CS 2000 Core Manager Basics

Functional description

The Communication Server 2000 Core Manager is a Succession element manager within Preside Management for Succession Solutions (Preside MSS). The CS 2000 Core Manager manages the XA-Core and the subtending TDM components of the Communication Server 2000.

The CS 2000 Core Manager resides on the SuperNode Data Manager (SDM) platform and provides operations, administration, maintenance, and provisioning (OAM&P) functionality.

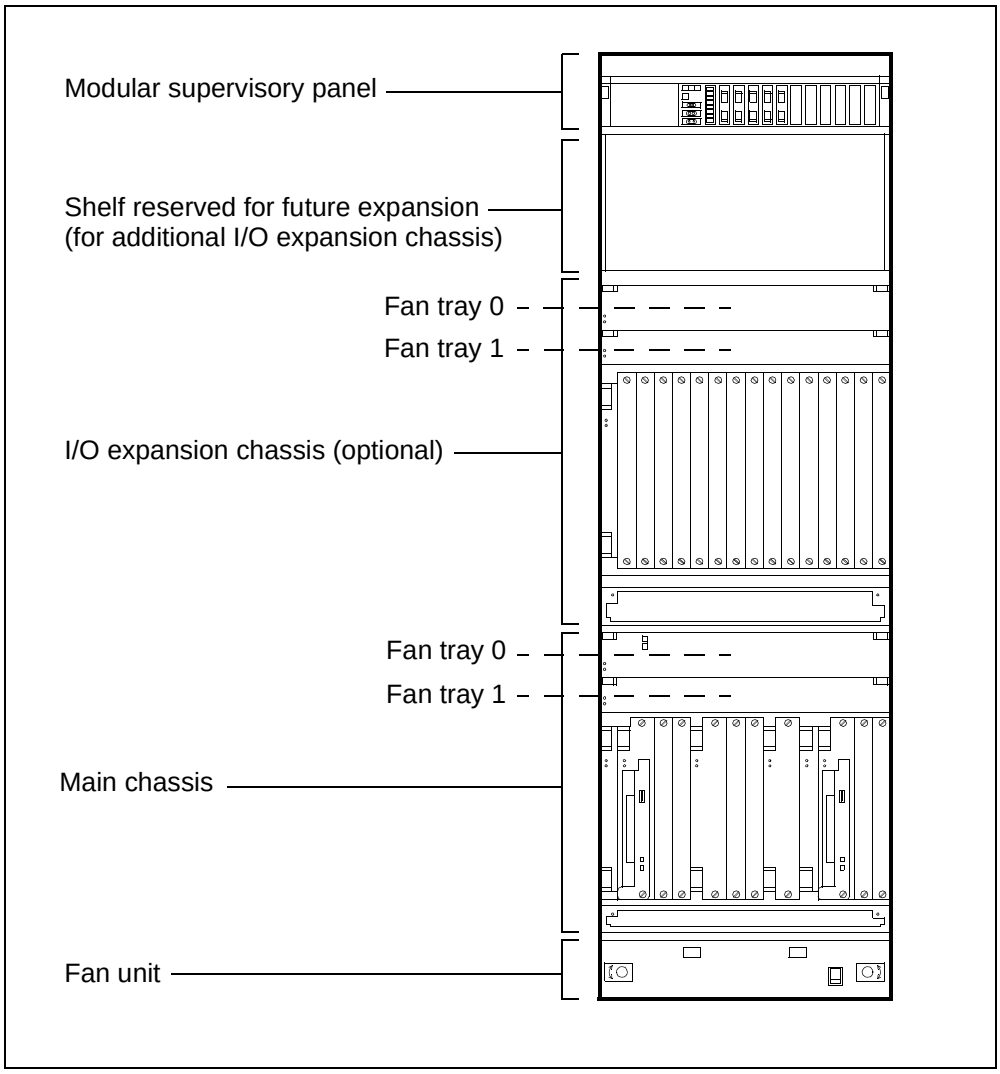
The CS 2000 Core Manager is fault-tolerant, and connects to the operating company network through an Ethernet connection (up to 10 Mbps) to the company operations intranet. The CS 2000 Core Manager also uses the Distributed Computing Environment (DCE) to provide a secure OAM&P applications platform.

Hardware overview

Cabinet

The CS 2000 Core 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



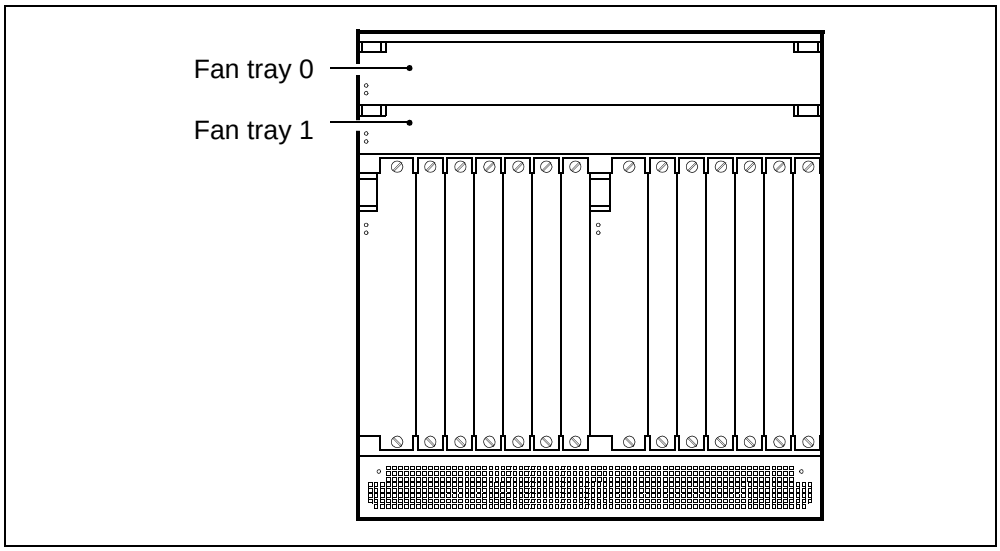
Modular supervisory panel

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 fault-tolerant system platform. Each feed is supplied from a separate breaker in the MSP into interconnect modules (ICMs) in the main and I/O expansion chassis.

Front-mounted I/O expansion chassis

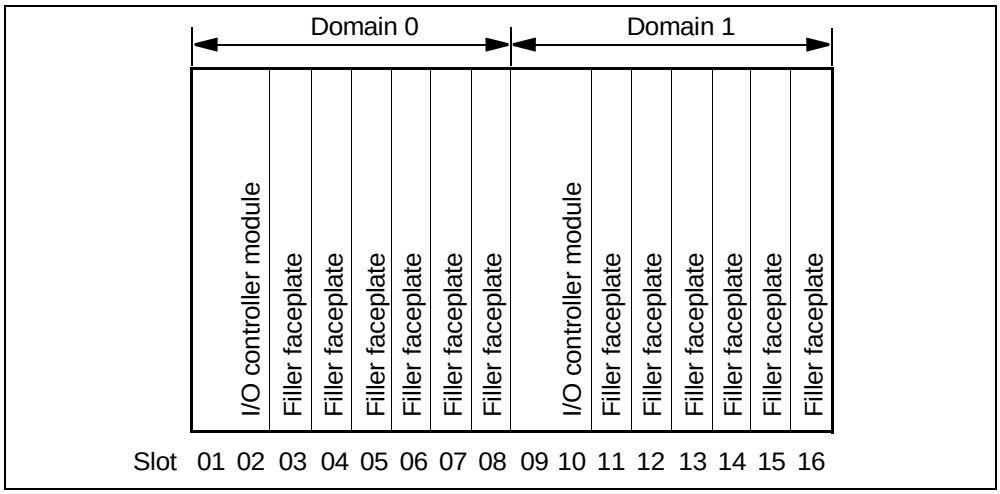
The I/O expansion chassis is for optional system modules. The chassis has two removable fan trays (NTRX50KD and NTRX50FF) that provide horizontal (front-to-rear) cooling to the chassis. Each fan try has three fans and are powered by separate battery feeds to ensure uninterrupted cooling during fan tray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

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 module mounts 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.

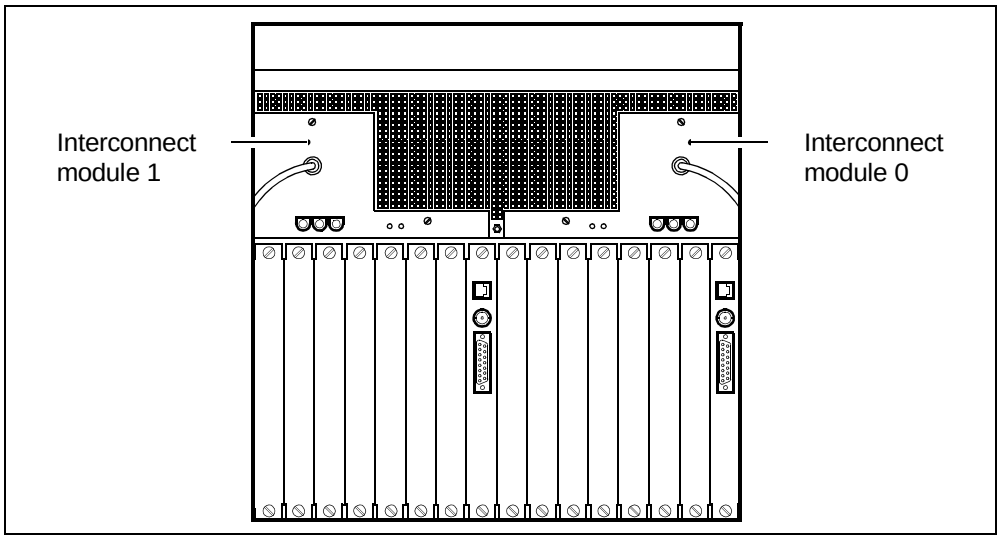
Front view of the I/O expansion chassis by slot number



Rear-mounted I/O expansion chassis

The rear of the I/O expansion chassis contains two interconnect modules (ICM)[1] that supply power to the CS 2000 Core Manager through separate battery feeds. The following figure shows the rear view of the I/O expansion chassis.

Rear view of the I/O expansion chassis

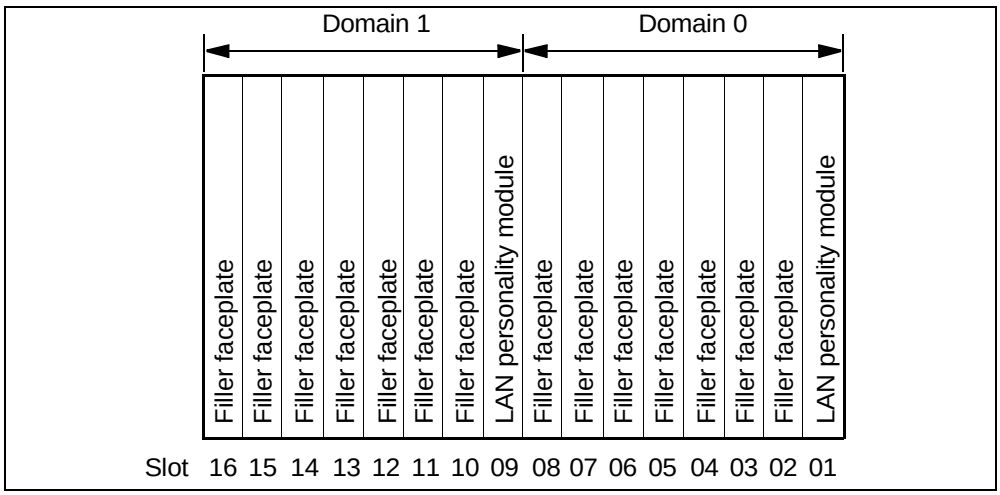


The chassis has a LAN personality module in slots 1 and 9. The module is used with the I/O controller module (NTRX50NL) that mounts at the front of the chassis. The following figure identifies the slot numbers in

[1] There is no alarm cable for the ICMs in the I/O expansion chassis.

domains 0 and 1, and the provisionable LAN personality modules in each slot number.

