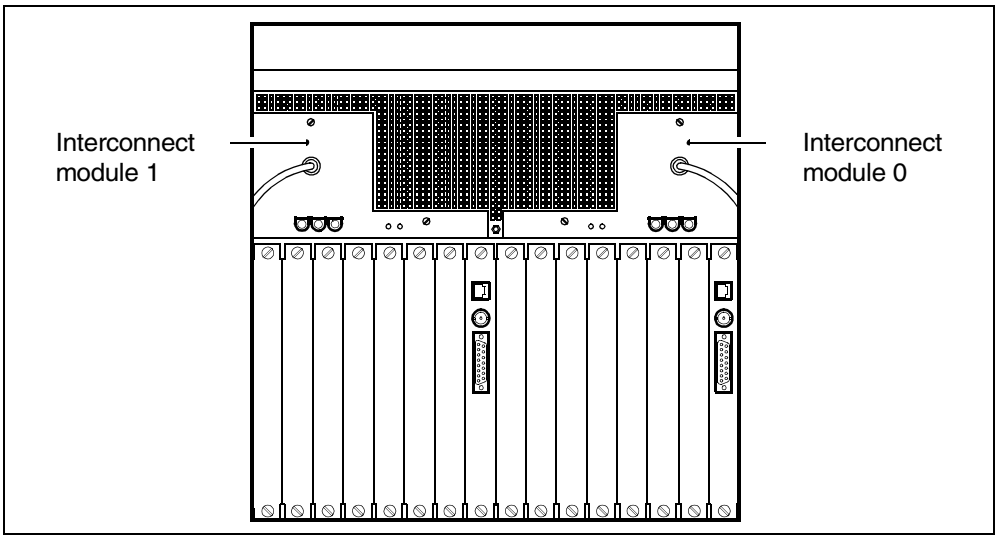
Front view of the I/O expansion chassis by slot number



Rear-mounted I/O expansion chassis

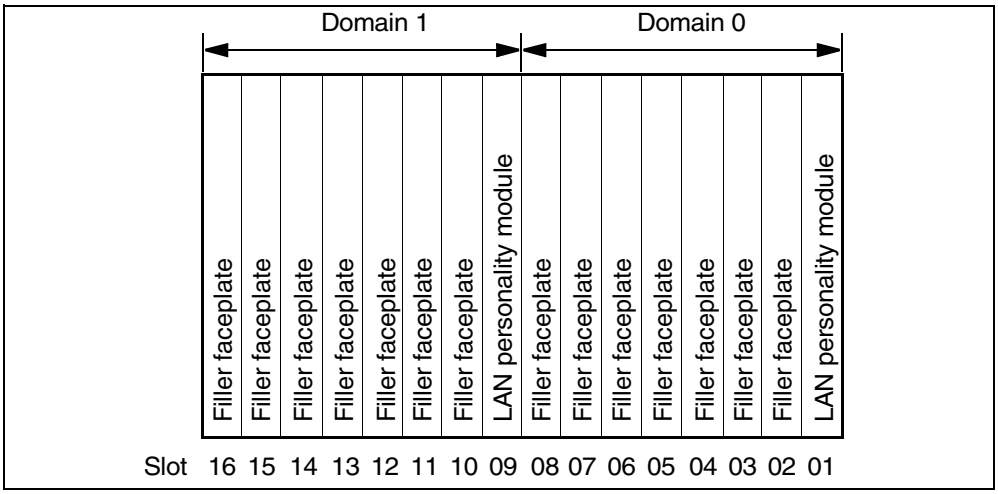
The rear of the I/O expansion chassis contains two interconnect modules (ICM) that supply power to the SDM through separate battery feeds. There is no alarm cable for the ICMs in the I/O expansion chassis. The following figure shows the rear view of the chassis.

Rear view of the I/O expansion chassis



The chassis has a LAN personality module (NTRX50FS) in slots 1 and 9. The LAN personality module at the rear of the I/O expansion chassis is used with the I/O controller module that mounts at the front of the chassis. The following figure identifies the slot numbers in domains 0 and 1, and the locations of the provisionable LAN personality modules.

Rear view of the I/O expansion chassis by slot number

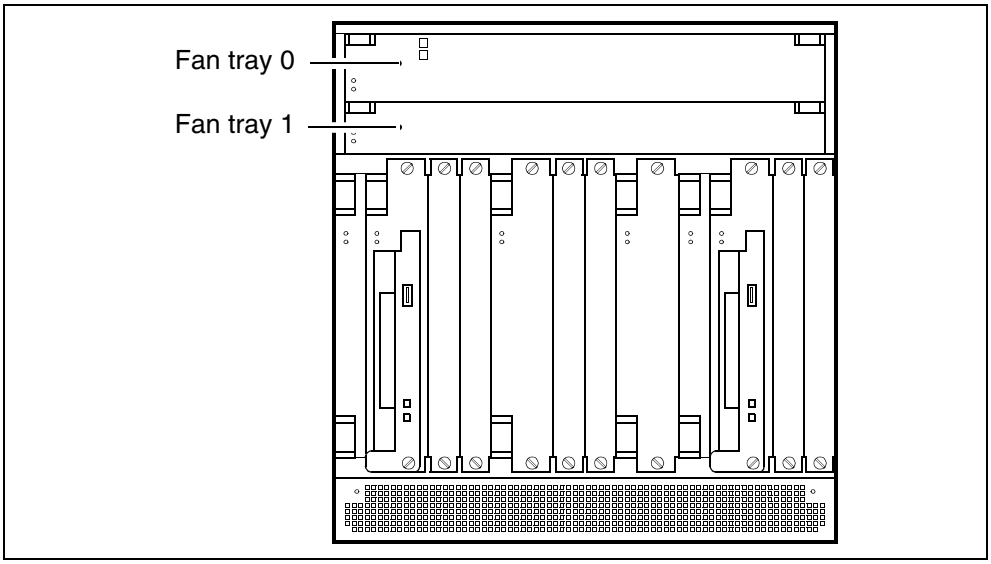


Provisionable personality modules in the I/O expansion chassis are not restricted to specific slot numbers. The LAN personality module mounts in any two slots. However, you must use the same slot numbers in each domain, and in the system module installed at the front of the chassis.

Front-mounted main chassis

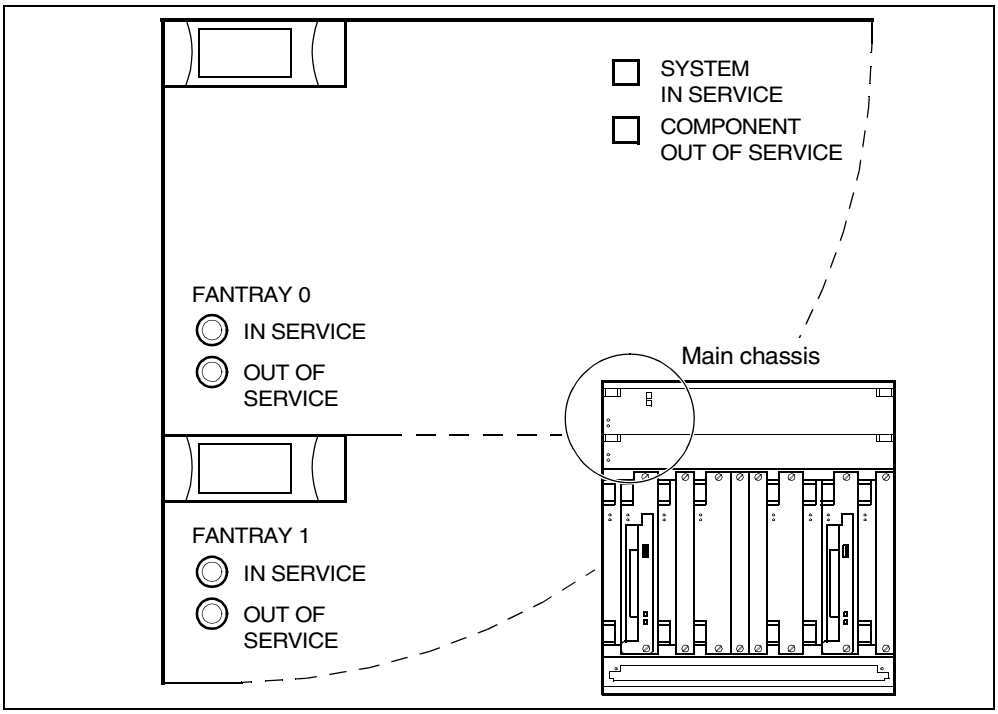
The front of the chassis has fan trays, provisionable system modules and controller modules. The following figure shows a front view of the chassis.

Front view of the main chassis



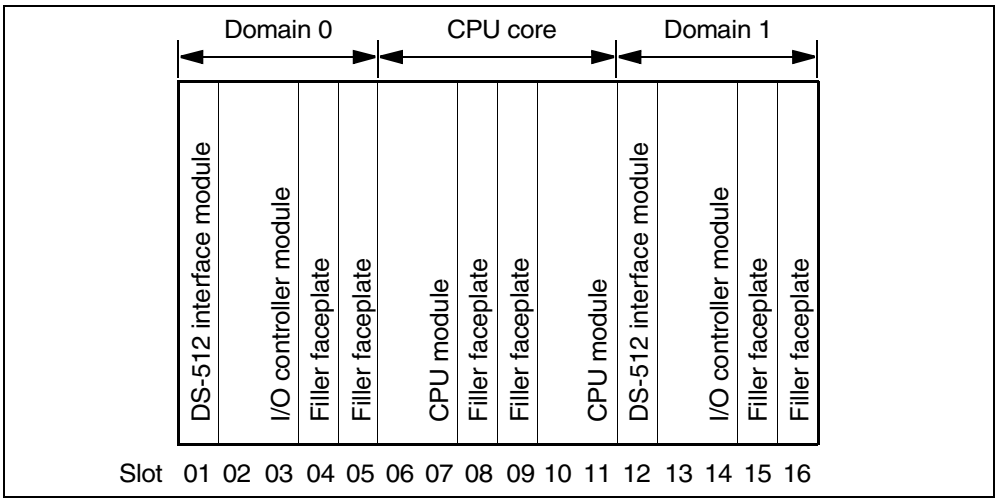
Two removable fan trays (NTRX50FE and NTRX50FF) provide horizontal (front-to-rear) cooling to the chassis. Both trays on the main chassis contain in-service and out-of-service LEDs. Unlike the fan trays in the I/O expansion chassis, which do not have system status LEDs, the top tray (NTRX50FE) also contains system status LEDs. The following figure shows the fan trays and fan tray LEDs.

Fan tray LEDs on the main chassis



The following figure shows the slot numbers in domains 0 and 1, the CPU core, and the required system controller modules in the main chassis. The remaining slots are available for provisioning optional system modules. The figure reflects a configuration without data volume group (datavg).