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

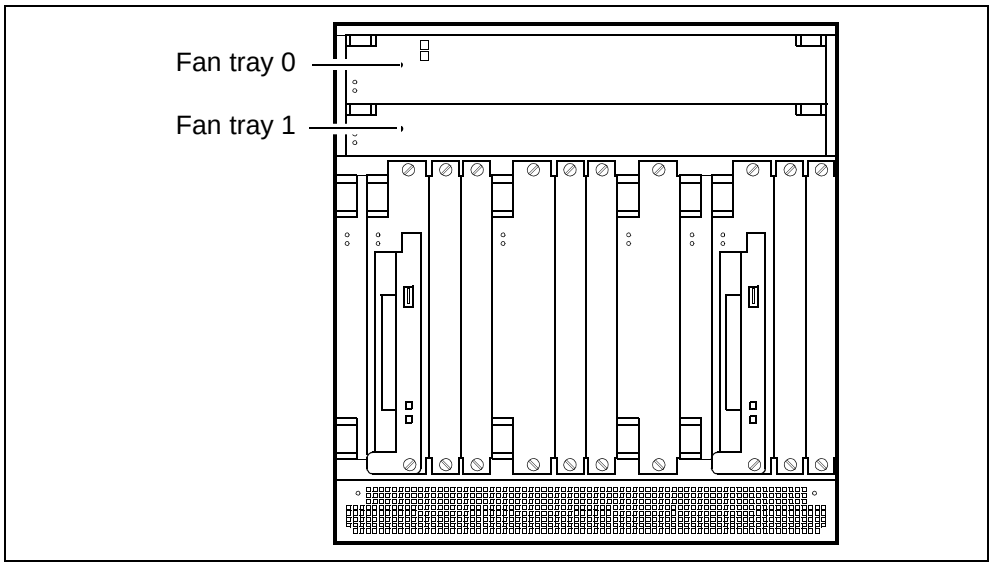


Provisionable personality modules in the I/O expansion chassis are not restricted to specific slot numbers. The LAN personality module mounts in any two slots. The slot numbers must match in each domain, and with the system module installed at the front of the chassis.

Front-mounted main chassis

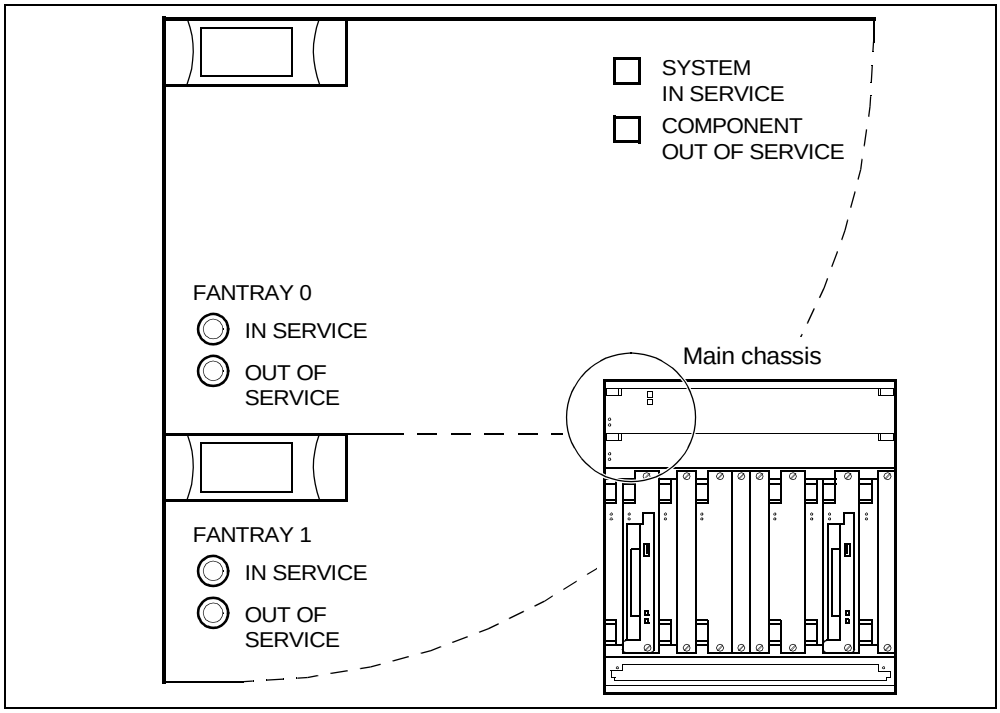
The front of the main chassis has fan trays, provisionable system modules and controller modules. The following figure shows a front view of the main chassis.

Front view of the main chassis



Two removable fan trays (NTRX50FE and NTRX50FF) provide horizontal (front-to-rear) cooling to the chassis. Both trays contain in-service and out-of-service LEDs.[2] 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



[2] The fan trays in the I/O expansion chassis do not have system status LEDs.

The following table lists the controller modules in the main chassis and their corresponding slot numbers.

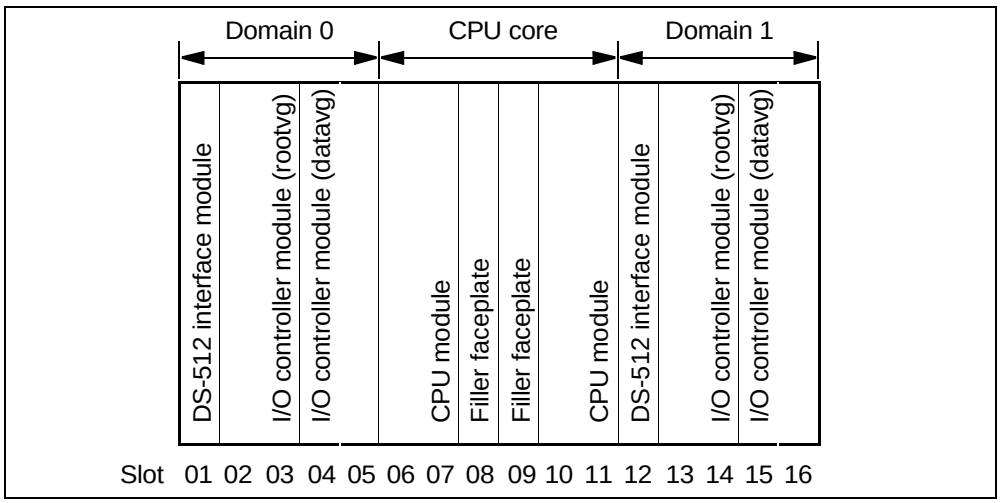
Quantity	PEC	Description	Slot(s)
2	NTRX50GX	DS-512 interface	1, 12
2	NTRX50ND or NTRX50NM	I/O controller (rootvg)	2, 3, 13, 14
2	NTRX50NC or NTRX50NL	I/O controller (datavg)	4, 5, 15, 16
2	NTRX50NB	CPU controller	6, 7, 10, 11

Note 1: If you have an NTRX50GA, you must upgrade it to the NTRX50GX. Refer to procedure “Upgrading the DS512 controller module from NTRX50GA to GX” in the Upgrades section.

Note 2: If you want to upgrade your I/O controller modules, refer to procedures “Upgrading the rootvg MFIO to MFIO or UMFIO” and “Upgrading datavg MFIO to MFIO or UMFIO” in the Upgrades section.

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.

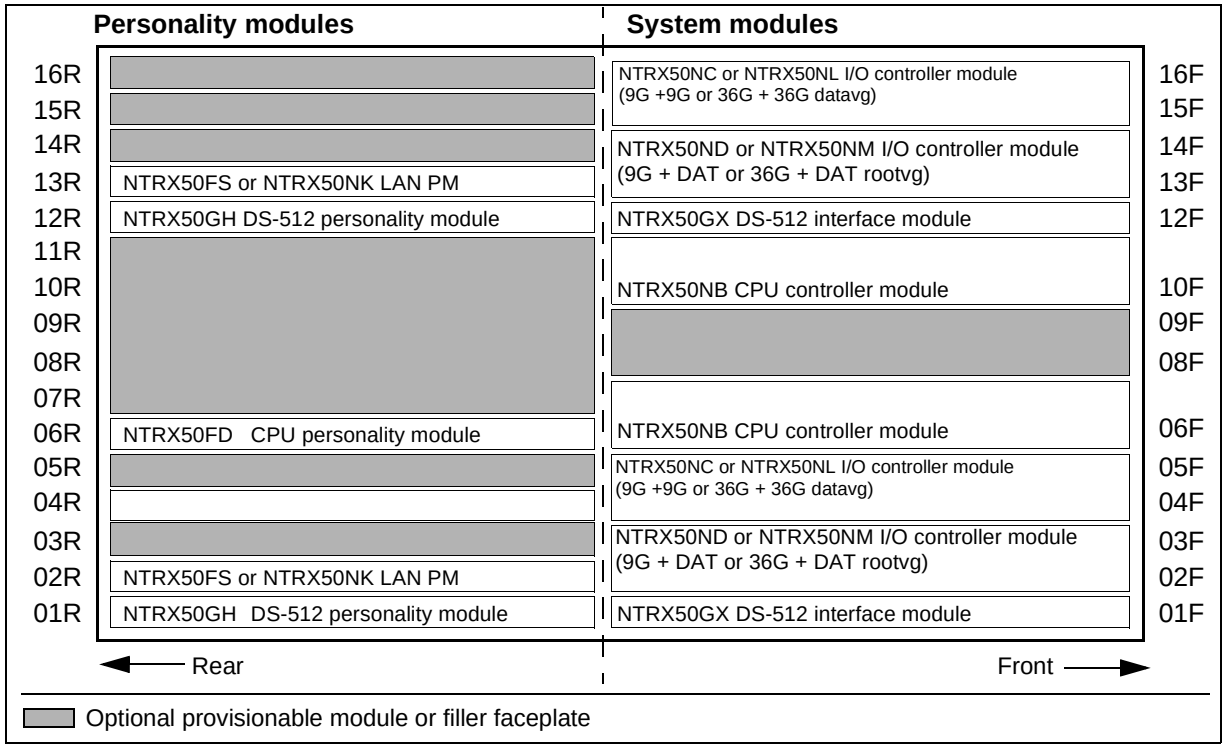
Front view of the main chassis by slot number



Module slot placement

The following figure shows the dedicated slot numbers for required CS 2000 Core Manager modules (front and rear). Provisionable equipment mounts in any slot number in either the main chassis or the I/O expansion chassis.

CS 2000 Core Manager module slot number layout (front and rear)



CPU controller module

The CPU controller module contains the main processing power and memory capacity of the CS 2000 Core Manager and is provisionable in slots 6, 7, 10 and 11 at the front of the main chassis.

DS-512 interface module

The DS-512 interface module is provisionable in slots 1 and 12 at the front of the main chassis. The module is used with the DS-512 personality module 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:

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

The following table lists the types of MFIO/UMFIO controller modules.

MFIO/UMFIO controller modules

PEC	Provides
NTRX50NC or NTRX50NL (datavg)	Two 9-GB (NC) or 36-GB (NL) DDUs, a 10Base-T Ethernet interface
NTRX50ND or NTRX50NM (rootvg)	One 9-GB (ND) or 36-GB (NM) DDU, a DDS-2 DAT drive, a 10Base-T Ethernet interface

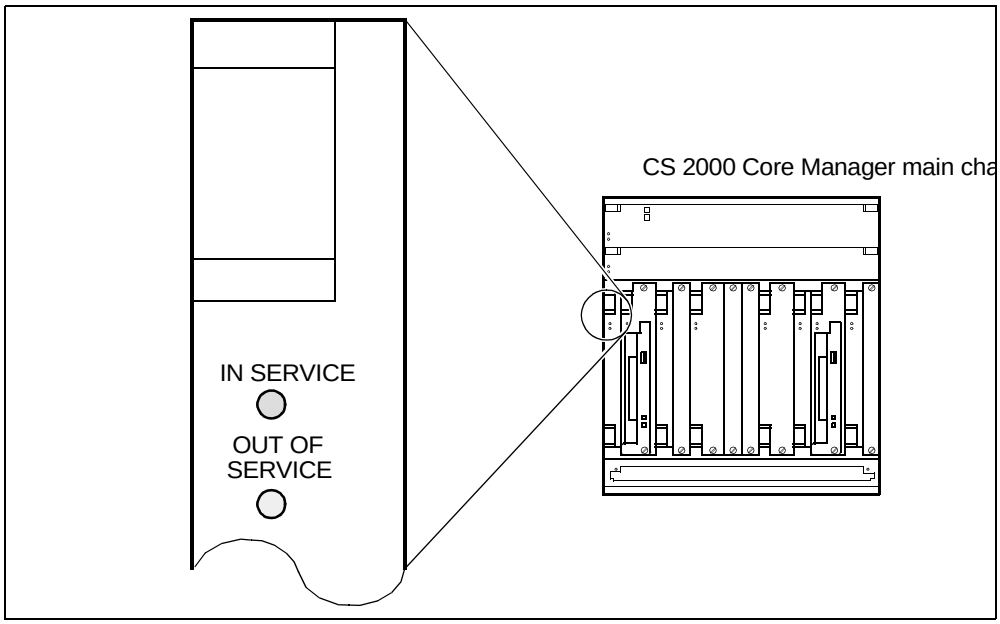
Optional slots at the front of the main chassis

Slots 4, 5, 8, and 9 at the front of the main chassis are not used except 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 (LED) 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.

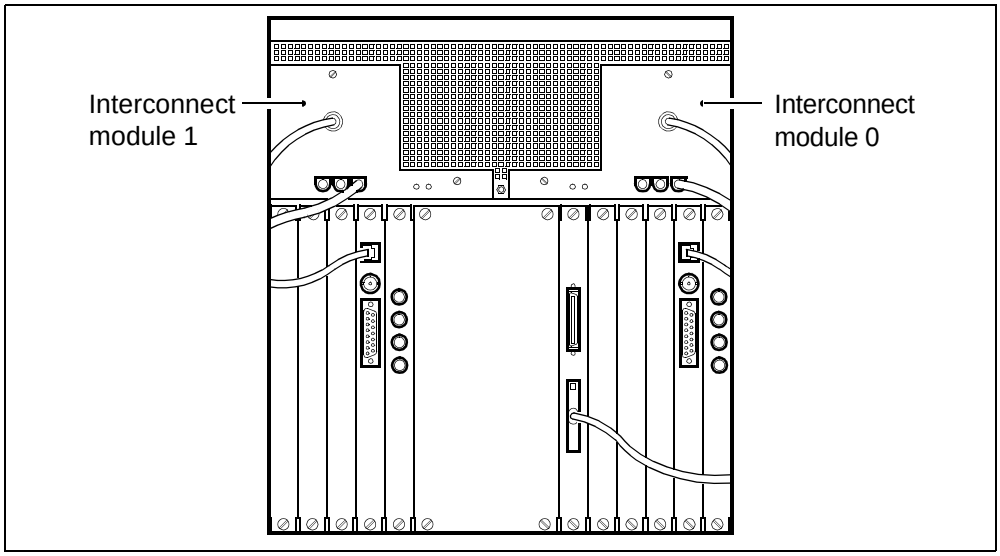
System module LEDs



Rear-mounted main chassis

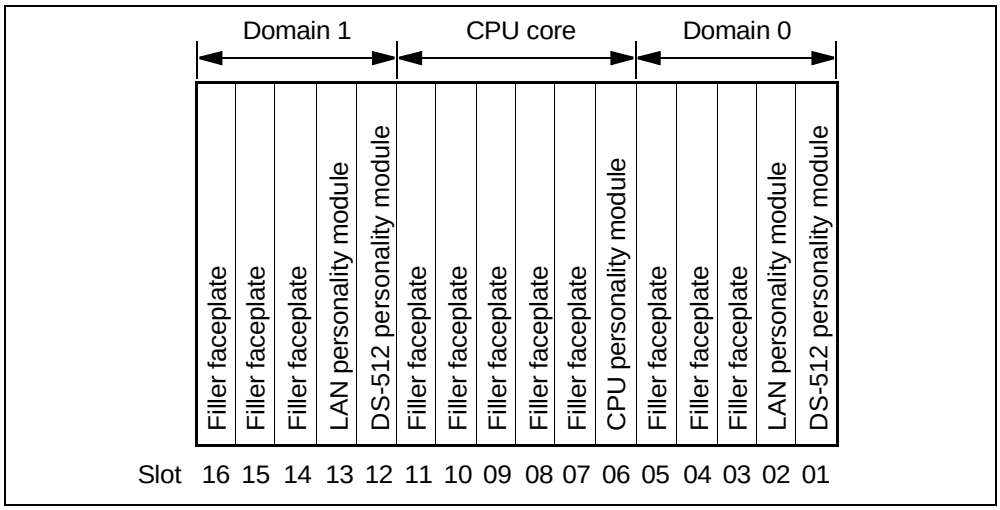
The rear of the main chassis contains two DS-512 personality modules (NTRX50GH) in slots 1 and 12, and two ICMs (NTRX50FG and NTRX50FH) that supply power to the CS 2000 Core Manager. The rear of the main chassis also contains two LAN personality modules (NTRX50FS or NTRX50NK) in slots 2 and 13, and one CPU personality module (NTRX50FD) in slot 6. The following figure shows a rear view of the main chassis.

Rear view of the main chassis



The following figure shows the slot numbers in domains 0 and 1, the CPU core, and required provisionable personality modules in each slot number. The remaining slots are available for optional personality modules.

Rear view of the main chassis by slot number



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

LAN personality module (NTRX50FS or NTRX50NK)
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 module supports 10Base-T port connection to the operating company LAN. Version NTRX50FS supports NTRX50NC MFIO controller modules. Version NTRX50NK (UMFIO LAN PM) supports NTRX50NL and NTRX50NM UMFIO controller modules.

CPU personality module (NTRX50FD)
The CPU personality module (NTRX50FD) mounts in slot 6 at the back of the main chassis. The CPU module NTRX50NB at the front of the main chassis 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 (NTRX50NN)

The NTRX50NN personality module is used with the NTRX50NM rootvg UMFIO module that has embedded X.25 functionality.

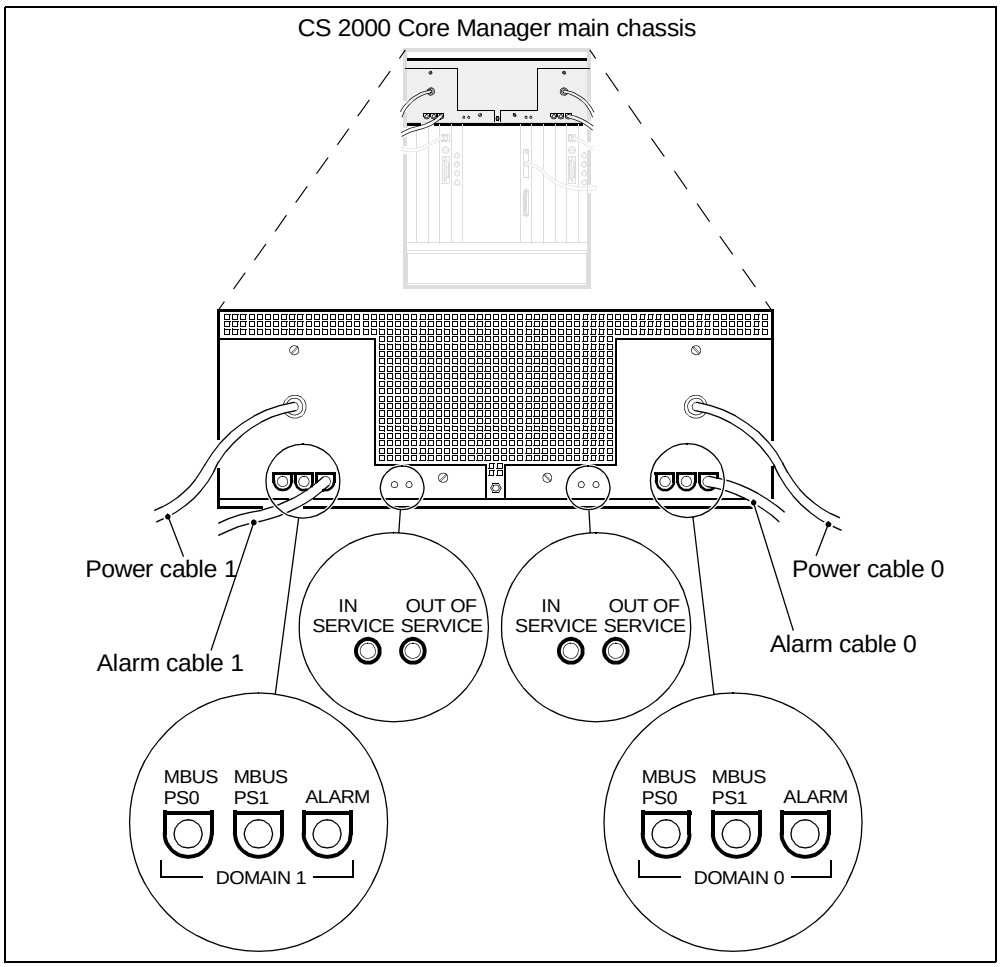
Optional slots at the back of main chassis

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 (NTRX50FG, NTRX50FH)

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 hardware for the CS 2000 Core Manager. 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 provides vertical cooling for the C28B cabinet.

Software overview

Architecture

The CS 2000 Core Manager 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 CS 2000 Core Manager 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 CS 2000 Core Manager to manipulate tables maintained on the Core.
Remote procedure call (RPC)	Allows software on the Core to raise RPC routines to software on the CS 2000 Core Manager. 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 CS 2000 Core Manager 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 CS 2000 Core Manager.

Software and application order codes

The following table lists the software order codes for the CS 2000 Core Manager.

Software order codes (Sheet 1 of 3)

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	

Software order codes (Sheet 2 of 3)

Name	Order code
PSPT 15K MSS Integration	PSPT0001
PSPT Exist OSS I/F Integration	
PSPT FCAPS API	
ATA ASCII Term Acc Gwy	ATA00001
ATA ASCII Access Gateway	
DDMS System Phase1	DDMS0001
DDMS Enhancement Pkg1	
DDMS OSS Data I/F	
DDMS Platform Ph1	
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	

Software order codes (Sheet 3 of 3)

Name	Order code
SFT ASG Enabling FT/SW SFT ASG Enabling FTSW fn	SFT00003
SFT Secure File Transfer SFT Secure File Transfer	SFT00001
UTA ASG Enabling TA/SW UTA ASG Enabling TASW fn	UTA00002
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, and is delivered on tape
- maintenance non-computing load (MNCL), a maintenance release scheduled approximately every three months for the first year of a released NCL, and is delivered on tape
- CS 2000 Core Manager patching, fix filesets delivered electronically as soon as they are available

The CS 2000 Core Manager supports software streams of up to three releases back from the latest release. When upgrading your CS 2000 Core Manager software from one release to another, ensure that the computing module (CM) load release on the Communication Server 2000 core is not higher than the software release on the CS 2000 Core Manager. Upgrade the CS 2000 Core Manager to the latest release of the software before you upgrade the Communication Server 2000 core load. Upgrading a Communication Server 2000 core to a release ahead of the CS 2000 Core Manager+ creates an unsupported configuration.

For information on upgrading your CS 2000 Core Manager to the latest software release, refer to one of the following procedures in the Upgrades section:

- “Upgrading CS 2000 Core Manager software using non-split mode”
- “Upgrading CS 2000 Core Manager software using split mode”
- “Upgrading CS 2000 Core Manager software using ESUP”

For information on upgrading your CS 2000 Core Manager with software fixes, refer to procedure “Upgrading the CS 2000 Core Manager with software fixes” in the Upgrade section.

User interfaces overview

Functional overview

The CS 2000 Core Manager supports local area network (LAN)-based input/output (I/O) interfaces to the components in the following table.

Components with interface to the CS 2000 Core Manager

Component	Description
Workstation	Configured as remote user interface (UI) client[a] for CS 2000 Core Manager applications; requires open software foundation (OSF) distributed computing environment (DCE) client software
Hub	Required for 10Base-T or unshielded twisted pair (UTP) LANs
Router[b]	Performs wide area networking (WAN) for CS 2000 Core Manager graphical user interfaces (GUI); provides gateway (or protocol translator) functions
Terminal server	Provides asynchronous access to the CS 2000 Core Manager; ports used either instead of integrated asynchronous application ports, or in addition to integrated ports; engineering rules applications determine the number of required asynchronous ports

a.UI client performance depends on workstation performance.
b.Routers in an Succession Network must support BOOTP forwarding.