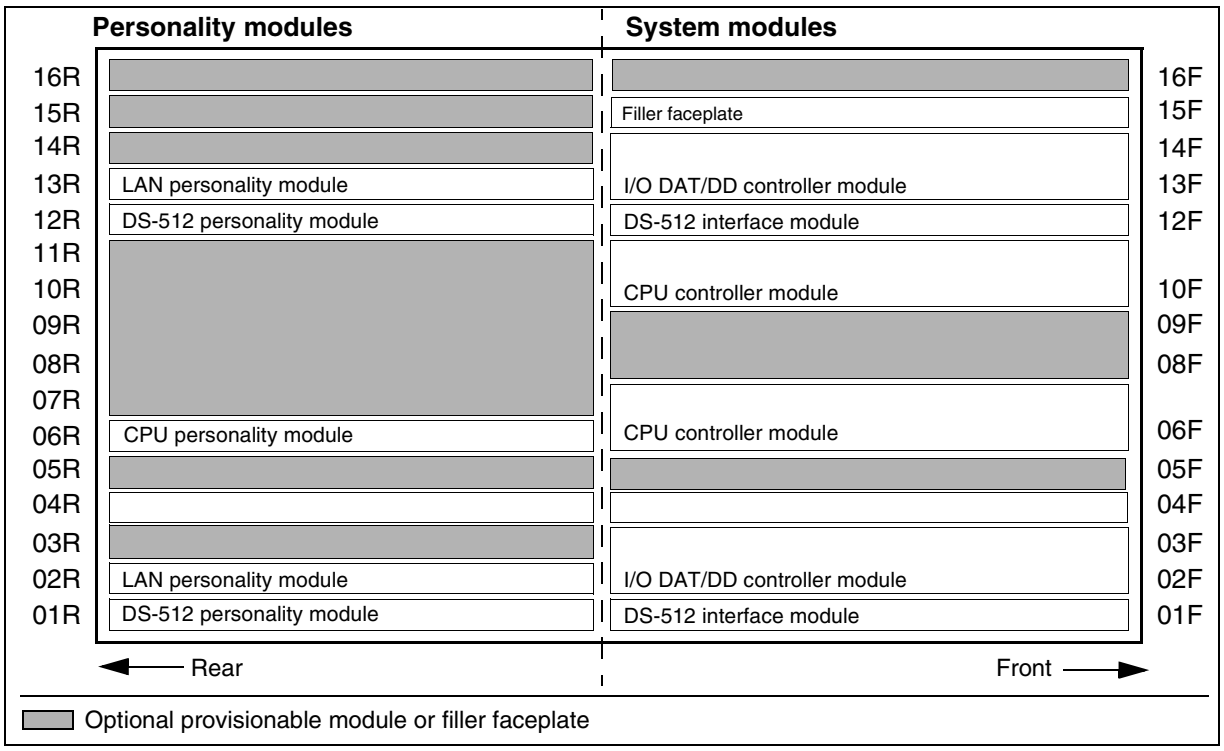
Front view of slots in the main chassis (without datavg)



Module slot placement

The following figure shows the dedicated slot numbers for required SDM modules (front and rear). Provisionable equipment mounts in any available slot number in either the main chassis or the I/O expansion chassis.

SDM module slot number layout (front and rear)



CPU controller module

The CPU controller module contains the main processing power and memory capacity of the SDM and is provisionable in slots 6, 7, 10 and 11 at the front of the main chassis. The module provides console port connections to the CPU modules. The following table lists the types of CPU controller modules.

CPU controller modules

PEC	Description
NTRX50CG	604e processor, 200MHz/256MB
NTRX50CH	604e processor, 200MHz/512MB
NTRX50NB	Arthur 750 processor, 400MHz/512MB

DS-512 interface module

The DS-512 interface module (NTRX50GX) is provisionable in slots 1 and 12 at the front of the main chassis. The module is used with the DS-512 personality module (NTRX50GH) located in slots 1 and 12 at the back of the main chassis.

I/O controller module

The I/O controller modules and the associated personality modules provide mirrored disk storage, redundant DAT drives, and redundant Ethernet links to the LAN. The controllers support the following volume groups in the SDM platform:

- root volume groups (rootvg), which have one physical volume (disk)
- data volume groups (datavg), which have multiple physical volumes (disks)

The SDM supports an X.25 controller module, a multi-function input/output (MFIO) controller module, and an ultra multi-function input/output (UMFIO)/X25PM controller module.

The UMFIO/X25PM module eliminates the need for an expansion chassis in the SDM. The rootvg UMFIO has an embedded X.25 functionality, and can replace the MFIO and X.25 standalone (SYNC X25) controller modules.

Both the X.25 and the UMFIO/X25PM controller modules are supported, but cannot coexist on the same system.

Each I/O controller module requires a LAN personality module (NTRX50FS) to provide Ethernet connectivity from the SDM to the operating company LAN.

The following table lists the types of MFIO controller modules.

MFIO controller modules

PEC	Description
NTRX50GP (datavg)	Two (2) 4-GB DDUs, a 10Base-T Ethernet interface
NTRX50NC (datavg)	Two (2) 9-GB DDUs, a 10Base-T Ethernet interface

MFIO controller modules

PEC	Description
NTRX50GN (rootvg)	One (1) 4-GB DDU, a DDS-2 DAT drive, a 10Base-T Ethernet interface
NTRX50ND (rootvg)	One (1) 9-GB DDU, a DDS-2 DAT drive, a 10Base-T Ethernet interface

The following table list the types of UMFIO/X25PM controller modules.

UMFIO/X25PM controller modules

PEC	Description
NTRX50NL (datavg)	Two (2) 36-GB DDU, an intelligent 10/100Base-T Ethernet interface
NTRX50NM (rootvg)	One (1) 36-GB DDU, DDS-3 DAT drive, intelligent 10/100Base-T Ethernet interface, and an integrated X.25 interface (X.25 requires operating system AIX 4.3.3)

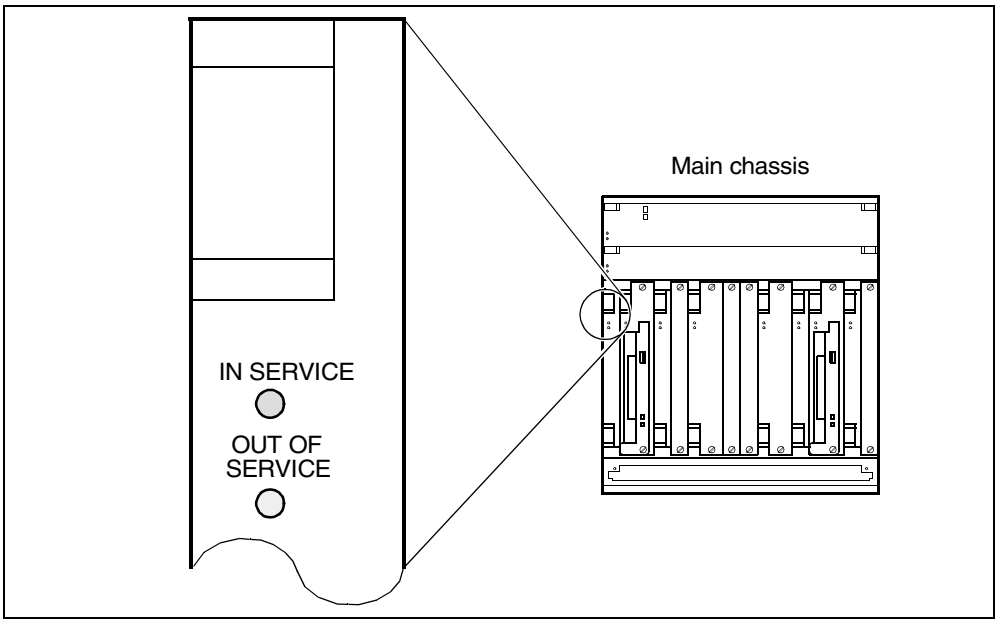
Optional slots at the front of the main chassis

Slots 4, 5, 8, 9, 15 and 16 at the front of the main chassis are used only for additional provisionable equipment. Unused slots at the front contain filler panels to ensure electromagnetic interference (EMI) compliance and even distribution of cooling.

System module LEDs

Light-emitting diodes (LEDs) are visible on all system modules in the main or optional I/O expansion chassis. The following figure shows the LEDs on the system modules at the front of the main chassis.

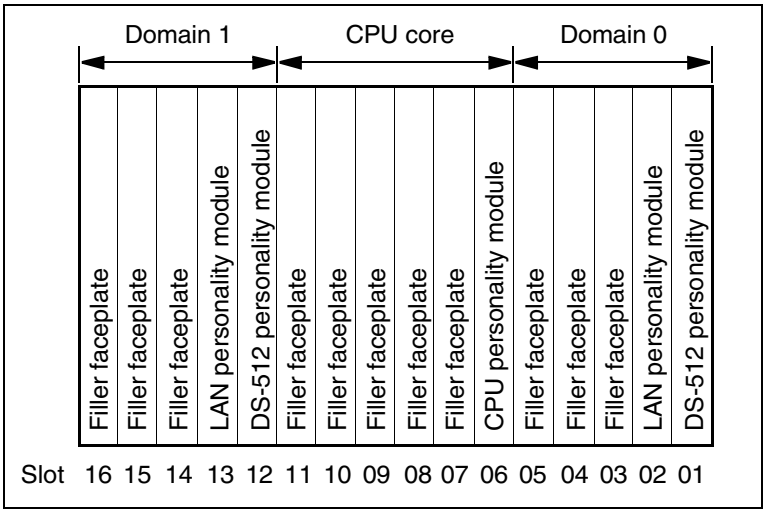
System module LEDs



Rear-mounted main chassis

The rear of the main chassis contains two ICMs (NTRX50FG and NTRX50FH), which supply power to the SDM. It also contains two DS-512 personality modules in slots 1 and 12, two LAN personality modules in slots 2 and 13, and one CPU personality module in slot 6, as shown in the following figure. The remaining slots are available for optional personality modules such as X.25 personality modules.

Rear view of the main chassis by slot number



DS-512 personality module

The DS-512 personality module (NTRX50GH) mounts in slots 1 and 12 at the back of the main chassis, and connects to the DS-512 interface module (NTRX50GX) in slots 1 and 12 at the front of the main chassis.

LAN personality module

The LAN personality module mounts in slots 2 and 13 at the back of the main chassis. A LAN personality module connects to each I/O controller module in slots 2, 3, 13 and 14 at the front of the main chassis. The LAN personality module supports a 10Base-T port connection to the operating company LAN. The following table provides information on the LAN personality modules.

PEC	Description
NTRX50FS	MFIO LAN personality module - used with the NTRX50NC and NTRX50GP MFIO controller modules
NTRX50NK	UMFIO LAN personality module - used with the NTRX50NL and NTRX50NM UMFIO controller modules

CPU personality module

The CPU personality module (NTRX50FD) mounts in slot 6 at the back of the main chassis. The CPU module connects to the CPU personality module, which provides console and modem port connection to the CPU module. For remote console access, port SP0 on the CPU personality module connects to a modem by a NTRX5093 cable. For local console access, port SP0 connects to a VT100 terminal by an NTRX5094 cable.

X.25 personality module

The X.25 personality module (NTRX50FZ) is used with the X.25 controller module (NTRX50FY).

LAN/X.25 personality module (NTRX50NN)

The NTRX50NN personality module provides two physical connections to a LAN: X.25 and 10/100 BaseT. The NTRX50NN supports the NTRX50NM rootvg UMFIO module and the NTRX50NL datavg UMFIO module.