Workstations

The following table lists the workstations that can be configured as UI clients for CS 2000 Core Manager 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 sources for SSH clients.

Sources for SSH clients

Source[a]	Type
PUTTY	freeware
OpenSSH[b]	freeware
SSH Inc.	commercial
Secure CRT	commercial
WinSCP	freeware

a.Sources for SSH clients are not limited to those listed in this table.

b.For more information about OpenSSH, refer to OpenSSH overview.

Maintenance interfaces

The following table lists the maintenance interfaces for the CS 2000 Core Manager.

CS 2000 Core Manager maintenance interfaces

Interface	Description
MAP (maintenance and administration position) CI (MAPCI)	Primary access to the Core for maintenance during normal CS 2000 Core Manager-to-Core operations. A dedicated CS 2000 Core Manager maintenance subsystem at the APPL level of the MAP allows users to • determine the node status and operating condition of the CS 2000 Core Manager • change the state of the CS 2000 Core Manager for maintenance • determine the status of connectivity between the Core and the CS 2000 Core Manager • reboot or halt the CS 2000 Core Manager • change the state of CS 2000 Core Manager hardware • use the QUERYSDM command to determine the status of CS 2000 Core Manager applications and operating system, including faults that currently affect applications and system software resources
CS 2000 Core Manager maintenance	Secondary access from the CS 2000 Core Manager for maintenance when CS 2000 Core Manager-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 CS 2000 Core Manager hardware, and of individual CS 2000 Core Manager application packages • complete administration capabilities, including software and user administration and configuration changes

Accessing the Core

Support for the CS 2000 Core Manager 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 CS 2000 Core Manager.

Types of Core access

TheCS 2000 Core Manager requires two types of access to the Core.

- Primary
- Secondary

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 activities are types of activities 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 CS 2000 Core Manager 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)/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

Following are the high-level steps to access the Core through a terminal server.

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. Following are the high-level steps to access the Core through the EIU.

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).

TheCS 2000 Core Manager 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. Following are the high-level steps to access the Core through the SDM.

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. Following are the high-level steps to access the Core through the SDM console.

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.

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 CS 2000 Core Manager

Support for the CS 2000 Core Manager 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 CS 2000 Core Manager.

Methods of access

Use the following methods to access the CS 2000 Core Manager.

- 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 CS 2000 Core Manager. Use the command to access CS 2000 Core Manager nodes that are either in service (InSv) or in-service trouble (ISTb). Both maint and root users can use SDMRLOGIN.

Restricted shell commands An SDMRLOGIN session accesses a restricted shell on the CS 2000 Core Manager, 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 (Sheet 1 of 4)

Command	Function
AFTAdd1	Adds a new AFT session
AFTAddfile1	Adds a file to an AFT session transfer list
AFTAlarm1	Queries or cancels AFT session alarms
AFTChange1	Changes the value of retry attempts for an AFT session
AFTDelete1	Deletes an AFT session
AFTList1	Lists configuration information about AFT sessions
AFTListfile1	Lists processed files for a stream
AFTQuery1	Queries and displays data about an AFT session
AFTRsetfile1	Resets the state of a file for an AFT session
AFTSetfile1	Sets override file or deletes a file from a list
AFTStart1	Starts an existing AFT session
AFTStop1	Stops an existing AFT session
amadump2	Displays record information contained in a billing file
awk	Pattern-directed scaling and processing language
bsyapp	Busies an application
closec2	Closes currently open billing file or files for each stream
CONFSTRM.act2	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 (Sheet 2 of 4)

Command	Function
CONFSTRM.add2	Adds a configured billing stream
CONFSTRM.change2	Changes an existing billing stream configuration
CONFSTRM.deact2	Deactivates a filtered stream
CONFSTRM.delete2	Deletes an existing billing stream configuration
CONFSTRM.list2	Lists configuration of a single billing stream or all billing streams
CONFSTRM.start2	Resumes receiving records on a filtered stream
CONFSTRM.stop2	Stops receiving records on a filtered stream
CONFSTRM.update2	Updates the criteria of a filtered stream
cut	Cuts out (extracts) selected fields of each line of a file
dispal2	Displays current billing alarms
displogs2	Displays billing logs not acknowledged by the Core
grep	Searches a file for a pattern
help	Displays generic help information
java	Java Runtime Environment
listfile2	Lists stored billing file or files for each stream
locate	Queries hardware module information
logout	Logs the user out of the CS 2000 Core Manager
logquery	Initiates the logquery tool to browse DMS logs
ls	Lists contents of the CS 2000 Core Manager remote login directory
mib2	Gets or sets MIB objects for billing
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 (Sheet 3 of 4)

Command	Function
offlapp	Offlines an application
ping	Sends ICMP ECHO_REQUEST packets to network hosts
ps	Reports process status
query2	Queries SBA billing stream status
readtape.sh2	File used by TAPE.send; should not be called directly
rtsapp	Returns an application to service
SCHEDULE.add2	Adds a tuple to the schedule
SCHEDULE.change2	Changes an existing tuple in the schedule
SCHEDULE.delete2	Deletes a tuple or tuples from the schedule
SCHEDULE.list2	Lists a tuple or tuples in the schedule
SCHEDULE.RTBAdd2	Adds Real-Time Billing (RTB) to a stream
SCHEDULE.RTBBsy2	Busies RTB for a stream
SCHEDULE.RTBChange2	Changes the RTB configuration for a stream
SCHEDULE.RTBConfQuery2	Queries the RTB configured destinations
SCHEDULE.RTBDelete2	Deletes RTB from a stream
SCHEDULE.RTBIptest2	Tests the IP address used by RTB for a stream
SCHEDULE.RTBOffl2	Offlines RTB for a stream
SCHEDULE.RTBQuery2	Queries the state of RTB for a stream
SCHEDULE.RTBRts2	Returns RTB to service for a stream
sendfile	Sends billing file or files for each stream to downstream DPMS

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 (Sheet 4 of 4)

Command	Function
TAPE.list2	Lists the billing files written to a digital audio tape (DAT)
TAPE.send2	Sends (FTP) billing files from a DAT
TAPE.write2	Writes billing files to a DAT
who_is_on	Displays the users logged in to the CS 2000 Core Manager
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 CS 2000 Core Manager is not in the InSv or ISTb state. Put the CS 2000 Core Manager in the InSv state, and re-enter the SDMRLogin command.
- A telnet session cannot be established between the CM and the CS 2000 Core Manager.
- The terminal that you are using for the remote login does not suppress the echoing of password entries. You either can 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 either can continue or exit the remote login session.

Tools and utilities

Logs

Logs from the computing module (CM) and CS 2000 Core Manager application software are routed and stored through Generic Data Delivery (GDD). GDD maintains a logical volume on the CS 2000 Core Manager (at /datavg/gdd) of up to thirty days of logs. For more details about GDD, refer to Generic Data Delivery overview.

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.

Administration

Root and maintenance (maint class) users can use tools at an CS 2000 Core Manager maintenance interface and UNIX-based utilities at a VT100 console (local or remote) to

- commission the CS 2000 Core Manager 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 section.

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 CS 2000 Core Manager are equivalent to file systems.[1] Root users can monitor file system partitioning, but cannot modify the logical volumes.

[1] Nortel Networks provisions the CS 2000 Core Manager file system structure.

Operational Measurement Delivery overview

Functional overview

The CS 2000 Core Manager 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 CS 2000 Core Manager 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 CS 2000 Core Manager to an operations support system (OSS). (For more information about SFT, refer to Secure File Transfer overview.) 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; multiple time periods in the same day require defining multiple schedules.
Weekly	Weekly start and stop time. Values: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday. Format: hhmm (see "Daily" repetition); multiple days can be specified in same schedule.
Monthly	Monthly start and stop time. Values:1 to 31. Format: hhmm (see "Daily" repetition); multiple days can be specified.

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 CS 2000 Core Manager. 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[1]

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 resent, 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

[1] The CS 2000 Core Manager does not authenticate the IP and port addresses or the login ID and password.

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 aCS 2000 Core Manager 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 CS 2000 Core Manager is commissioned.

OMD data collection capacity

Collection of more than 10,000 tuples reduces CS 2000 Core Manager performance and the retention period for OM report files.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. Use the formulas in the following table to calculate the limit for OMD data collection.

Formulas for calculating the limit for OMD data collection

OMD data capacity transfer type	Formula
5- and 15-minute	**x+ y/3 = n <= 10,000 tuples** *(without loss of data)*
5- and 30-minute	**x+ z/6 = n <= 10,000 tuples** *(without loss of data)*
where: **x** = the number of OM tuples collected every 5 minutes **y** = the number of OM tuples collected every 15 minutes **z** = the number of OM tuples collected every 30 minutes **n** < 10,000 tuples	

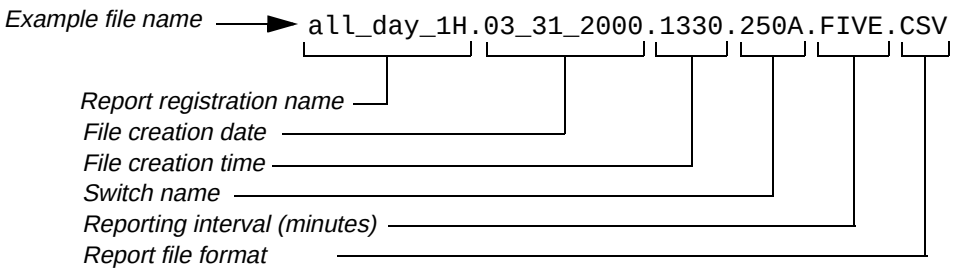
The following table lists the current OMD data collection capacity.

OMD maximum data collection capacity

Transfer type	Capacity (number of tuples)
5-min.	6000
15-min.	12,000
30-min.	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 CS 2000 Core Manager, and by entering the OMSHOW command on the MAP. The following table shows an OM report file.

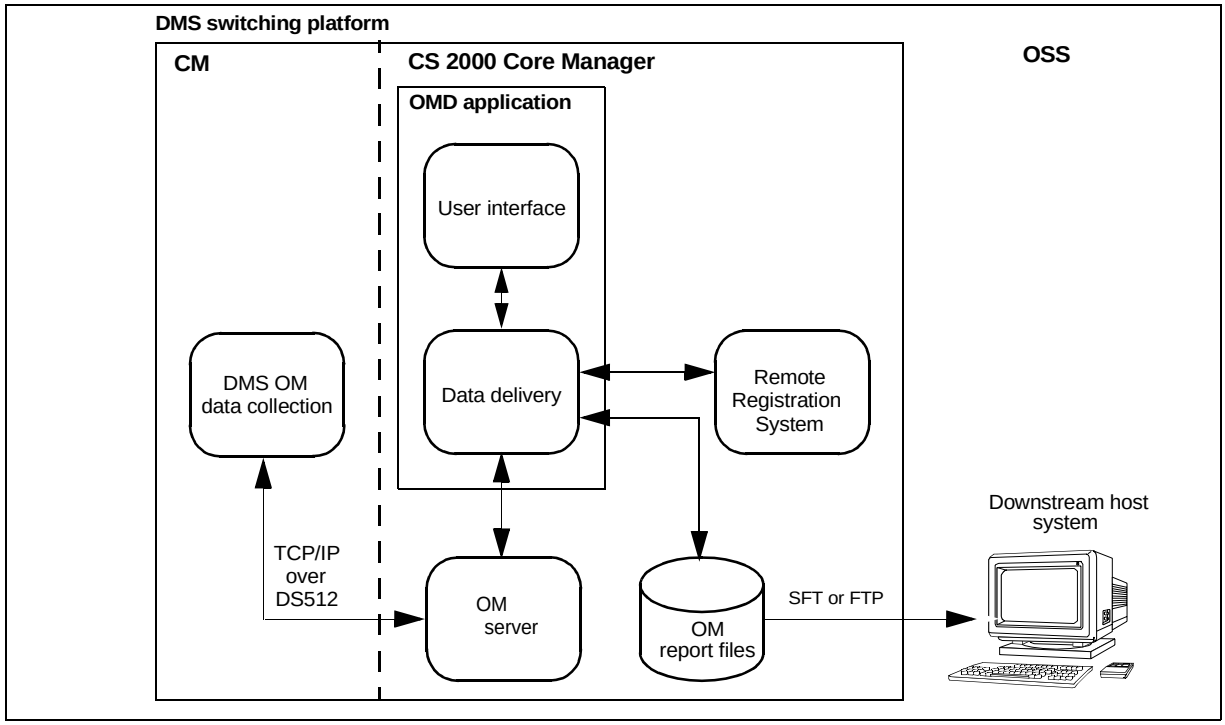
Contents of an OM report file

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, CS 2000 Core Manager and OSS.

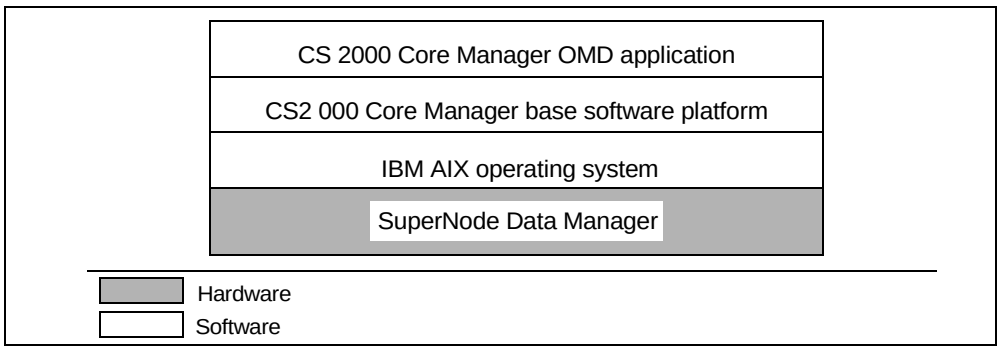
CS 2000 Core Manager OM delivery components



Software

The CS 2000 Core Manager base software platform runs on the IBM AIX operating system. The CS 2000 Core Manager OMD application runs on the CS 2000 Core Manager base software platform layer. Refer to the following figure.

Software overview



The following table lists the subsystems and components of the CS 2000 Core Manager OMD application.

CS 2000 Core Manager 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 CS 2000 Core Manager. 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 CS 2000 Core Manager.

SuperNode Billing Application overview

Functional description

The SuperNode Billing application (SBA) runs on the CS 2000 Core Manager and computing module (CM) platforms. The CM side receives formatted billing records, buffers them, and sends them to the CS 2000 Core Manager for storage in files until they are sent to downstream billing processors. The SBA uses billing processors access the files using either File Transfer Protocol (FTP), File Transfer Access and Management (FTAM) Protocol, or both.

The SBA

- off-loads billing activities from the CM. The SBA supports a maximum of four streams of CM or filtered billing records that can be routed to processors.
- provides real-time delivery of Call Detail Recording (CDR) billing records in the billing file, device-independent recording package (DIRP), within 30 seconds of record generation
- records at the CS 2000 Core Manager within 5 minutes of call completion (near-real time delivery)
- supports Bellcore AMA Format (BAF), Universal AMA, Station Message Detail Recording (SMDR), and the following CDR formats:
  - Universal Carrier Switch (UCS) DMS-250 CDR.
    The SBA converts UCS DMS-250 CDR stream records to a specified BAF standard AMA files as defined in GR-1343
  - DMS-300 CDR formats 09, 14, and 15
  - DMS-Global Services Platform (GSP) CDR
  - Sprint DMS-250 CDR
- stores BAF records in DIRP formatted files

Note: Currently, the CS 2000 Core Manager does not support an SMDR stream in DIRP format. Although the CS 2000 Core Manager allows you to configure an SMDR stream in DIRP format, the command **sdmbctrl smdr on** from the Communication Server 2000 core produces the following error message: `The stream is not configured or not supported on the SDM`.

SBA operating modes

The SBA runs in either normal, backup or recovery mode.

When the CS 2000 Core Manager is unavailable, SBA goes into backup mode, writes billings files on the Communication Server 2000 core. When the CS 2000 Core Manager becomes available again, SBA goes into recovery mode, sends all backup files from the Communication Server 2000 core to the CS 2000 Core Manager.

Backup mode processing

The SBA enters backup mode when

- communication between the CS 2000 Core Manager and CM fails
- the CS 2000 Core Manager does not send an acknowledgment that the buffered billing record is successfully written to disk
- maintenance personnel enter the BSY command either on the CM-side of SBA to busy the CS 2000 Core Manager, or on the CS 2000 Core Manager-side of SBA to busy SBA
- maintenance personnel upgrade SBA software on the CS 2000 Core Manager
- a CS 2000 Core Manager software error generates a critical alarm
- the CS 2000 Core Manager disk volume is full

The SBA buffer system routes billing records from `amaproc` to the SBA auxiliary storage system. The auxiliary storage system writes the records to disk on the CM-side until communication resumes between the CM and the CS 2000 Core Manager.

Recovery mode processing

The SBA enters recovery mode after communication between the CS 2000 Core Manager and the CM resumes. The buffer system routes the active (real-time) and the backed-up recovery records through the SBA communication system. The SBA file manager writes the active records to one file and the records from auxiliary storage to a separate file.

SBA user interface

The SBA user interface, or billing maintenance interface (BILLMTC), is similar to the MAP (maintenance and administration position) for the CM. Through the maintenance interface, the user can schedule file transmissions, list and send files, set the stream context for subsequent commands, query a stream, close a current file, view and set management information base (MIB) parameters, and configure a stream. The user login (root or maint) determines which commands and command parameters are available. Access to BILLMTC is through either Telnet or Enhanced Terminal Access (ETA). For more information about ETA, refer to Enhanced Terminal Access overview.

The user interface to SBA has the standard DMS/CM display. To initiate the SBA user interface, enter the BILLMTC command. Access to the `sdmbil` level is through the MAPCI under the APPL banner. Functions at this level display and query status of the SBA and associated alarms.

File Status

The CS 2000 Core Manager receives billing records from the CM and adds them to an open file (in the *open* directory) so the records can be written to the buffer. Once the file reaches a predetermined size or time, it closes and moves to the *closedNotSent* directory until it is transferred to all configured clients. Once the file transfers, it moves to the *closedSent* directory until its space is needed, at which time it is removed from the disk. Files are closed and available for transfer to the collector according to the conditions in the following table.

Conditions for file transfer to collector

Condition	Description
Max file size[a] (bytes) reached	Values: 1MB to 20MB for BAF (default: 20MB), 100KB to 20 MB for SMDR (default: 20MB)
Max file size (records) reached	Values: 10,000 to 500,000 for BAF (default: 500,000), 1000 to 500,000 for SMDR (default: 500,000)
File close time	Near real-time timer closes files before they reach max size. Values: 5 min. to 10,080 min., disabled (default: 120 min.)

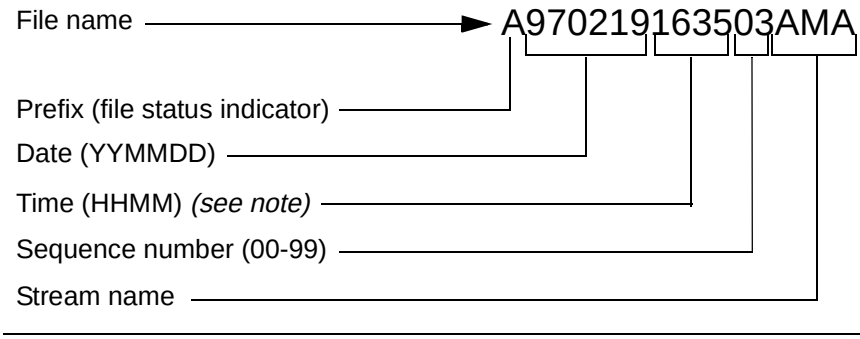
a.Maximum file sizes for bytes and records are specified by the user.

Use the **CLOSEC** command to close files.

DIRP file names

The following figure shows an example of a DIRP file name.

Example DIRP file name



Note 1: Initially, the value for time in DIRP file names is OPEN. For each stream, the files can have the time and date updated when they are closed. The parameter is stored in the Management Information Base (MIB).

Note 2: Currently, the CS 2000 Core Manager does not support an SMDR stream in DIRP format. Although the CS 2000 Core Manager allows you to configure an SMDR stream in DIRP format, the command **smdbctrl smdr on** from the Communication Server 2000 core produces the following error message: "`The stream is not configured or not supported on the SDM.`"

When a DIRP file changes status, the prefix in the DIRP file name also changes. The following table lists the status indicators used as the prefix in DIRP file names that are valid for SBA.

Status indicators in DIRP file names

Prefix	DIRP file status
A	Active
P	Processed (*ClosedSent* name)
U	Unprocessed (*ClosedNotSent* name)

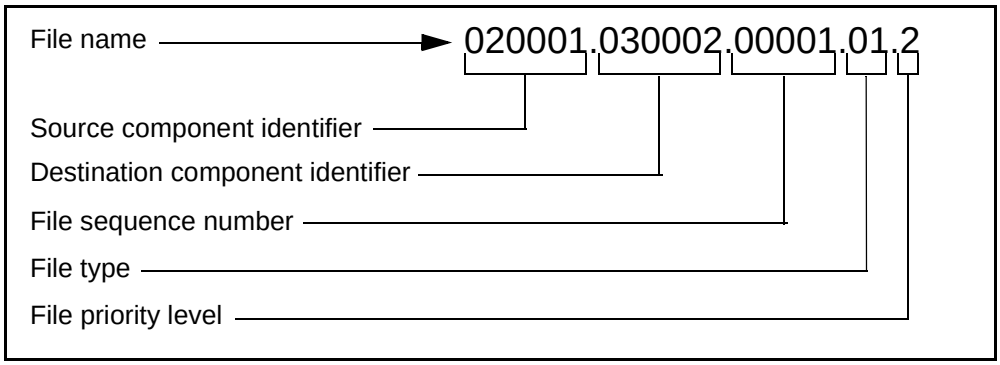
The following status indicators are also valid for DIRP, but are *invalid for SBA* and therefore are *not supported by SBA*.

- R - Removed. A file with the R prefix is removed from recording (not deleted) and not meant for transfer. To make the file eligible for deletion by volume management, you must first change the prefix to P by using the DIRP **CLEANUP** command.
- B - Backup. SBA uses disk mirroring instead of the parallel recording that is required to create the backup file.

AMA file names

The standard AMA file is a streamlined file that contains a header followed by the billing records. The AMA file name contains the elements defined in Bellcore Automatic Message Accounting Data Networking System (AMADNS) Specification GR-1343. The following figure shows an example of an AMA file name.

Example AMA file name



The following table describes the components of an AMA file name.

Components of an ama file name

Component	Description
Source component identifier	A unique number that identifies which AMADNS component is the source of the file
Destination component identifier	A unique number that identifies which AMADNS component is the source of the file
File sequence number	A number that defines the files in the same file category. Examples: file type, file priority level, source component and destination component.
File type	Type of data contained in a file
File priority level	Level of priority of data in a file

An AMADNS file header is 28 bytes and contains the fields in the following table.

AMADNS file header (Sheet 1 of 2)

Byte	7	6	5	4	3	2	1	0
1	File header length							
2	Source component identification number							
3	Source Component Type				Source component identification number			
4	Destination component identification number							
5	Destination component type				Destination component identification number			
6	File type code:					Data format type		
	Standard file: BAF code=01, SMDR code=11							
	Error file: BAF code=02, SMDR code=12							
7	Field suppression type		File priority level			Reset status	Pri/Sec status	Record source info type
8-9	File sequence number							
10	File creation time							
11	File creation date				File creation time			
12-13	File creation date							
14	File last modification time							
15	File last modification date				File last modification time			
16-17	File last modification date							
18-21	File length							
22-24	Number of records in file							
25	Record resource type							

AMADNS file header (Sheet 2 of 2)

Byte	7	6	5	4	3	2	1	0
26	Record source identification number				Record source type			
27-28	Record source identification number							

File transfers

The SBA provides the following methods for transferring billing files of a particular stream to a downstream destination:

- outbound file transfer
- inbound file transfer
- Real Time Billing (RTB) - DIRP file format only
- Automatic File Transfer (AFT) - DIRP file format only

  AFT is not a required application for SBA. For more information about AFT, refer to SBA Automatic File Transfer application overview.
- manual requests

Billing files always move from SBA to the downstream destination, but the file transfers can be initiated by SBA (this is called outbound) or by the downstream destination (this is called inbound).