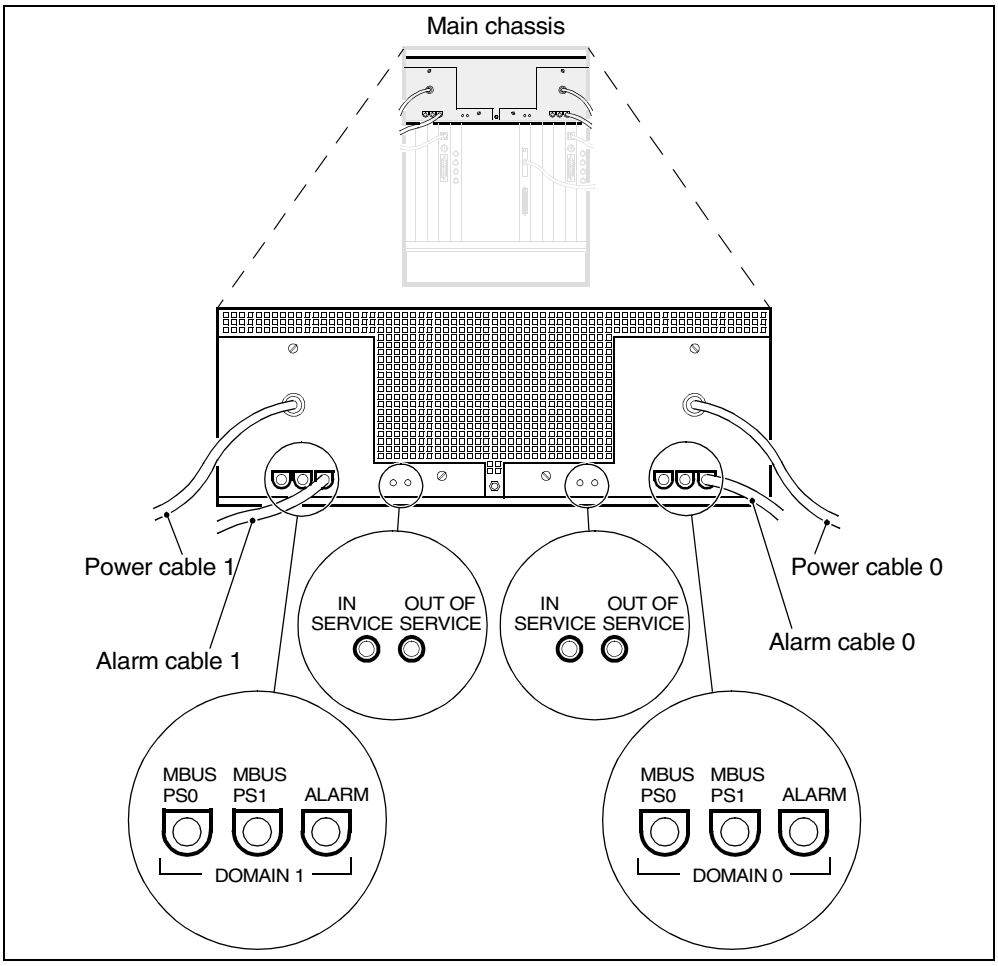
Optional slots at the back of the main chassis

Slots 3 to 5, 7 to 11, and 14 to 16 at the back of the main chassis are for optional equipment. Unused slots must be equipped with filler panels to ensure EMI compliance, and to distribute cooling air evenly.

Interconnect modules

Two ICMs at the rear of the main chassis and the I/O expansion chassis plug directly into the backplane. Each ICM supplies -48V dc to its corresponding domain through separate battery feeds, and has two LEDs that indicate when it is either in or out of service. The following figure shows a rear view of the interconnect modules.

Rear view of the interconnect modules



Power supply

Battery feeds A and B supply power to the SDM hardware. The feeds connect from the MSP to the chassis through the ICMs at the back of the chassis. Battery feed A supplies power to hardware in domain 0, and battery feed B supplies power to hardware in domain 1. Both domains provide power to CPU modules. Normally, both feeds are operational. During a single feed failure, the unaffected domain continues to provide service.

Fan unit

The fan unit of the SDM cabinet provides vertical cooling for the SDM cabinet.

Provisionable hardware

Provisionable hardware modules can mount at the front of the main chassis and I/O expansion chassis, and are not restricted to designated slot numbers. (Corresponding slot numbers must be used for each domain to support fault-tolerant operation.) The following table lists I/O controller modules that can be provisioned to meet system requirements for a separate datavg.

I/O controller modules for separate datavg

For	Controller module	Personality module
MFIO	NTRX50GP or NTRX50NC	NTRX50FS
UMFIO/X25PM	NTRX50NL or NTRX50NM	NTRX50NK

Use the NTRX50GP module with the NTRX50GN module to meet the following system requirements for a separate datavg:

- Use a pair of NTRX50GP modules to provide 8 GB of datavg.
- Use two pairs of NTRX50GP I/O modules to provide 16 GB of datavg.

Software overview

Architecture

The SDM software has base, service and application layers that support parallel development in each stream. This architecture allows independent delivery of new services and applications and interim delivery of maintenance release software.

Base software layer

The base software layer supports SDM maintenance and operation, and consists of

- the AIX 4.3.3 operating system and server software
- node and process control services
- maintenance and administration services

Service software layer

The service layer provides common software utilities and functions for multiple applications, and internal application support software for current and future application packages. The following table lists the components of the service software layer.

Service software layer components

Component	Description
Table access utility	Allows applications on the SDM to manipulate tables maintained on the Core.
Remote procedure call (RPC)	Allows software on the Core to raise RPC routines to software on the SDM. RPC routines allow a program running on one host to request and receive a message with results of a service on another host.
Open Software Foundation (OSF) Distributed Computing Environment (DCE)	Provides authentication and authorization mechanisms for network security.
Operational measurement (OM) collection and application programming interface (API)	Allows applications on the SDM to receive OM data from the Core.

Application software layer

The application software layer provides applications for Core operations, administration, maintenance and provisioning (OAM&P), and contains all application software installed on the SDM.

Software and application order codes

The following table lists the software order codes for the SDM.

Software order codes

Name	Order code
CNCD Billing Filtering	CNCD0006
CNCD Billing Filtering	
CNCD CDR 01	CNCD0002
CNCD CDR Base	
CNCD CDR PH1	CNCD0001
CNCD CDR to AMA	CNCD0003
CNCD RTB OFT	CNCD0004
CNCE SDM AT&T Custom	CNCE0001
CNCE AMA DNS features	
CNOM OM 02	CNOM0002
CNOM OM Base	
CNOM PH1	CNOM0001
LCS AdventNet SNMP V3	LCS00016
LCS Lic AdventNet SNMP V3	
LCS ILOG JView	LCS00014
LCS JView	
PSPT 15K MSS Integration	PSPT0001
PSPT Exist OSS I/F Integration	
PSPT FCAPS API	

Software order codes

Name	Order code
ATA ASCII Term Acc Gwy	ATA00001
ATA ASCII Access Gateway	
ENTA Enhanced Term Access	ENTA0001
ENTA Enhanced Term Access	
NMDC TCP/IP I/F NTM/DC	NMDC0001
NMDC TCP/IP I/F NTM/DC	
SBM AMADNS DDI I/F	SBM00003
SBM AMADNS DDI I/F FN	
SBM Billing Appl Base	SBM00001
SBM Auto File Xfer AFT	SBM00007
SBM Billing Appl Base FN	
SBM Capacity & Performance	
SBM Multi-Stream BAF/CDR	
SBM SBA-SMDR Delivery	SBM00006
SBM SBA SMDR	
SFT ASG Enabling FT/SW	SFT00003
SFT ASG Enabling FTSW fn	
SFT Secure File Transfer	SFT00001
SFT Secure File Transfer	
UTA ASG Enabling TA/SW	UTA00002
UTA ASG Enabling TASW fn	

Software order codes

Name	Order code
PLAT SDM STD FT Platform PLAT HiSpeed Log I/F PLAT SDM STD S/W	PLAT0005
CMNO Base001 CMNO FTAM001 CMNO x25L001	CMNO0002

Software delivery

New software is made available through the following methods:

- non-computing load (NCL), a major release of the software scheduled once or twice a year, delivered on tape
- maintenance non-computing load (MNCL), a maintenance release scheduled approximately every three months for the first year of a released NCL, delivered on tape
- SDM patching, fix filesets delivered electronically as soon as they are available

The SDM supports software streams of up to three releases back from the latest release. When upgrading your SDM software from one release to another, ensure that the computing module (CM) load release on the DMS core is not higher than the software release on the SDM. Upgrade the SDM to the latest release of the software before you upgrade the DMS core load. Upgrading a DMS core to a release ahead of the SDM+ creates an unsupported configuration.

For information on upgrading your SDM to the latest software release, refer to one of the following procedures in the SDM Upgrades document:

- “Upgrading SDM software”
- “Upgrading SDM software using ESUP”

For information on upgrading your SDM with software fixes, refer to the procedure “Upgrading the SDM with software fixes” in the Upgrades document.

User interfaces overview

Functional overview

The SDM supports local area network (LAN)-based input/output (I/O) interfaces to the components in the following table.

Components with interface to the SDM

Component	Description
Workstation	Configured as remote user interface (UI) client for SDM applications; requires open software foundation (OSF) distributed computing environment (DCE) client software ***Note:*** UI client performance depends on workstation performance.
Hub	Required for 10Base-T or unshielded twisted pair (UTP) LANs
Router	Performs wide area networking (WAN) for SDM graphical user interfaces (GUI); provides gateway (or protocol translator) functions ***Note:*** Routers in a Succession Network must support BOOTP forwarding.
Terminal server	Provides asynchronous access to the SDM; ports used either instead of, or in addition to, integrated asynchronous application ports; engineering rules applications determine the number of required asynchronous ports

Workstations

The following table lists the workstations that can be configured as UI clients for SDM applications.

Workstations that support UI clients

Workstation	Operating system
Hewlett-Packard 700/800 series	HP-UX 10.20 with HP DCE version 1.5 (based on OSF DCE version 1.1)
Sun SPARC	Solaris 2.7, 2.8, 2.9 (to current) with IBM DCE version 3.2 (based on OSF DCE version 1.2.2)

Access to some functions requires the use of Secure Shell (SSH)-compatible client software for access to secure telnet and ftp services (via the SSH standard). SSH clients are supplied bundled with some operating systems, but may need to be obtained separately. The

following table lists some sources for SSH clients; sources are not limited to those listed in this table.

Sources for SSH clients

Source	Type
PUTTY	freeware
OpenSSH ***Note:*** For more information about OpenSSH, refer to OpenSSH overview on page 81.	freeware
SSH Inc.	commercial
Secure CRT	commercial
WinSCP	freeware

Maintenance interfaces

The following table lists the maintenance interfaces for the SDM.

SDM maintenance interfaces

Interface	Description
MAP (maintenance and administration position) CI (MAPCI)	Primary access to the Core for maintenance during normal SDM-to-Core operations. A dedicated SDM maintenance subsystem at the APPL level of the MAP allows users to • determine the node status and operating condition of the SDM • change the state of the SDM for maintenance • determine the status of connectivity between the Core and the SDM • reboot or halt the SDM • change the state of SDM hardware • use the QUERYSDM command to determine the status of SDM applications and operating system, including faults that currently affect applications and system software resources
SDM maintenance	Secondary access from the SDM for maintenance when SDM-to-Core communication is interrupted (CM is unavailable). Provides • control and maintenance access to all maintenance capabilities normally available through the MAP interface when connectivity to the CM is not available • control and maintenance of SDM hardware, and of individual SDM application packages • complete administration capabilities, including software and user administration and configuration changes

Accessing the Core

Support for the SDM requires access to Core-based maintenance interfaces, such as the Maintenance and Administration Position (MAP). The method used to access the Core helps identify the scope of activities that can be performed on the SDM.