Note: A stream can have a file transfer mode of either Inbound or Outbound, but not both.

The Inbound file transfer mode allows the customer's FTP client to selectively retrieve billing files. Because the FTP requests are inbound from the customer client to the CS 2000 Core Manager, this is known as inbound file transfer mode.

Streams can be configured on an individual basis for either inbound file transfer or scheduled outbound file transfer. While a stream is in inbound mode, it is still possible to back up data using TAPE level commands. Inbound and outbound file transfer are enabled through the CONFSTRM command, which is accessible through the BILLMTC level.

Real time billing (RTB) allows billing records to be available for transfer from the CS 2000 Core Manager 30 seconds after the call is disconnected. Real time billing downloads a small group of records to the DIRP billing file on the downstream destination as the records are added to the open billing file on the CS 2000 Core Manager. Real time

billing uses FTP (file transfer protocol) through an Ethernet connection to deliver records.

Note: Scheduled outbound file transfer and real time billing (RTB) allow for multiple destinations for a single billing stream.

SBA block flushing

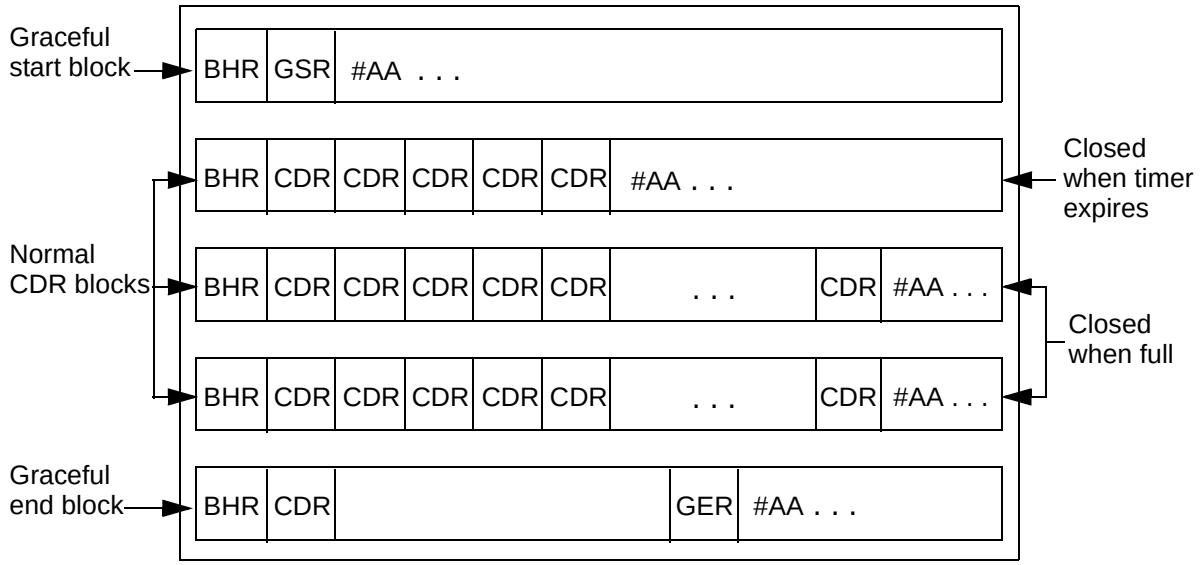
SBA block flushing uses a timer-based mechanism to close DIRP file blocks after a specified time, and allows the timer value to be set through the BILLMTC level during billing stream configuration on the CS 2000. When a DIRP file block is closed based on time, the block is padded with hex 0xAA for each unused byte in the block. Each block can contain a variable number of call records even when the size of each call record is fixed. SBA block flushing supports only BAF and CDR250 record formats. SBA block flushing does not support DNS file formats.

Note 1: SBA block flushing does not support customized DIRP file formats that do not allow hex *AA* padding at the end of a block. This type of DIRP file expects CDRs to be of equal size, and each block ends with a special event record. Therefore, GSP and MCI CDR DIRP files are not supported.

Note 2: It is recommended that SBA block flushing be used with real-time transfer mechanisms such as Automatic File Transfer (AFT) and Real-Time Billing (RTB).

The following figure shows an example CDR DIRP file when SBA block flushing is activated.

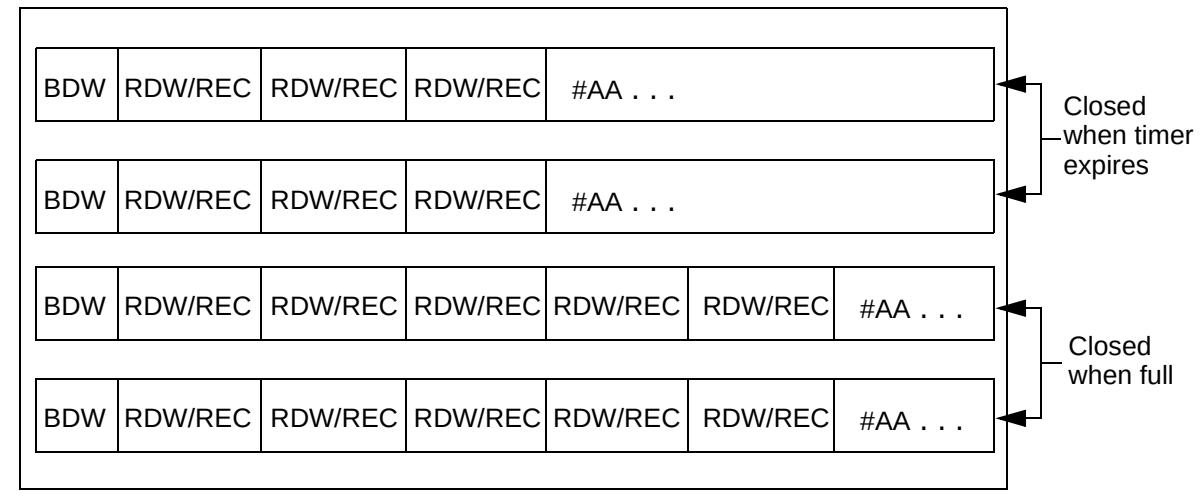
Example: DIRP file when SBA block flushing is activated



Note: The size of CDR is provisioned from the Core. Each CDR is the same size. The figure does not show other SBA-supported event records.

The following figure shows an example BAF DIRP file when SBA block flushing is activated.

Example: BAF DIRP file when SBA block flushing is activated



BDW = 4 bytes; indicates the size of the data in the block
RDW = 4 bytes; and indicates the size of RDW and REC
RDW/REC does not necessarily have to be the same size.

Secondary file processing

ATTENTION
Secondary file processing is supported *only* for billing streams containing AMA billing records that are stored in an AMADNS standard file on the CS 2000 Core Manager.

ATTENTION
To ensure that AMADNS and CS 2000 Core Manager performance objectives continue to be met, secondary file processing is not recommended for AMA record throughput greater than 52.9. kbyte/sec. For example, maximum throughput support for 150-byte records is 1.3 million records for each busy hour.

Secondary file processing is an optional capability that is supported by the SuperNode Billing Application (SBA). With secondary file processing, the previously-output indicator is set in every AMA billing record in all AMADNS billing files in the *closedSent* directory.

When secondary file processing is activated, the processed file is sent to the *closedSentProcessed* directory, which resides in the logical volume defined for the billing stream. A successfully processed file is available for repoll from the *closedSentProcessed* directory.

If a file is not successfully processed, the system generates an SDMB655 information log indicating that it was unable to update the previously-output indicator for the file. The unprocessed file remains in the *closedSent* directory, and is available for repoll from the *closedSent* directory.

SBA Automatic File Transfer application overview

Functional description

SuperNode Billing Application (SBA) Automatic File Transfer (AFT) is a data communications application that allows Device Independent Recording Package (DIRP) files to be transferred automatically from the CS 2000 Core Manager to a downstream collector.

ATTENTION
Automatic File Transfer is an optional application, and is not required for SBA.

The SBA AFT application

- transmits billing files to the downstream collector (processor) in chronological order
- supports retransmission of files previously transferred to the downstream collector
- retransmits files previously transmitted to the downstream collectors by AFT
- supports only one billing stream of a specified format. The following table lists the values that must be used when SBA installed.

Required values for SBA

Field	Required value
Billing stream name	OCC
Stream record format	CDR250
File format type	DIRP

Components

The SBA AFT application provides the following components to transfer billing files to the downstream collectors.

SBA AFT components

Component	Description
Message Transfer Protocol (MTP)	Transfers billing files in 2048-byte fixed block, via AFT software, through the CS 2000 Core Manager Ethernet connection
AFT transfer utility	Maintains data integrity and ensures that no records are lost between the CS 2000 Core Manager and downstream systems.
AFT maintenance interface commands	Configure, monitor and control AFT sessions

Controlling an AFT

This section describes AFT file types, file transfer order and AFT commands.

AFT file types

A billing file is assigned an AFT status depending on where the file is in the AFT process. The AFT software uses the file types in the following table.

AFT file types

Status indicator	File type	Description
A->	Active	Currently being transferred by the AFT session. The file has a DIRP file name prefix (A, U or P).
O->	Override	Marked to be transferred after the file that is currently transferring and before the next logical file in the AFT session file list
N->	Next	Marked internally by the AFT session to be transferred after the Active transfer has completed
R->	Recovery	Contains data from the recovery stream. The recovery stream operates only when billing records on the CM emergency backup volume must be transferred. Recovery files are indicated as such through the AFT maintenance interface session Query utility.

File transfer order

The following table lists the rules that AFT uses to determine the file transfer order during normal operation.

AFT rules for file transfer order (Sheet 1 of 2)

Rule	Description
1	When an AFT session starts, the oldest pending file is selected as the next file to transfer.
2	For each subsequent file transfer, the Override file, if there is one, is chosen first. An Override file can be set manually by using the **Setfile** command in the AFT level of BILLMTC.[a] If no Override file exists, the next logical file is chosen. Each time a file transfer starts, the next oldest transferable file is the new Next file. It can also be a file with a Partial File Transfer (PFT) status. When a file is successfully transmitted, the status of the file changes from Unprocessed to Processed. For example, billing file U980224092602OCC (closedNotSent) changes to P980224092602OCC (closedSent, written to tape). After a refresh, the name of an open file that appears in the transfer list can change. For example, a file name such as A980224092602OCC (open file) that appears in the transfer list can change to U980224092602OCC (closedNotSent) or to P980224092602OCC (closedSent, written to tape).
3	The files transferred by AFT are listed in chronological order, according to UNIX file creation date and time.[b]
4	An AFT session may omit the transfer of some billing files, if the TCP connection with the downstream client is disconnected for more than 7 days. At this time, the AFT sessions internal registration with the CS 2000 Core Manager Billing File Manager expires.
5	Billing files can change to a Processed status during the time period between the disconnect and re-establishment of a TCP connection. You must manually add these Processed files to the AFT session for transmission to the downstream collector.
6	Automatic retransfer of a file occurs when the error message CNT-ERR with error value 00xECx0C (Data Media Error) is received from the AFT Client. When this message is received, the AFT server stops transferring the file, sets the last acknowledged block to 0, and starts transferring the same file from the beginning. A file with at status of Partial can be retransmitted from the beginning by using the **Rsetfile** command in BILLMTC.

AFT rules for file transfer order (Sheet 2 of 2)

Rule	Description
7	Automatic termination of a file transfer occurs when the error message CNT-ERR with value 00xE1x01 (Data Out of Sequence Error) is received form the AFT client. This error indicates that a problem has occurred with the sequence of data blocks between the AFT server and client. Receipt of this message • generates a critical alarm under SDMBBILL on the MAPCI • generates an alarm log • stops the file transfers for that AFT session
8	If a file is interrupted while being transferred, it is marked PFT (Partial File Transfer). The number of the last block that was acknowledged by the downstream collector is saved for the file. Once connectivity is reestablished with the downstream collector, transfer continues starting with the block one greater than the last acknowledged block. File transfers can be recovered when[c] • a connection with the downstream collector is disrupted. • conditions occur that require the AFT session to stop. For example, a CNT-ERR error message with value 00xE3x03 is received from the AFT client. • the AFT server detects a data block acknowledgement timer time out.
9	An internal retry counter is pegged for a file interrupted during transfer. If the number of transfer retries for the file exceeds the datafill limit, an AFT critical alarm with a corresponding log is generated, and the session stops. The file is not retransferred unless an AFT command in the AFT level of BILLMTC issued for the file to reset its status (retry count). The retry counter is configured through the AFT level of BILLMTC. The retry counter value cannot be changed for an active AFT session. That is, you must stop the AFT session to change the count.

a.The name of a billing file does not change when it is set as an Override file the by the AFT server.

b.In a non-Distributed Computing Environment (DCE), time changes can reset the time backwards. File names can result that indicate a file creation date and time before the creation date and time of files that were created earlier. Sorting these files by the time stamp in each file name does not reflect the true order of creation. Backward time changes can also result in duplicate file names. The chronological transfer order of these files cannot be guaranteed.

c.A maximum of only 50 PFT files is allowed. If this limit is exceeded, the session stops and the user must either delete a file or files, or reset the PFT state of some or all of the files. Refer to the Rsetfile command for more information on resetting the file state.

User interface

The AFT user interface is in the billing maintenance interface (BILLMTC), which is similar to the MAP (maintenance and administration position) for the CM. You can control and monitor AFT sessions through the AFT maintenance interface. To Access BILLMTC, use either Telnet or Enhanced Terminal Access (ETA). For more information about ETA, refer to Enhanced Terminal Access overview.

AFT commands

The AFT commands control and monitor AFT sessions and transfer of billing files over Transmission Control Protocol/Internet Protocol (TCP/IP) through an Ethernet connection to the downstream collector. The commands are available using either SDMRLOGIN or from BILLMTC. To access the AFT level of BILLMTC, enter **BILLMTC;APPL;AFT**.

The following table describes AFT commands.

AFT commands (Sheet 1 of 3)

Command	Function
Quit	*Quits the AFT level and returns to the APPL level.*
AFTCONFG	*Accesses the AFTCONFG subdirectory (AFT sublevel)* The AFTCONFG subdirectory is accessed from the AFT level, and allows you to configure the AFT sessions. The subdirectory contains commands that **Add**, **Delete**, **Change**, and **List** tuples in the AFT configuration table automaticFileTransferTable in the management information base (MIB).
Add	*Adds AFT tuples in the automaticFileTransferTable in the AFT MIB database* The **Add** command requires the stream name as an argument, and does not acquire the stream set as the default stream by the **Set** command.
Delete	*Deletes AFT tuples from the automaticFileTransferTable in the AFT MIB database*
Change	*Changes the value of the retry attempts field for an AFT session tuple in the automaticFileTransferTable in the AFT MIB database*

AFT commands (Sheet 2 of 3)

Command	Function
List	*Lists AFT tuples in the automaticFileTransferTable AFT MIB database* If a session name or stream name is not specified, the **List** command displays all tuples in the automaticFileTransferTable table. The command does not acquire the stream set as the default stream by the **Set** command.
Query	*Queries information about the file transfer list for AFT sessions*
	Displays all files in the transfer list that meet specified criteria. (For a list of file status indicators, refer to table AFT file types.)
Setfile	*Sets an override pointer on a specified AFT file* The override indicator (*O->*) appears next to the file specified by the second parameter. The file specified by this command is the next file to transfer. Any file in the list, except the active file, can be made an override file.
	Deletes a file from an AFT session file list The command does not erase a billing file from disk or delete a file that is currently transferring. An unprocessed file changes to a processed file when other AFT sessions and CS 2000 Core Manager applications finish with the file. Processed files remain unchanged.
Rsetfile <PFT | OVR>	***(<PFT>)*** *Resets a file from Partial to Pending* The command resets the transfer status from Partial to Pending and the last acknowledged block to 0. This option works only for files with a transfer state of Partial. When a reset file transfers, the transfer starts at the beginning of the file.
	(<OVR>) *Resets Override file information* With the Override (OVR) option, the Override (*O->*) indicator is deleted from the file display, and the file with the Next (*N->*) pointer is the next file to transfer. The **Rsetfile** command does not execute while the override file is transferring.
AFTRESND	*Accesses the AFTRESND subdirectory (AFT sublevel)* The subdirectory contains commands that allow you to add files that are already processed to an AFT session list for retransmission to the downstream collectors[a]
Listfile	*Lists processed files for the specified stream*

AFT commands (Sheet 3 of 3)

Command	Function
Addfile	*Adds a processed file to an AFT session file transfer list for retransmission to the downstream collector*
Start	*Starts a new AFT session transferring billing files* *Restarts an AFT session ended by the **Stop** command*
Stop	*Stops an AFT session from transferring billing files* AFT stops transferring files after the completed transfer of the current file. The **Stop** command does not interrupt the current transfer.
Alarm	*Queries the status of and cancels the following AFT session alarms*[b] • *Critical*: occurs when a network connection is disrupted during file transfer, the transfer retry count has been exceeded for a file, and the Data Out of Sequence error is received • *Major*: occurs when a session is stopped by AFT maintenance interface command
Help	*Provides information about AFT commands*
Refresh	*Refreshes the current screen*

a.If the AFT application is busied (BSY) and returned to service (RTS), the AFT sessions lose processed files that are in the file transfer list. You must add the files to the file transfer list through the AFTRESND level of BILLMTC. Processed files can figure in the file transfer list if an unprocessed file is written to tape and moves to the closedSent directory, or if a file form the closedSent directory is added to the file transfer list through the AFTRESND level.
b.A cancelled AFT alarm can re-occur if the cause of the alarm is not cleared.

If a new billing file(s) is opened (because of SBA file rotation) while an AFT session is transferring a previously closed file, the new file is not visible on the AFT query list for the session until the transfer of the previously closed file is complete. The period of time that the newly opened files(s) is not visible depends on AFT throughput and the size of the transferring file.

The following table shows the amount of time that AFT requires to transfer files based on their size, assuming a throughput of 100 Kbytes/sec.

File Transfer time periods for AFT

File size (MBytes)	Throughput (KBytes/sec.)	Time (sec.)
20	100	204
10	100	102
5[a]	100	51
1	100	10

a.Recommended scheme.

The time period during which the new files are not visible is less than or equal to the file transfer time listed in the table. To avoid excessive delay in the visibility of billing files, it is recommended that SBA files be set up to be rotated when their size reaches 5 MB.

Files that are closed during this period of time are still displayed on the AFT query list as open/active. For example, closed file U020220123776OCC, appears as A020220123776OCC because it was open at the beginning of the current file transfer. At the end of this time period, the closed files are displayed with the correct name (that is, prefixed with the letter *U*).

For a new AFT session, billing files that are in the closedNotSent directory are listed as PENDING files by the AFTquery command (for that session). If SBA initiates a file rotation while AFT is transferring a PENDING file, you must wait until the current file transfer is complete before you can override the order of sending files (that is, set any subsequently opened billing files or the previously closed billing file as the next file to transfer). Previously closed files are not affected, and their order of sending can still be controlled.

To avoid resending files, AFT polls SBA for the list of files at the end of every transfer. The time required for the poll depends on the size of the billing file (created by SBA) and throughput of AFT (Refer to table File Transfer time periods for AFT for transfer times).

Restrictions and limitations

The SBA AFT application *does*

- require that the downstream collector always initiate a TCP/IP connection with the CS 2000 Core Manager. The collector must use port number 30000 (HEX 7530) to establish a connection for file transfers.
- support a maximum of 10 billing destinations. One connection establishment is allowed for each downstream collector.
- use an MTP data acknowledgment window size of 1 block
- supports a 2048-byte fixed data block size
- use the DIRP file name for the MTP message file name
- support a maximum of 50 partial files for each session
- support only one specific stream (OCC) with a specific format (CDR250)

The SBA AFT application does *not*

- provide AFT client software. AFT client software must be compliant with the protocol semantics implemented and used by SBA AFT.
- support the Multi Network Protocol (MNP), which is a modified MTP implementation
- variable data block size
- a file size >134.215680 Mb (65,535 blocks of 2048-byte size)
- support the use of file naming conventions other than DIRP file naming conventions
- support filtered streams

AMADUMP overview

Functional description

Amadump is a CS 2000 Core Manager tool that allows users to filter and view records from both standard AMA files and DIRP formatted files. The output can be refined by limiting the maximum number of records to search and display. In the case of DIRP formatted files, amadump allows users to specify the start block of the record from which to begin the search.

You can display all the records using amadump or you can create filters that allow you to display only records matching a specific search criteria. You view the results of amadump on your screen. You can display more records on your screen by first setting the display to compact using command "`set display compact`" from the AMADUMP prompt.

The amadump command is available from the maintenance interface on the CS 2000 Core Manager at the billmtc level, and the CM at the sdmrlogin level.

> ***Note:*** Amadump only views files that are created while the BAFSuppression mib is set to the same value at the time the command is issued. For example, if you change the BAFSuppression mib value after the stream is turned on, you are unable to use amadump to view files that are created prior ot you changing the mib.

You can perform the following tasks with the amadump command:

- dump records
- maintain a list of filters
- specify the number of records to search and output
- specify the starting block of DIRP files
- list fields
- set the record display to compact or regular
- request help
- quit to exit amadump

Enhanced Terminal Access overview

Functional overview

The Enhanced Terminal Access (ETA) application provides secure remote access to the CS 2000 Core Manager across transmission control protocol/Internet protocol (TCP/IP)-based local- and wide-area networks (LAN/WAN). ETA has a server on the CS 2000 Core Manager and either an ETA client or an ASCII Terminal Access (ATA) client. ETA supports

- CS 2000 Core Manager applications that have a command line interface, such as the CS 2000 Core Manager maintenance interface
- CS 2000 Core Manager 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 CS 2000 Core Manager or CM.

Components

ETA has one server application installed on the CS 2000 Core Manager, 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 for ETA.

ETA components (Sheet 1 of 2)

Component	Description
ETA server	Provides Telnet emulation of CM and CS 2000 Core Manager for ETA and ATA clients; logs client applications into CM and CS 2000 Core Manager; handles information exchange between the CM and CS 2000 Core Manager and clients; supports max. 50 CM sessions. Max. number of sessions depends on number of TCP sessions used on DMS (configured in Table IPHOST in DMS switch); supports up to 64 CS 2000 Core Manager sessions.
ETA client	Connects to ETA server to perform CM and CS 2000 Core Manager 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 (Sheet 2 of 2)

Component	Description
ATA client	Connects to ETA service to perform CM and CS 2000 Core Manager 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 CS 2000 Core Manager. (UserIDs must be set up in DCE before using ETA). For more information about DCE, refer to Secure File Transfer overview.

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 CS 2000 Core Manager and CM-hosted sessions.

ETA control characters (Sheet 1 of 2)

Character	Function
Ctrl B	Toggles break mode ON or OFF[a]
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
Ctrl \	Toggles control character sequence ON or OFF[b]

ETA control characters (Sheet 2 of 2)

Character	Function
Delete key	Deletes the current character
?	Recalls one of the last three lines (depending on the number of ?s)

a.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.
b.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 CS 2000 Core Manager-hosted sessions, the control characters are off by default.