Types of Core access

The SDM requires two types of access to the Core:

- Primary
- Secondary

Having two types of access allows staff to perform configuration, maintenance, and operations activities in most fault scenarios. Offices should have mechanisms and procedures to support both types of access.

Primary access

Primary access is the normal method of access available to most staff. Primary access is suitable for most maintenance activities that do not affect service.

Secondary access

Secondary access is the emergency method of access available to a restricted group of office and support staff. Secondary access requires direct access to console ports and reset terminal interface (RTIF) terminals.

Secondary access is suitable for most maintenance activities that affect service. The following types of activities are performed through secondary access:

- Core restarts
- Core maintenance switch of activity
- Changes to tables IPNETWRK and IPHOST
- Changes in state of the following network elements:
  - Ethernet interface unit (EIU)
  - Link peripheral processor (LPP)
  - SDM
- Software upgrades

Methods of Core access

The SDM offers the following methods to access the Core:

- Local access through Core console
- Remote access through Core console
- Telnet access through terminal server
- Telnet access through EIU
- Nortel Networks access applications

- Telnet access through SDM
- Local access through SDM console
- Telnet access through a terminal server with Atlantic Systems Group (ATA) Universal Terminal Access (UTA)
- Telnet access through a terminal server with ASG UTA

Note: A secure shell (SSH) client is available in some releases as an alternative to telnet.

Core console

The Core console is a VT100 console physically connected to the input-output controller (IOC)/input- output module (IOM) port in the Core. The console provides two types of access:

- Local access at the console
- Remote access through a modem to the console

The Core console has an RS-232 connection to the IOC/IOM port. Remote access requires a modem and an analog telephone line to the modem.

Terminal server

Some offices use a terminal server to provide remote access to the Core through a local area network (LAN) or a wide area network (WAN). A terminal server can provide access through a LAN/WAN to the following ports and devices:

- RTIF
- IOC/IOM port
- SDM SP0 and SP1 ports

To access the Core through a terminal server, perform the following tasks:

1. From a workstation on the LAN/WAN, telnet to the terminal server.
2. From the terminal server, manually log in to the Core with a Core userid.

The terminal server uses Transmission Control Protocol (TCP) for LAN/WAN communications and an RS-232 connection to the switch-based device or port.

EIU

The EIU is an optional component in XA-Core configurations. To access the Core through the EIU, perform the following tasks:

1. From a workstation on the LAN/WAN, telnet to the EIU.
2. From the EIU, manually log in to the Core with a Core userid.

The EIU uses TCP for communications to the LAN/WAN and the Core.

Nortel Networks access applications

The following Nortel Networks applications provide access to the Core:

- ASCII Terminal Application (ATA)
- Enhanced Terminal Application (ETA).

The SDM Configuration module in this documentation suite provides procedures to use these applications to access the Core.

ATA and ETA use the following interfaces to access the Core:

- Distributed Computing Environment (DCE) cell for access to client and server applications
- TCP for communications to the Core and LAN/WAN-based nodes
- DCE/TCP/User Datagram Protocol (UDP) for LAN-based communications to DCE security servers and the SDM

SDM

The SDM provides indirect telnet access to the Core. To access the Core through the SDM, perform the following tasks:

1. From a workstation on the LAN/WAN, telnet to the SDM.
2. Manually log in to the SDM as admin user.
3. From the SDM, telnet to the Core over the DS-512 link.
4. Manually log in to the Core with a Core userid.

The SDM uses TCP for communications to the Core and LAN/WAN-based nodes.

SDM console

The SDM console is a VT100 console physically connected to the SP0 port on the SDM. The SDM console provides indirect access to the

Core. To access the Core through the SDM console, perform the following tasks:

1. Manually log in to the SDM console as an admin user.
2. Telnet to the Core over the DS-512 link.
3. Manually log into the Core with a Core userid.

ASG UTA

ASG UTA is a third-party application that provides secure access to the Core. ASG UTA is an optional application available with some releases. Consult the ASG UTA documentation for information on this product.

Comparison of methods

The following table compares the characteristics of each access method.

Table 1 Comparison of Core access methods

Method	# sessions per port	Speed	LAN/WAN interface	SDM/LAN interface	SDM/Core interface	SDM-based applications	Type of access	Remote Access	Terminal security	Re-connect after SWACT
Local access through Core console	1	2400 baud	N	N	N	N	S	N	Y	Y
Remote access through Core console	1	2400 baud	N	N	N	N	S	Y	N	Y
Telnet access through terminal server	1	2400 baud	Y	N	N	N	S	Y	N	Y
Telnet access through EIU	30	30 kbps	Y	N	N	N	P	Y	N	N
Nortel Networks access applications	64 per SDM	30 kbps	Y	Y	Y	• DCE • ATA • Telnet	P	Y	N	N
Telnet access through SDM	16 per SDM	20 kbps	Y	Y	Y	Telnet		Y		N
Local access through SDM console	1	9600 baud	N	N	Y	Telnet		Y	Y	N

Note: *Type of access* identifies the type of access suited for the method. *P* represents Primary access and *S* represents Secondary access.

Accessing the SDM

Support for the SDM requires access to Core-based maintenance interfaces, such as the Maintenance and Administration Position

(MAP). The method used to access the Core helps identify the scope of activities that can be performed on the SDM.

Methods of access

Use the following methods to access the SDM.

- Local access through SDM console
- Remote access through Core console
- Telnet access through the operating company local area network (LAN)
- Nortel Networks access applications
- SDMRLOGIN

SDM console

The SDM console is a VT100 console physically connected to the console port (SP0) on the CPU controller module on the SDM. The console provides two types of access:

- Local access at the console
- Remote access through a modem to the console

The SDM console uses a null modem cable to connect to the SDM. Remote access requires a modem and an analog telephone line to the modem.

LAN

Some operating companies allow telnet access through the local LAN. This method of access requires telnet enabled on the SDM.

SDMRLOGIN

SDMRLOGIN is a non-menu command available at any level of the maintenance and administration position (MAP). SDMRLOGIN creates a telnet session from Core to the SDMCS 2000 Core Manager. Use the command to access SDM nodes that are either in service (InSv) or in-service trouble (ISTb). Both maint and root users can use SDMRLOGIN.

> ***Note:*** SDMRLOGIN is supported only on DS-512 connected core managers.

Restricted shell commands An SDMRLOGIN session accesses a restricted shell on the SDM which provides a limited set of commands. Type **help** within an SDMRLOGIN session to display a list of available

commands. The following table lists some of the commands available during an SDMRLOGIN session.

Note: SDMRLOGIN commands are case-sensitive.

Commands available during an SDMRLOGIN session

Command	Function
AFTAdd (see Note 1)	Adds a new AFT session
AFTAddfile (see Note 1)	Adds a file to an AFT session transfer list
AFTAlarm (see Note 1)	Queries or cancels AFT session alarms
AFTChange (see Note 1)	Changes the value of retry attempts for an AFT session
AFTDelete (see Note 1)	Deletes an AFT session
AFTList (see Note 1)	Lists configuration information about AFT sessions
AFTListfile (see Note 1)	Lists processed files for a stream
AFTQuery (see Note 1)	Queries and displays data about an AFT session
AFTRsetfile (see Note 1)	Resets the state of a file for an AFT session
AFTSetfile (see Note 1)	Sets override file or deletes a file from a list
AFTStart (see Note 1)	Starts an existing AFT session
AFTStop (see Note 1)	Stops an existing AFT session
amadump (see Note 2)	Displays record information contained in a billing file
awk	Pattern-directed scaling and processing language
bsyapp	Busies an application
closec (see Note 2)	Closes currently open billing file or files for each stream
CONFSTRM.act (see Note 2)	Activates a filtered stream
Note 1: Applies only to SuperNode Billing Application (SBA) Automatic File Transfer (AFT). ***Note 2:*** Applies only to SBA.	

Commands available during an SDMRLOGIN session

Command	Function
CONFSTRM.add (see Note 2)	Adds a configured billing stream
CONFSTRM.change (see Note 2)	Changes an existing billing stream configuration
CONFSTRM.deact (see Note 2)	Deactivates a filtered stream
CONFSTRM.delete (see Note 2)	Deletes an existing billing stream configuration
CONFSTRM.list (see Note 2)	Lists configuration of a single billing stream or all billing streams
CONFSTRM.start (see Note 2)	Resumes receiving records on a filtered stream
CONFSTRM.stop (see Note 2)	Stops receiving records on a filtered stream
CONFSTRM.update (see Note 2)	Updates the criteria of a filtered stream
cut	Cuts out (extracts) selected fields of each line of a file
dispal (see Note 2)	Displays current billing alarms
displogs (see Note 2)	Displays billing logs not acknowledged by the Core
grep	Searches a file for a pattern
help	Displays generic help information
java	Java Runtime Environment
listfile (see Note 2)	Lists stored billing file or files for each stream
locate	Queries hardware module information
logout	Logs the user out of the SDM
logquery	Initiates the logquery tool to browse DMS logs
Note 1: Applies only to SuperNode Billing Application (SBA) Automatic File Transfer (AFT). ***Note 2:*** Applies only to SBA.	

Commands available during an SDMRLOGIN session

Command	Function
ls	Lists contents of the SDM remote login directory
mib (see Note 2)	Gets or sets MIB objects for billing
offlapp	Offlines an application
ping	Sends ICMP ECHO_REQUEST packets to network hosts
ps	Reports process status
query (see Note 2)	Queries SBA billing stream status
readtape.sh (see Note 2)	File used by TAPE.send; should not be called directly
rtsapp	Returns an application to service
SCHEDULE.add (see Note 2)	Adds a tuple to the schedule
SCHEDULE.change (see Note 2)	Changes an existing tuple in the schedule
SCHEDULE.delete (see Note 2)	Deletes a tuple or tuples from the schedule
SCHEDULE.list (see Note 2)	Lists a tuple or tuples in the schedule
SCHEDULE.RTBAdd (see Note 2)	Adds Real-Time Billing (RTB) to a stream
SCHEDULE.RTBBsy (see Note 2)	Busies RTB for a stream
SCHEDULE.RTBChange (see Note 2)	Changes the RTB configuration for a stream
SCHEDULE.RTBConfQuery (see Note 2)	Queries the RTB configured destinations
SCHEDULE.RTBDelete (see Note 2)	Deletes RTB from a stream
Note 1: Applies only to SuperNode Billing Application (SBA) Automatic File Transfer (AFT). ***Note 2:*** Applies only to SBA.	

Commands available during an SDMRLOGIN session

Command	Function
SCHEDULE.RTBIptest (see Note 2)	Tests the IP address used by RTB for a stream
SCHEDULE.RTBOffl (see Note 2)	Offlines RTB for a stream
SCHEDULE.RTBQuery (see Note 2)	Queries the state of RTB for a stream
SCHEDULE.RTBRts (see Note 2)	Returns RTB to service for a stream
sendfile	Sends billing file or files for each stream to downstream DPMS
TAPE.list (see Note 2)	Lists the billing files written to a digital audio tape (DAT)
TAPE.send (see Note 2)	Sends (FTP) billing files from a DAT
TAPE.write (see Note 2)	Writes billing files to a DAT
who_is_on	Displays the users logged in to the SDM
Note 1: Applies only to SuperNode Billing Application (SBA) Automatic File Transfer (AFT). ***Note 2:*** Applies only to SBA.	

Troubleshooting SDMRLOGIN errors The following errors can occur during an SDMRLOGIN session.

- The SDM is not in the InSv or ISTb state. Put the SDM in the InSv state, and re-enter the SDMRLogin command.
- A telnet session cannot be established between the CM and the SDM.
- The terminal that you are using for the remote login does not suppress the echoing of password entries. You can either continue or exit the remote login session.
- The terminal that you are using for the remote login is being used to output DMS logs. You can either continue or exit the remote login session.

Tools and utilities

Logs

Logs from the computing module (CM), other nodes within the network, and from the SuperNode Data Manager (SDM) application software are routed and stored through Generic Data Delivery (GDD). GDD maintains a /gdd directory on the SDM (in volume group datavg) of up to 30 days of logs. For more details about GDD, refer to Generic Data Delivery overview on page 67.

The Log Delivery application includes the following tools for viewing and managing log files:

- logquery
- logroute log receiver
- logroute log delivery commissioning

For more information about Log Delivery, refer to Log Delivery Application overview on page 61.

Administration

Root and maintenance (maint class) users can use tools at an SDM maintenance interface and UNIX-based utilities at a VT100 console (local or remote) to:

- commission the SDM platform
- set up root and maint user groups and passwords
- monitor system resources
- back up and restore software functions

For details about the Commissioning tool and related procedures, refer to “Using the configuration tool” in the Configuration Management document.

The AIX operating system partitions disks into logical volumes to prevent disk occupancy errors (full disk), which allows the system to read from and write to the remaining disks without interruption. Logical volumes on the SDM are equivalent to file systems.

Note: Nortel Networks provisions the SDM file system structure.

Maintenance class users can monitor file system partitioning, but cannot modify the logical volumes. Root users can modify the logical volumes.

Operational Measurement Delivery overview

Functional overview

The SDMCBM 800 Operational Measurement Delivery (OMD) application collects customer-defined operational measurement (OM) data from the DMS switch, and stores the data in OM report files on the SDMCBM 800 in comma-separated value (CSV) format. The OMD application is configured using the OM user interface (OMUI).

An OM report file is a collection of OM groups that are monitored at selected reporting intervals. Secure File Transfer (SFT) or File Transfer Protocol (FTP) sends OM report files from the SDMCBM 800 to an operations support system (OSS). (For more information about SFT, refer to Secure File Transfer overview on page 53.) A data browser such as a spreadsheet program provides access to the contents of the files.

Report elements

Report elements define the content of OM report files, and combine content of related OM groups for monitoring and analysis. A report element contains a user-defined report element name, a reporting interval for a report element (five minutes, or the office transfer period of 15 or 30 minutes), and names of the OM groups and registers.

Subtraction profiles

The subtraction profile determines the change in the value of an OM group register between five-minute OM reports, as defined in a report element. The subtraction profile applies only when the reporting interval is set to five minutes. The following table lists the types of subtraction profiles.

Subtraction profiles

Type	Description
Single	A single register represents a running total
Double	Two registers (base and extension) represent a running total
Non-subtraction	Subtraction is not performed on selected registers

Data collection schedules

A data collection schedule defines start and stop times for OM report collection. The collecting interval determines how often in the time

period an OM report collection occurs. The data is collected to the same report file for schedules with collecting intervals after midnight. The following table lists the data collection schedule types.

Data collection schedule repetition types

Repetition	Schedule information
Daily	Daily start and stop time. Format: `hhmm`, *where* `hh` = hour (00 to 24), and `mm` = minute (00 or 30). Specifies only a single time period; for multiple time periods in the same day, you must define multiple schedules.
Weekly	Weekly start and stop time. Values: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday. Format: `hhmm`; multiple days can be specified in same schedule.
Monthly	Monthly start and stop time. Values:1 to 31. Format: `hhmm`; multiple days can be specified in the same schedule.

File rotation schedules

File rotation schedules specify when to rotate report files. File rotation closes an open report file and moves it to the */omdata/closedNotSent* directory on the SDMCBM 800. Each file rotation schedule contains

- a user-defined file rotation schedule name
- a repetition rate for the rotation schedule based on either the number of report records collected or the number of hours to collect records
- a schedule that defines the time to rotate the report file

The data collection and file rotation schedules operate independently of each other. If a file rotation schedule event occurs during a scheduled data collection period, the file rotation schedule closes and rotates the OM report file, and a new OM report file with the same name is opened. The new file starts collecting immediately and continues until the end of the collection period. The open OM report file remains in the */omdata/open* directory until the file rotation schedule closes it and rotates it to the */omdata/closedNotSent* directory.

File transfer destinations

File transfer destinations define remote downstream destinations of OM report files. Each destination entry contains

- a user-defined file transfer destination name
- the valid IP address of a remote destination host (xxx.xxx.xxx.xxx)

- the FTP port address of the remote host (default: 21)
- the remote host login ID and password

Note: The SDMCBM 800 does not authenticate the IP and port addresses or the login ID and password.

An invalid destination causes the file transfer to fail. When a file fails to transfer, log entries are written to the customer log file at */var/adm/custlog*. The file is not re-sent, and the report file must be transferred manually using either the OMFTP command, SFT or standard FTP.

File transfer schedules

File transfer schedules specify when to transfer OM report files downstream. The files are transferred downstream using FTP, and move from the */omdata/closedNotSent* directory to the */omdata/closedSent* directory. If a scheduled file transfer fails, the report file moves to the */omdata/closedSent* directory, and log entries are written to the customer log file at */var/adm/custlog*. Because the OMD application does not resend the report file, it must be transferred manually using the OMFTP command.

Each file transfer schedule contains a

- user-defined file transfer schedule name
- repetition rate for the transfer schedule
- schedule defining when to transfer the report file (if using a repetition rate)
- remote file transfer destination host system (<16 destinations/schedule)
- destination storage directory for each defined transfer destination

Report registrations

A report registration links information from the report element and schedules for data collection, file rotation and file transfer to collect OM data. The user can create up to 32 report registrations. Once a report registration has been created, it can be deleted but not modified. Each report registration contains user-defined names for the report registration, report elements and each schedule type. The schedules become active immediately after the creation of the report registration.

An OM report file opened by the data collection schedule in the */omdata/open* directory uses the name of the report registration as part of the OM report file name. Linking a file transfer schedule into a report registration provides regular and automatic transfers of OM report files

to remote downstream destinations. Unless you link a file transfer schedule to a report registration, you must manually transfer your OM report files downstream.

Report registration limit

The report registration limit is the maximum number of report registrations that can be configured on an SDMa CBM 800 without affecting processing performance. The number of report registrations range from 1 to 32 (default value: 32). To set the limit, use the “Set Report Registration Limit” from the OMUI main menu.

File retention periods

A cleanup of OM report files that have been sent downstream automatically occurs every night at midnight (00:00 or 24:00). Files in the */omdata/closedSent* directory are deleted at an interval based on the file retention period defined in the OMUI (range: 1 to 14 days). The default interval is set to 7 days at OMD installation. Unsent OM report files older than 32 days in the */omdata/closedNotSent* directory are deleted. This 32-day default value is read from a configuration file set up when the SDMCBM 800 is commissioned.

OMD data collection capacity

To determine the number of tuples in an OM group, either monitor the OM group and count the tuples in the report file or use the OMSHOW command from the MAP (maintenance and administration position) on the DMS switch.

The following table lists the current OMD data collection capacity.

Note: Collection of more than these maximum tuples will reduce SDM performance and retention period for OM report files.

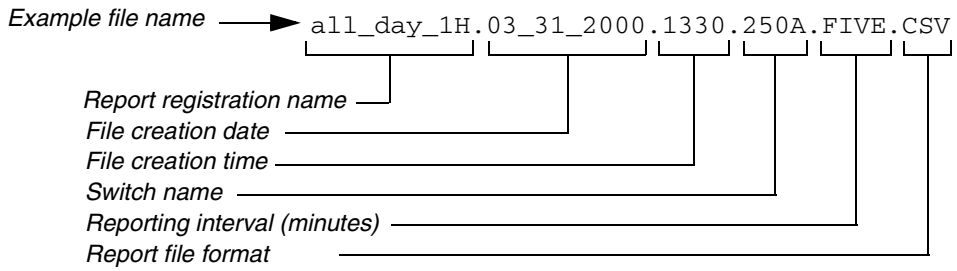
OMD maximum data collection capacity

Transfer type	Capacity (number of tuples)
5-minute	6000
15-minute	12,000
30-minute	24,000

OM report file naming

Report files are named according to the report registration name, file creation date and time, name of the switch generating the OMs, and

reporting interval. Refer to the following example file name and explanation.



OM report file contents

Tuple information for an OM group can be viewed in CSV format from the OM report file on the SDMCBM 800, and by entering the OMSHOW command on the MAP. The following table shows an OM report file.

Contents of an OM report file

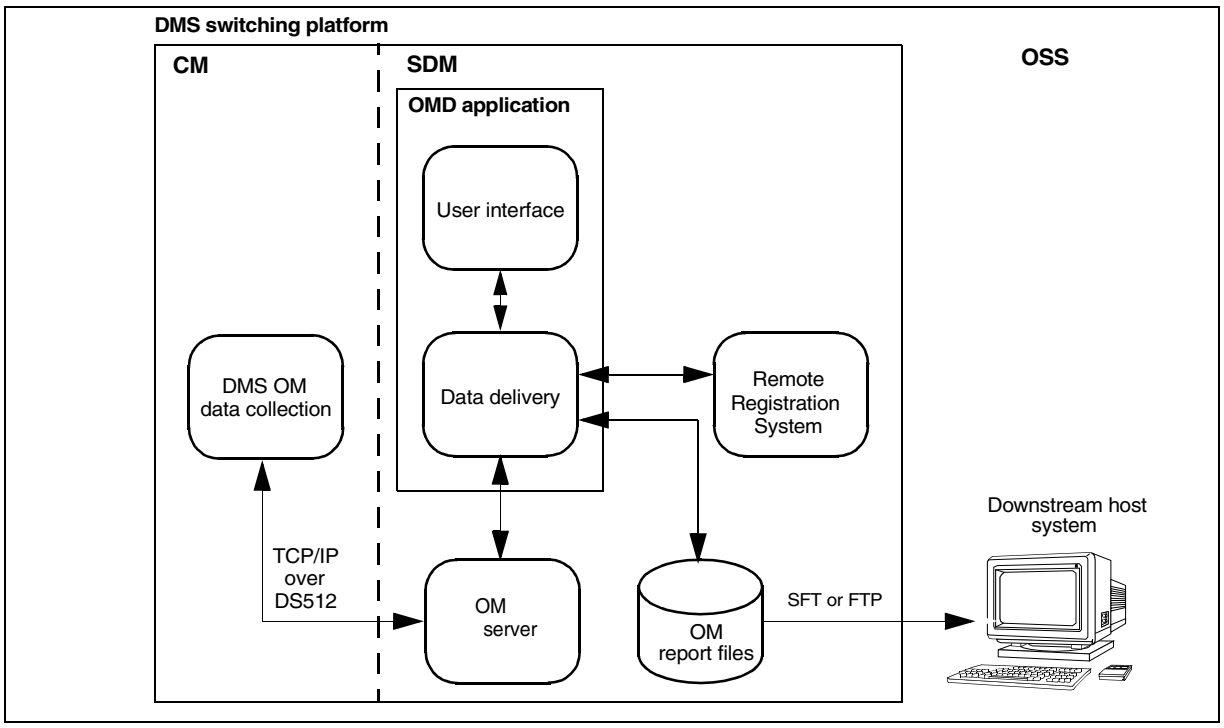
Date	Time	Switch Names	Group Name	Key/Info Field	Reg1 Name	Reg1 Value	Reg2 Name	Reg2 Value	Reg31 Name	Reg31 Value
2/23/00	3:35 :00	250U	TRK	ISU_GWC.2W.0.0	AOF	0	ANF	0		
2/23/00	3:35 :00	250U	TRK	ESADGTR.OG.0.0	AOF	0	ANF	0		
2/23/00	3:35 :00	250U	TRK	HSET.OG.3.0	AOF	0	ANF	0		
2/23/00	3:35 :00	250U	TRK	JACK.OG.2.0	AOF	0	ANF	0		
2/23/00	3:35 :00	250U	TRK	LTU.OG.2.0	AOF	0	ANF	0		
2/23/00	3:35 :00	250U	TRK	MONTALK.OG.0.0	AOF	0	ANF	0		
2/23/00	3:35 :00	250U	TRK	OCKT.OG.0.0	AOF	0	ANF	0		

Hardware

The following figure shows the architecture and interactions between the components in the CM, SDMCBM 800 and OSS.

CBM 800**OM delivery components**

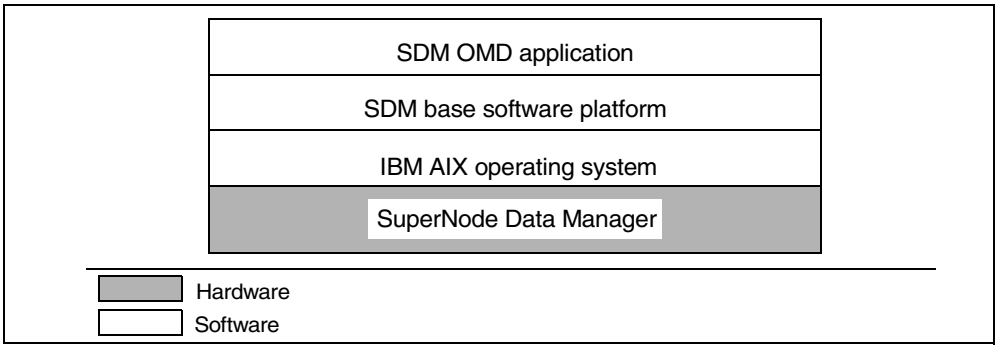
SDM OM delivery components



Software

The SDMCBM 800 base software platform runs on the IBM AIX operating system. The SDMCBM 800 OMD application runs on the SDMCBM 800 base software platform layer. The following figure illustrates the software architecture.

Software overview



The following table lists the subsystems and components of the SDMCBM 800 OMD application.

SDMCBM 800 **OMD subsystem and components**

Subsystem/component	Description
Data delivery	Manages OM requests/reports; builds OM report files; encodes OM data into a usable format.
OM user interface (OMUI)	Menu-driven, text-based UI that starts from the user prompt on the SDMCBM 800. Allows the user to • configure OMD application and data delivery • configure, list, delete or modify report elements, collection schedules, file rotation schedule, file transfer destination, file transfer schedule. User can configure up to 50 each of these components on the SDMCBM 800.

SuperNode Billing Application overview

Functional description

SuperNode Billing Application (SBA) runs on the SDM and Core platforms. The Core receives formatted billing records, buffers them, and sends them to the SDM for storage in files until they are sent to downstream billing processors.

For complete information about the SBA, and about tools related to SBA processing, refer to “*SDM Accounting*, NN10125-811”.

Enhanced Terminal Access overview

Functional overview

The Enhanced Terminal Access (ETA) application provides secure remote access to the SDM across transmission control protocol/Internet protocol (TCP/IP)-based local- and wide-area networks (LAN/WAN). ETA has a server on the SDM and either an ETA client or an ASCII Terminal Access (ATA) client. ETA supports

- SDM applications that have a command line interface, such as the SDM maintenance interface
- SDM UNIX shells
- the computing module (CM) command interpreter (CI)
- MAP (maintenance and administration position)

Encryption protects information sent between the ETA server and the ETA clients, and between the ETA server and the SDM or CM.

Components

ETA has one server application installed on the SDM, two client applications, and Distributed Computing Environment (DCE) client user profiles. The two client applications can be used at the same time on the network. The following table describes the components of ETA.

ETA components

Component	Description
ETA server	Provides Telnet emulation of CM and SDM for ETA and ATA clients; logs client applications into CM and SDM; handles information exchange between the CM and SDM and clients; supports a maximum of 50 CM sessions. Maximum number of sessions depends on number of TCP sessions used on DMS (configured in Table IPHOST in DMS switch); supports up to 64 SDM sessions.
ETA client	Connects to ETA server to perform CM and SDM terminal sessions; has graphical user interface (GUI); allows user to change DCE password. UNIX platforms that support ETA clients are Hewlett-Packard (HP) and SUN.

ETA components

Component	Description
ATA client	Connects to ETA service to perform CM and SDM terminal sessions; has command line interface; does not allow user to change DCE password.
DCE security server	Validates users; used by system administrator to configure and store user profiles, which determine user access privileges to ETA, CM and SDM. (UserIDs must be set up in DCE before using ETA.) For more information about DCE, refer to Secure File Transfer overview on page 53.

ETA control characters

The ETA server uses control character and break sequences that are supported through input/output controller (IOC)-based VT100 type terminals. The control sequences in the following table are available on both ETA and ATA clients for SDM and CM-hosted sessions.

ETA control characters

Character	Function
Ctrl B	Toggles break mode ON or OFF ***Note:*** The break sequences are CM-specific. Once you enter the break mode, you can use all available break commands. The keyboard sequence, Ctrl-B, is used to toggle the break sequences ON or OFF.
Ctrl E	Deletes all characters from the cursor position to the end of the line
Ctrl F	Moves the cursor 1 position to the right
Ctrl H	Moves the cursor 1 position to the left
Ctrl I	Places the terminal in insert mode
Ctrl Q	Allows the screen to scroll
Ctrl S	Prevents the screen from scrolling
Ctrl U	Erases the entire line
Ctrl X	Exits from insert mode

ETA control characters

Character	Function
Ctrl \	Toggles control character sequence ON or OFF ***Note:*** The ETA control character sequences can interfere with other tools. To use a tool like the UNIX editor vi or the UNIX command passwd, you must turn off the ETA control characters. For CM- and SDM-hosted sessions, the control characters are off by default.
Delete key	Deletes the current character
?	Recalls one of the last three lines (depending on the number of ?s)

File transfer overview

Functional overview

File transfer can be accomplished with FTP, Secure File Transfer (SFT), or File Transfer Protocol Proxy (FTPP).

In an SFT session, the SFT client can access either the SDM, or the computing module (CM) for the purpose of doing file transfers. You must have a DCE account and password to use SFT. (If you do not have a DCE account, your DCE administrator can create one for you.)

FTP clients can access the CM FTP server by typing SITE CM. You can use standard FTP commands with some exceptions.

Installing the regular and secure file transfer software

Installing file transfer software is described in the SDM Configuration Management document.

The SWIM package provides the user interface (UI) for local SDM software installation and maintenance. You can access SWIM from the SDMmaintenance interface (sdmmtc).

Before you can perform an installation using SWIM, you must have the SDM base software installed on the SDM.

ATTENTION

Risk of revealing the administrative user password:
To prevent this security risk, Nortel Networks recommends that you execute the command from a terminal attached to the SDM console port. If you use telnet to access the SDM remotely, and use the default sdm_admin or cell_admin “master administrator” account to add the FTP proxy server, the system sends the password of the administrative user in clear text across the network.

Secure File Transfer overview

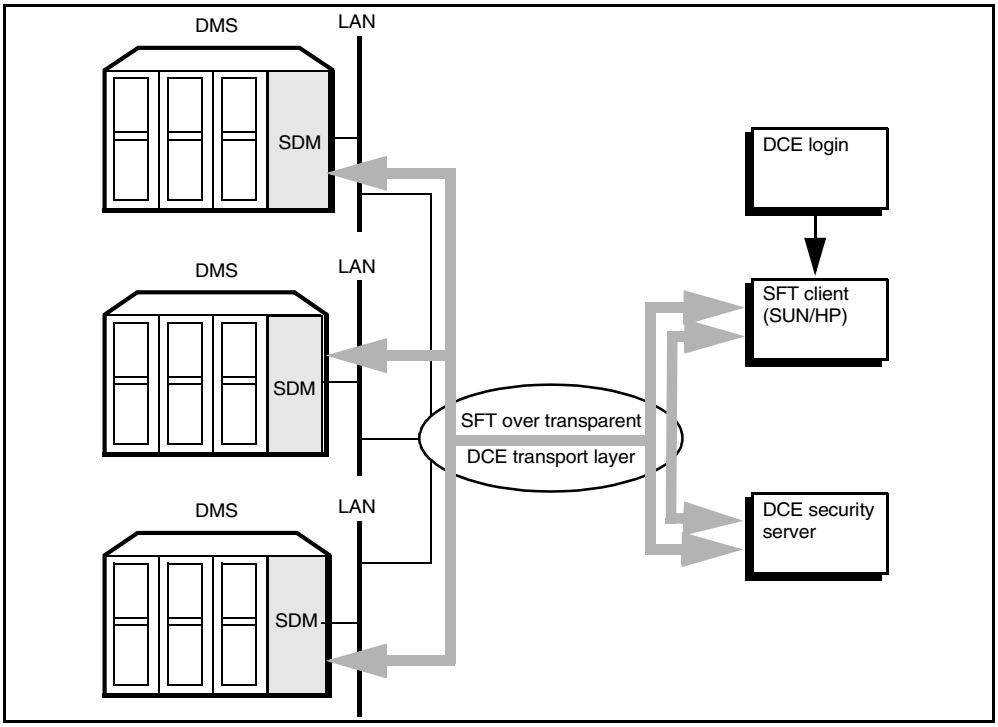
Functional description

The Secure File Transfer (SFT) application provides file transfer to or from a DMS SuperNode or SDM across local- and wide-area networks (LAN/WAN). The SFT application can be either Distributed Computing Environment (DCE)-based or non-DCE based.

DCE-based configuration

The SFT uses DCE security servers to validate users. The SFT server and client user must be configured in the DCE cell. A remote procedure call (RPC) sets up the transparent Transmission Control Protocol/Internet Protocol (TCP/IP) connection for user validation. The following figure shows the components of the DCE-based SFT.

DCE-based SFT application



The following table describes the components of the DCE-based SFT.

Components of DCE-based SFT

Component	Description
SFT client	Provides secure file transfers to and from the SDM and the CM. Runs on Hewlett-Packard (HP) and Sun SPARC platforms on remote workstations. DCE security server authenticates login. For a list of specific platforms, refer to User interfaces overview on page 21.
SFT server	Transfers files to and from remote SFT or FTP clients. Requires SDMN0009 or higher operating systems.
CM server	Provides file transfer service to and from the CM storage devices; number of concurrent sessions limited to available FTP server connections on the CM. Each connection to CM uses specially assigned UserID. System randomly generates password.
DCE security server	Contains the database of extended registry attributes (ERA) that store SFT client user profiles. Authenticates SFT client UserID, password, and server. Login requires UserID and password.

The DCE-based SFT application supports a single login. UserIDs and passwords are encrypted and correspond to a DCE security account. For more information on logging in to DCE, refer to “Configuring the SFT server application software” in the Configuration management document. The following table describes workstation login configurations.

DCE login configurations

Login type	Description
Integrated	Login session begins when you log on to UNIX
Non-integrated	User profile includes a DCE login command; DCE authentication occurs once for each work session
No DCE	SFT starts without login to DCE; SFT client prompts for the DCE UserID and password each time the SFT client starts

Non-DCE-based configuration

The non-DCE SFT configuration uses standard file transfer protocol (FTP) to send un-encrypted (ASCII text) login UserIDs and passwords across the network from the FTP client to the SFT server. Because the

configuration does not provide user authentication, it does not offer secure file transfer.

Because the DCE security server is not present in a non-DCE based configuration, a DCE login is not required. Instead of a single login, the user enters a UNIX login for each SDM. The following figure shows how an FTP client uses FTP to connect to the CM and the SDM.

Non-DCE based SFT application

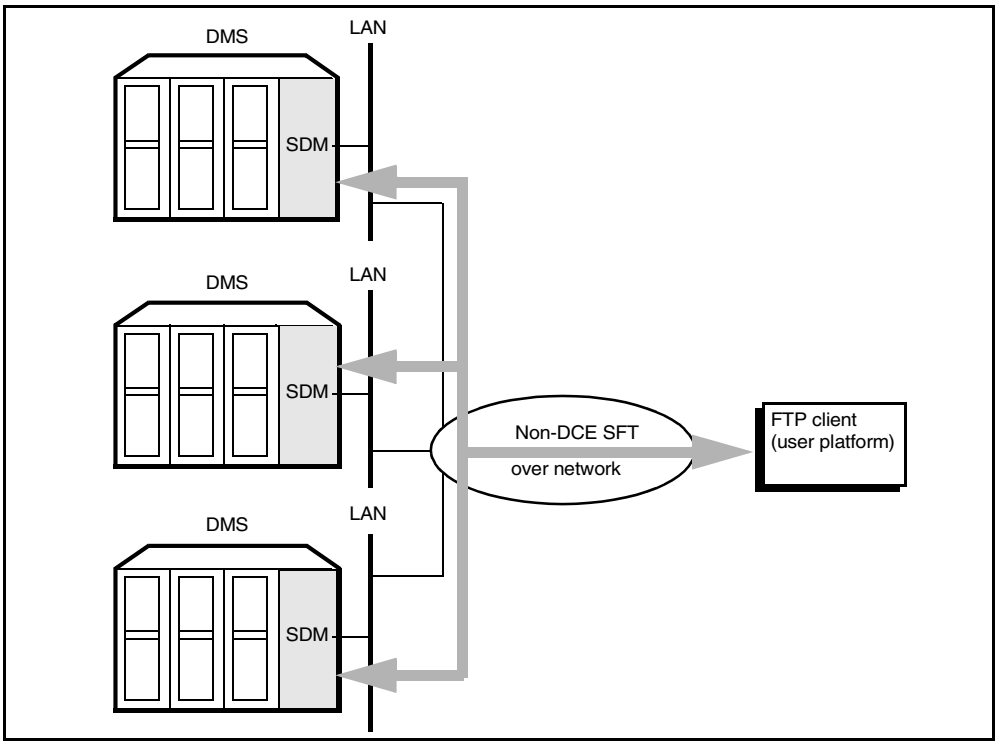


Image Dump Service Application overview

Functional description

The Image Dump Service application on the SDM is an interface between the system load module (SLM) on the call server's computing module (CM) and the SDM. The purpose of the image dump service application is to reduce the amount of time the CM restricts table changes when performing an image dump.

The CM sends a partial image dump to the SDM. The SDM stores the partial image on a local disk. After the transfer, the CM allows table changes and completes the image dump of the data on the SDM to the CM's SLM drive in the background. The image dump data is deleted immediately after the CM completes the image dump process.

The CM controls the image dump application. The SDM acts only as a temporary storage device.

The image dump service application is installed and removed using the Software Inventory Manager (SWIM).

Software inventory manager (SWIM) overview

Functional description

The software inventory manager (SWIM) provides you with an easy-to-use interface to perform the following tasks:

- install new software
- install and schedule the automatic application of software fixes
- update existing software with a newer version
- remove existing software
- sort and toggle the filesets listed
- view the history of when software was applied, removed, or configured
- change the software source
- configure software

You can access the SWIM level from anywhere in the maintenance interface by typing **swim** and pressing the Enter key.

The SWIM level displays the filesets that differ from the defined load, the status of those filesets, and the product code and version of the installed software load. The Details level displays a list of all the filesets that exist on the system and their status. The Fixes level displays a list of the fix filesets that exist in the predefined fixes directory and their status.

Use the Help command at the SWIM level or any of its sublevels to obtain information on the commands available at that level, as well as the meaning of the fileset status. An example of the SWIM level is provided in the following figure.

Example of SWIM level screen

```
   SDM    CON     512    NET    APPL    SYS    HW    CLLI: MSH2XACORE
    .      .      ..      .      .      .      .    Host: pcary71c
                  ..                                 Fault Tolerant


SWIM
 0 Quit          Product Code                          Version
 2 Apply         CS2E0006                              6.0
 3 Details
 4 Fixes      Fix Fileset Description          Version       Status
 5 Config     SSH Secure File Transfer         18.20.0.0     NEW
 6 Options    CS2E0006.0                       19.72.0.0     NEW
 7 History
 8                                      Fileset Status: 1 to 2 of 2
 9
10
11
12 Up
13 Down
14 Search
15
16 View
17 Help
18 Refresh
  root
Time 15:28 >
```

SWIM modes

SWIM operates in read-only mode and full-function mode.

- Read-only mode lets you view the version and state of the filesets currently installed. You can also use this mode to view history information for filesets. When the platform is running in split-mode, only read-only mode is available on the SYSOLD side while SYSNEW is upgraded. SWIM is available to the maintenance user in read-only mode.

  Note: The Fixes level is not accessible in read-only mode.

- full-function mode lets you use all of the SWIM functions; however, you must be a root user. When the system is running in split-mode, the full-function mode is available on the SYSNEW side only.

Log Delivery Application overview

Functional description

The Log Delivery Application consists of a group of application filesets that run on the SDM. The following table describes the application filesets that must be installed for full operation of the Log Delivery Application.

Log Delivery Application filesets

Fileset	Description
Log delivery service (SDM_BASE.logs)	Collects logs generated by the SDM, the computing module on the call server, and other network elements, and delivers them to operational support systems (OSS). It includes the *logquery* and *logroute* tools.
Log delivery service client (SDM_BASE.logs.client)	Runs on a remote workstation, and includes the *logreceiver* tool.
Generic data delivery (GDD) (SDM_BASE.gdd)	Provides a permanent storage mechanism for logs. (See Generic Data Delivery overview on page 67.)

For details about installing the tools and filesets required by the Log Delivery Application, refer to the procedure “Installing and configuring the Log Delivery Application” in the Configuration Management document.

Log Delivery Application tools

The Log Delivery Application in the SDM base software platform sends user-defined streams of DMS, SDM, and other logs generated by different nodes to a maximum of 30 operations support systems (OSS) and 30 UNIX files on the SDM. A maximum of 30 Log Delivery output devices can be commissioned. (The maximum includes the sum of Transmission Control Protocol/Internet Protocol (TCP/IP) links and UNIX files.) The application delivers DMS logs from LogUtil.

Log Delivery provides the tools listed in the following table.

Tools in the Log Delivery Application

Tool	Description
Logquery	Allows you to view logs stored in the generic data delivery (/gdd) directory
Logroute logreceiver	A client application that receives SDM logs sent over a TCP/IP connection through the operating company local area network (LAN) for storage and viewing on remote workstations
Logroute log delivery commissioning	Sends logs over a TCP/IP to either a LAN or a UNIX file device; allows you to • view, set, and modify global application parameters, including buffer size, reconnect time-out value, lost logs threshold (number of lost logs before a system log is generated), and ASCII line and log delimiter characters. • delete logs and log types • modify the output device list (parameters, device type, format) • modify incoming log streams from the CM and number of days to store logs in /gdd. Changing the number of days to store logs erases logs older than the number of days specified from /gdd. ***Note:*** Settings changed by the Log Delivery global parameters menu do not affect GDD settings or the logs in /gdd volume.

The logroute log commissioning tool includes an online help facility that provides valid parameter ranges and default values. To route logs from an SDM to a workstation, the SDM must be configured to send logs to a TCP device with an IP address that matches the IP address of the workstation.

CAUTION

The logroute tool does not have a locking mechanism and must be run by only one user at a time. Otherwise, changes made by one user can overwrite those of another user.

Log formatting

The Log Delivery Application formats logs using Nortel Networks standard (STD) or Switching Control Center 2 (SCC2) format. Formatting can be set for each device.

Log Delivery procedures

The following table includes a list of procedures associated with the Log Delivery Application and tools.

Log Delivery procedures

If you want to	Use procedure
access log devices from a remote location	"Accessing TCP and TCP-IN log devices from a remote location" in the Fault Management document
add a TCP, TCP-IN, or file device	"Configuring an SDM for log delivery" in the Configuration Management document
modify parameters for an existing device	"Modifying a log device using logroute" in the Configuration Management document
specify logs to be delivered to a specific device	• for a new device, use "Configuring an SDM for log delivery" in the Configuration Management document • for an existing device, use "Modifying a log device using logroute" in the Configuration Management document
delete a log device	"Deleting a device using logroute" in the Configuration Management document
define the set of logs sent from the CM	"Specifying the logs delivered from the CM to the SDM" in the Configuration Management document
change the log delivery global parameters (applicable to all devices)	"Configuring the Log Delivery global parameters" in the Configuration Management document
configure the Generic Data Delivery (GDD) parameter	"Configuring GDD parameter using logroute" in the Configuration Management document

Log Delivery procedures

If you want to	Use procedure
display log records	“Displaying or storing log records using logreceiver” in the Fault Management document
install log delivery service	“Installing the Log Delivery application” in the Configuration document
install the logreceiver tool	“Installing the logreceiver tool on a client workstation” in the Configuration Management document
view logs	“Retrieving and viewing log records” in the Fault Management document
store logs in a file	“Displaying or storing log records using logreceiver” in the Fault Management document
troubleshoot log delivery problems	“Troubleshooting the Log Delivery problems” in the Fault Management document

Logreceiver overview

Functional description

The logreceiver tool is a client application, included with the Log Delivery Application, that runs on a remote workstation and receives logs sent from an SDM through the operating company local area network (LAN). The logreceiver tool can either store these logs in a file or display them on the screen.

To route logs from an SDM to a workstation using the logreceiver tool, ensure that

- the logreceiver tool is installed on the workstation. Refer to the procedure “Installing the logreceiver tool” in the Configuration Management document.
- the SDM is configured to send logs to a TCP device. Refer to the procedure “Configuring an SDM for log delivery” in the Configuration Management document.

With the logreceiver tool, you can display logs directly on the workstation screen as they are generated, or store logs in a file. Refer to the procedure “Displaying or storing log records using logreceiver” in the Fault Management document.

Generic Data Delivery overview

Functional description

Generic Data Delivery (GDD) is a permanent storage mechanism that stores the previous 30 days of logs in separate files. Each file contains 12 hours of log activity (00:01 to 12:00 and 12:01 to 24:00). The log files are stored by GDD in the /gdd directory on the datavg volume (rootvg will be used if a datavg volume is not present). Because of the potential for a large number of logs to be generated, proper sizing of the /gdd directory is necessary when commissioning the SDM.

Note: At initial commissioning, the default value for the number of days to store logs in the /gdd directory is automatically set to 30.

Set the size of the /gdd directory using the following formula:

(average size of 12-hour log file) x (2 log files per 24-hour period) x (50 days)

Note: 50 days is used as an engineering figure to ensure that there is enough capacity for 30 days of logs. Nortel Networks recommends that your initial /gdd volume size be at least 300 Mbytes. This is based on a 3-Mbyte file size for each 12-hour period. The calculation, using the above formula, is: 3 Mbytes x 2 x 50 = 300.

When the number of days to store logs limit is reached (maximum=30), the logs are rotated, and the oldest log file is replaced by the newest log file.

To view log files in the /gdd volume, use the log query tool. To configure the number of days to store logs in the /gdd directory, use the logroute tool. For more information about the log query and logroute tools, refer to Tools and utilities on page 35.

Network time protocol overview

Functional description

Network time protocol (NTP) is used to synchronize the internal clocks of various network devices across large, diverse networks to universal standard time. NTP automatically adjusts the time of devices over a period of time so that they are synchronized within a millisecond (ms) on LANs and up to a few tens of milliseconds on WANs, relative to Coordinated Universal Time (UTC).

Network time protocol is commissioned on the SDM to make it the time server for the other components or nodes within the network, and can replace the use of DCE's Distributed Time Service (DTS). Refer to the procedure "Commissioning or decommissioning Network Time Protocol (NTP)" in the Configuration Management document.

GR-740 Passthrough overview

Functional description

The GR-740 software application on the SDM enables the SDM to receive GR-740 compliant messages from and deliver GR-740 compliant messages to a network data collection operations system (NDC OS) on the operating company's LAN/WAN. These messages are received and sent over a TCP/IP link in accordance to GR-740.

The GR-740 software application is installed and removed using the SDM Software Inventory Manager (SWIM), and can be configured in DCE mode (secure mode) or in non-DCE mode (insecure mode). To use GR-740 TCP/IP passthrough in secure mode, the Distributed Computing Environment (DCE) server must be installed and configured.

SPM ReachThrough overview

Functional description

The SPM ReachThrough application allows telecommunication transport monitoring and maintenance centers to query the Spectrum Peripheral Module (SPM) for monitored performance parameters on the OC-3 resource module. The feature provides transport network access to the SPM through the SDM. A customer Network Element uses Transaction Language 1 (TL1) to retrieve OC-3 performance parameter information from the SPM.

The ReachThrough Surveillance for NA100 SPM feature is optional. SPM ReachThrough includes utilization of current products with existing messaging software to transport TL1 messages between the customer network and the SPM.

Routine exercise (REX) test overview

Functional description

The REX test is designed to help detect problems in the system. You can perform the following routine exercise (REX) tests on the SDM:

- Ethernet REX
- CPU REX

You can run a specific REX test or all REX tests at any time. It is highly recommended that you run all REX tests prior to performing an upgrade.

When a REX test is invoked, log report SDM630 is generated to indicate the start time. The same log report is generated when a REX test is complete, to indicate the end time. Results from the REX test are recorded in a report stored in the /var/adm directory, which you can view at any time.

Related procedures

Refer to the procedure “Performing a REX test” in the Fault Management document to perform a REX test.

System audit overview

Functional description

A system audit consists of various system pre-checks to ensure all requirements are met before an upgrade is performed. The system audit is set to run automatically on a daily basis at 2 am (default value), and consists of the following checks:

- hardware state and faults (hw command) - ensures that the modules present on the SDM are fault-free and have a state of ‘Available’ and ‘online’
- EEPROM status (eeprom command) - ensures that no eeprom problems exist on any of the hardware modules
- AIX LVM - rootvg & datavg (lvm command)
  - ensures that there are no orphaned AIX LVM commands in the process table that could affect integration of an I/O module
  - ensures that all available volume groups are FTVG (fault tolerant) status, fully mirrored and the quorum attribute is set to “no”
  - ensures that all filesystems are mounted with no stale partitions, and that the mount point for each logical volume matches the label
  - ensure that all datavg filesystems are properly created under the datavg volume group in a rootvg/datavg system
  - ensures that all the physical volumes are created and paired, the physical volume identifier of rootvg and datavg physical volumes match the output in lspv (no bogus physical volume identification numbers), and that sufficient disk space is present on the datavg and rootvg volumes
- CPU integrity (cpu command) - verifies that the data associated with a previous split-mode has been flushed, and that the autoboot attribute has been set on the CPUs
- intersystem communication (isc command) - verifies that the intersystem communication (isc) process is not running when split mode is not running

- system resources (sys command)
  - verifies that the “maxuproc” value is set to “500”
  - verifies that the “maxmbuf” value is set to “0”
  - verifies that the “maxpout” value is set to “31”
  - verifies that the “minpout” value is set to “15”
  - verifies that the “cms_notify_meth” value is set to “/sdm/mtce/smm/smm_cms_notify”
  - verifies that the “cms_notify_attr” value is set to “condition,req_condition”
  - verifies that the DAT drive block size is set to “512”
  - verifies that no runaway processes exist
  - checks for excess CPU usage
  - verifies that the appropriate SDM processes are running
  - verifies that the autorestart flag is set to “true”

The system audit is set by default to run all checks automatically on a daily basis at 2 am. You can manually run specific checks or all checks of the system audit at any time. You can change the default time, or you can disable the system audit altogether. It is highly recommended that you keep the default setting and let the system audit run on a daily basis. If you decide to change the time of the system audit, it is recommended that you schedule it during low traffic periods.

The system audit records failures when they exist, but does not resolve the failures. Results from the system audit are recorded in a report, which you can view to determine if any failures need to be resolved.

The system audit is alarmed under the system (sys) level of the maintenance interface. The status of the system audit can be offline (offl) when it is disabled, in service (.), or fail. When the system audit is in a fail state, action is required to resolve the failure. In addition, log SDM550 is generated on the CM, and logs SDM632 and SDM332 are generated on the SDM. For more information on the logs, see “Logs” in the Fault Management document.

Related procedures

Refer to the following procedures in the Fault Management document to perform tasks related to the system audit:

- “Performing a system audit”
- “Viewing the system audit report and taking corrective action”

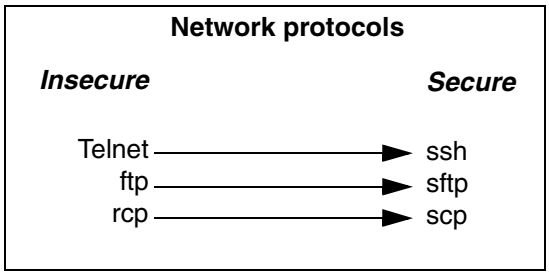
- “Disabling or enabling/changing the time of a system audit”
- “Clearing a system audit alarm”

OpenSSH overview

Functional description

ATTENTION
This document is an overview only of the OpenSSH functionality. Nortel Networks does not provide any detailed usage information or client installation procedures. For this information, refer to the official OpenSSH website located at http://www.openssh.com/.

OpenSSH is an open source version of the Secure Shell (SSH) protocol suite of network connectivity tools. Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. OpenSSH is a suite of tools that provides strong authentication and secure communications over unsecure channels.



The suite of tools is as follows:

- SSH (secure shell) - a replacement for telnet

  Using SSH, you can log in to the core manager from a remote system or log in to a remote system from the core manager. You can also execute commands on a remote system. SSH connects and logs into the specified hostname. You must provide your identity to the remote machine. You can also establish a secure CM session from a remote system through the core manager using SSH.

  Access to some functions requires the use of SSH-compatible client software for access to secure telnet and ftp services (via the SSH standard). SSH clients are supplied bundled with some operating systems, but may need to be obtained separately. The following

table lists some sources for SSH clients (sources are not limited to those listed in this table).

Sources for SSH clients

Source	Type
PUTTY	freeware
OpenSSH	freeware
SSH Inc.	commercial
Secure CRT	commercial
WinSCP	freeware

- scp (secure copy) - improved (secure) functionality of rcp (remote copy)

  Using scp, you can securily copy files to and from the core manager or a remote system. Scp uses ssh for data transfer, and uses the same authentication and provides the same security as SSH.

- sftp (secure file transfer program) - a replacement for ftp

  Using sftp, you can perform secure file transfers. Sftp is an interactive program that connects and logs into the specified host, then enters an interactive command mode.

- sshd (OpenSSH SSH daemon) - the server-side daemon

  Sshd is the daemon program for SSH. Together these programs provide secure encrypted communications between two hosts over an insecure network.

Note: The functionality of OpenSSH does not interfere with existing networking services, such as telnet, FTP, DCE, NTP, or SFT.

The implementation of OpenSSH on the core manager provides three authentication methods:

1 password

2 keys (when you are creating the key, you are asked to add an encrypted password associated with this key)

3 combination of keys and password

Note: The administrator on the SDM and the client must be familiar with the key authentication method, before using it.

The basic utilities of OpenSSH are:

- ssh-add - adds RSA or DSA identities to the authentication agent
- ssh-agent - authentication agent
- ssh-keygen - authentication key generation, management and conversion
- sftp-server - an sftp server subsystem

Note 1: For detailed instructions on the use of key authentication, refer to the official OpenSSH website http://www.openssh.com/.

Note 2: Because the man command is not supported on the SDM, it is not available from SSH shell level.

Related procedures

Refer to the procedure “Installing OpenSSH” in the Upgrades document to install the OpenSSH fileset.

For more information, you can refer to the following web sites:

- http://www.openssh.com/ - for Sun, HP, Linux and AIX
- http://www.chiark.greenend.org.uk/%7Esgtatham/putty/ - a free Win32 Telnet/SSH client for Windows

Product and customer support

Introduction

The SDM component product and customer support includes:

- product support and customer services
- training
- documentation

Product support and customer services

Nortel Networks provides product support using standard Customer Service Center (CSC) and Global Product Support (GPS) policies and procedures. For issues that cannot be resolved, contact Nortel Networks' regional Customer Services Center and a representative will open a Customer Service Report (CSR). If the regional representative cannot resolve the problem, the Customer Service Center representative will refer the matter to the next level of support to provide an answer to the problem or corrective action.

Corrective action can include:

- amendment in a future software release
- incremental software update (patch)
- customer information change
- request for feature development to address new or changed functionality

Once the problem is resolved, the customer is notified and the CSR is closed.

Training

Training is available for the SDM component. All course descriptions, prerequisites, schedules and locations can be viewed at www.nortelnetworks.com/td.

Note: For the most recent curriculum information, please contact your Nortel Networks Training and Documentation representative. For enrollment assistance, please contact Training registration at 1-800-4-NORTEL (1-800-466-7835), express routing code #280.

Documentation

Documentation for the SDM component is provided on a Helmsman CD. The customer information provided includes overview and upgrades information in addition to the following FCAPS areas:

- faults
- configuration
- administration
- performance
- security and administration