Secure File Transfer overview

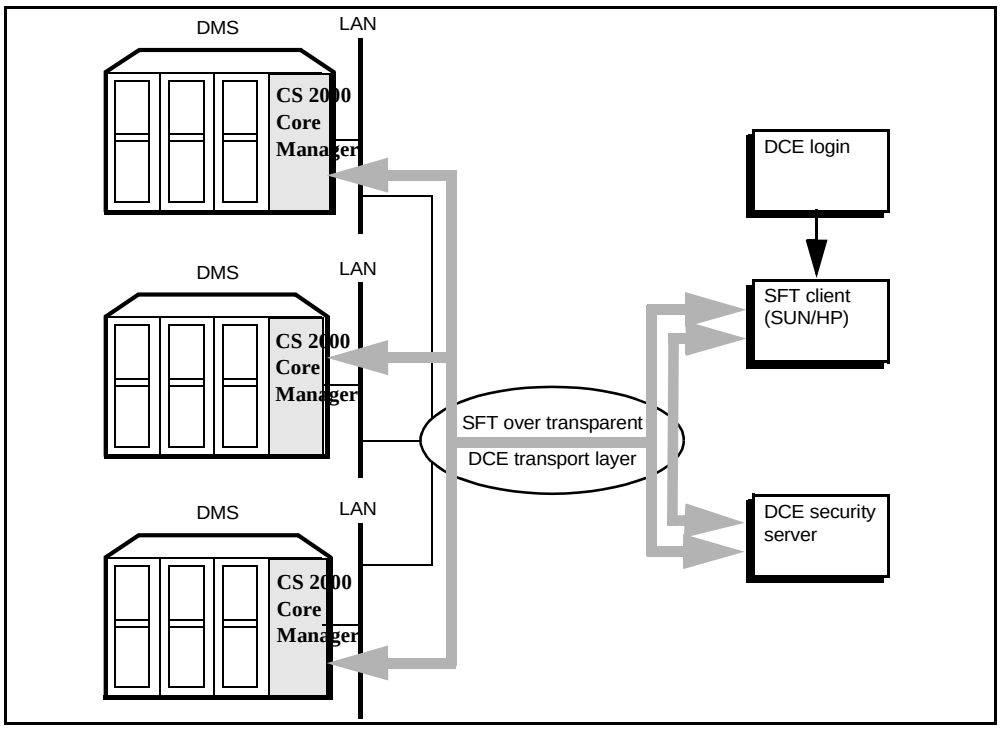
Functional description

The Secure File Transfer (SFT) application provides file transfer to or from a DMS SuperNode or CS 2000 Core Manager 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.[1] 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



[1] For DCE-based SFT, the SFT server and client user must be configured in the DCE cell.

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

Components of DCE-based SFT

Component	Description
SFT client	Provides secure file transfers to and from the CS 2000 Core Manager 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.
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 and 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. The following table describes workstation login configurations.[2]

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

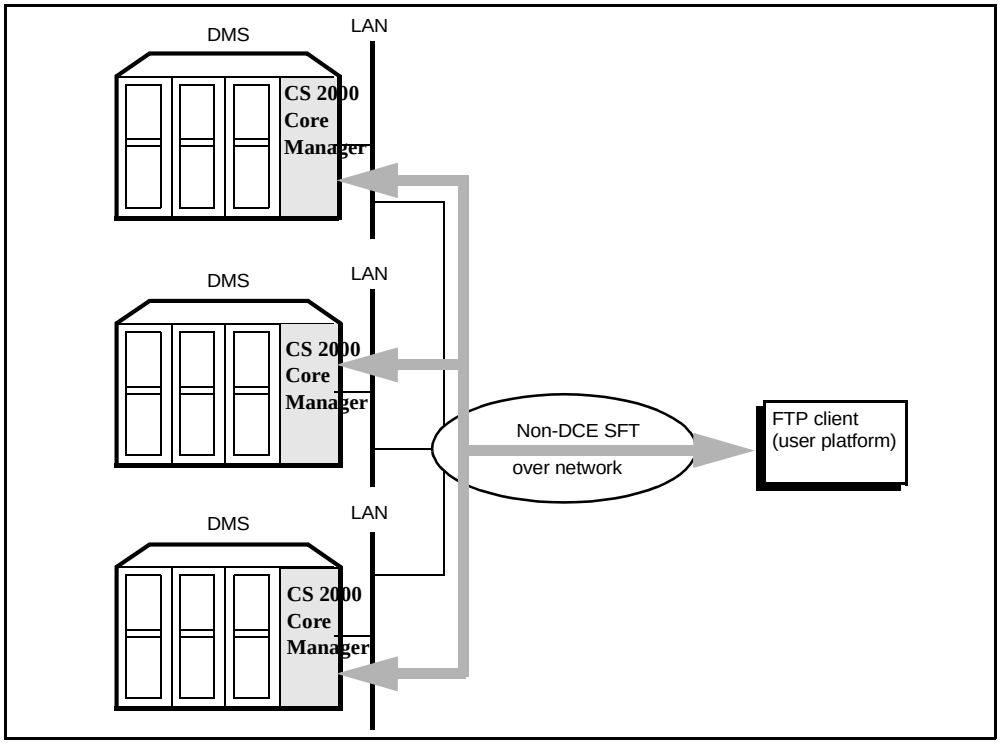
Non-DCE based configuration

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. The configuration does not provide user authentication and therefore, no secure file transfer.

[2] For more information on logging in to DCE, refer to “Configuring the SFT server.”

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 CS 2000 Core Manager. The following figure shows how an FTP client uses FTP to connect to the CM and the CS 2000 Core Manager.

Non-DCE based SFT application



DMS Data Management System overview

Functional overview

The DMS Data Management System (DDMS) application runs on the CS 2000 Core Manager platform, provides an interface for accessing DMS provisioning data, and supports the Operation Support System Data Interface (OSSDI). The OSSDI is a DMS common machine interface that defines a message protocol between the operations support system (OSS) and the DDMS.

Hardware

The following table describes the hardware components associated with the DDMS. For details of DDMS requirements, refer to the procedure “Installing DDMS.”

DDMS components

Component	Description
Client workstation	Runs the client application or web browser
Web server	Manages communications with the client workstation
CS 2000 Core Manager	Is the host for the DDMS

Software

Use the latest software version and patch loads available. For details of DDMS requirements, refer to the procedure “Installing DDMS.”

The following table describes the interactive DDMS subsystems.

DMS subsystems (Sheet 1 of 2)

Subsystem	Description
User administration (uAdmin)	Controls user authorization profiles through OSSDI commands; assigns client, operation, table and network element (NE) security groups
Communications router (COMMS)	Controls communications between external clients and local DDMS subsystems, and communications between local subsystems; provides single point of entry into DDMS through a DCE/RPC interface

DMS subsystems (Sheet 2 of 2)

Subsystem	Description
Synchronization interaction and maintenance (SIMS)	Propagates table updates to the computing module (CM); handles maintenance for provisioning
System administration (SysAdmin)	Supports commands for system parameters, logs and process control
Transaction manager (TxMgr)	Coordinates interactions between the client and the DMS

DMS Maintenance Application Overview

Functional description

The DMS Maintenance Application on the CS 2000 Core Manager is used to communicate trunk and line maintenance messages from the Preside Management for Succession Solutions (MSS) to the Computing Module (CM) through the CS 2000 Core Manager maintenance interface.

The DMA translates the OSSDI trunk and line maintenance messages into a format that the CS 2000 Core Manager maintenance interface understands and can forward to the CM.

Image Dump Service Application overview

Functional description

The image dump service application on the CS 2000 Core Manager is an interface between the system load module (SLM) on the call server's computing module (CM) and the CS 2000 Core Manager. 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 CS 2000 Core Manager. The CS 2000 Core Manager 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 CS 2000 Core Manager 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 CS 2000 Core Manager 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, 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.

SWIM level

```
   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 maint 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 CS 2000 Core Manager. 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	Collects logs generated by the CS 2000 Core Manager and the computing module on the call server, and delivers them to operational support systems (OSS). It includes the *logquery* and *logroute* tools.
Log delivery service client	Runs on a remote workstation, and includes the *logreceiver* tool.
Generic data delivery (GDD)	Provides a permanent storage mechanism for logs. (See Generic Data Delivery overview in the Basics section)
Passport log streamer	Collects Passport logs from the Preside MDM, and delivers them to an OSS. This application fileset is only required for Succession offices where the CS 2000 Core Manager needs to communicate with the Preside MDM for fault data.

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 section.

Log Delivery application tools

The Log Delivery application in the CS 2000 Core Manager base software platform sends user-defined streams of DMS and CS 2000 Core Manager logs to a maximum of 30 operations support systems (OSS) and 30 UNIX files on the CS 2000 Core Manager. 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 CS 2000 Core Manager 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. • 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 1:*** Settings changed by the Log Delivery global parameters menu does not affect GDD settings or the logs in /gdd volume. ***Note 2:*** You do not have to busy the Log Delivery application and return it to service to activate the changes made in the Device List Global Parameters GDD Configuration menus. The changes are active when you save them. • delete logs and log types • modify the output device list (parameters, device type, format)

The logroute log commissioning tool includes an online help facility that provides valid parameter ranges and default values. To route logs from an CS 2000 Core Manager to a workstation, the CS 2000 Core

Manager 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 only by 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. Logs in STD format specify switch and node (CS 2000 Core Manager) names. Formatting can be set for each device.

Log Delivery procedures

The following table includes a list of procedures in this document that are associated with Log Delivery application and tools.

Log Delivery procedures (Sheet 1 of 2)

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 section
add a TCP, TCP-IN, or file device	“Adding a log device using logroute” in the Configuration section
change the set of logs sent from the CM	“Changing the set of logs sent from the CM” in the Fault section
commission the log delivery CM configuration file	“Commissioning the Log Delivery CM configuration file” in the Configuration section
commission the log delivery global parameters	“Commission the Log Delivery global parameters” in the Configuration section
configure a CS 2000 Core Manager for fault forwarding	“Configuring a CS 2000 Core Manager for fault forwarding” in the Configuration section

Log Delivery procedures (Sheet 2 of 2)

If you want to	Use procedure
delete a log device	“Deleting a device using logroute” in the Fault section
display log records	“Displaying or storing log records using logreceiver” in the Fault section
install the log delivery application filesets	“Installing and configuring the log delivery application” in the Configuration section
install and configure log delivery service	“Installing and configuring the Log Delivery application” in the Configuration section
install and configure the pserver application	Refer to the Preside MDM information for instructions on how to install and configure the pserver application.
install the logreceiver tool	“Installing the logreceiver tool on a client workstation” in the Configuration section
view logs	“Retrieving and viewing log records” in the Fault section
specify logs to be delivered	“Specifying logs delivered to a device” in the Fault section
store logs in a file	“Displaying or storing log records using logreceiver” in the Fault section
troubleshoot log delivery problems	“Troubleshooting the Log Delivery problems” in the Fault section

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 aCS 2000 Core Manager 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 aCS 2000 Core Manager to a workstation using the logreceiver tool, ensure

- the logreceiver tool is installed on the workstation. Refer to the procedure titled “Installing the logreceiver tool” in the Configuration section.
- the CS 2000 Core Manager is configured to send logs to a TCP device. Refer to the procedure titled “Adding a log device using logroute” in the Configuration section.

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 titled “Displaying or storing log records using logreceiver” in the Fault section.

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 CS 2000 Core Manager.[1]

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 Mbyte. This is based on a 3 Mbyte file size for each 12-hour period. The calculation, using the above formula is: 3 Mbyte 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 overview.

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

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 CS 2000 Core Manager 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 procedure "Commissioning or decommissioning Network Time Protocol (NTP)" in the Configuration Management section.

GR-740 Passthrough overview

Functional description

The GR-740 software application on the CS 2000 Core Manager enables the CS 2000 Core Manager 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 CS 2000 Core Manager 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 CS 2000 Core Manager. 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 SPM.

Bootp Loading Service Overview

Functional description

The bootp loading service application on the CS 2000 Core Manager allows electronic software loading of multi-service platform (MSP) nodes. This includes initial image loading (IBL), as well as software delivery for regular software upgrade of MSP nodes.

A bootable image resides on the CS 2000 Core Manager in a predefined location and is used to load the MSP nodes at installation time or whenever the initial boot image is required to restart the MSP nodes. Basically, an MSP node sends a bootp request to the CS 2000 Core Manager bootp server. The CS 2000 Core Manager bootp server responds with an acknowledge reply, which contains the MSP node's IP address and loadname. Once the MSP node receives the reply from the CS 2000 Core Manager bootp server, it sends a request to the CS 2000 Core Manager tftp server to begin transfer of the load.

The bootp loading service application is managed using the Software Inventory Manager (SWIM) on the CS 2000 Core Manager.

CS 2000 Core Manager-to-MDM connectivity overview

Functional description

In a Succession configuration, the CS 2000 Core Manager has Ethernet connectivity to the Preside Multi-Service Data Manager (Preside MDM). After operating company personnel log into the CS 2000 Core Manager, they can then use this connection to access both of the Preside MDMs as well as the ATM Network Management System (NMS) software which runs on the Preside MDMs.

Users can establish a connection to the CS 2000 Core Manager by any of these methods:

- an enhanced terminal access (ETA) session
- an ASCII terminal access (ATA) session
- a telnet session

Once user authentication has been confirmed on the CS 2000 Core Manager, users can access any of the existing NMS software tools, including GUI and CLI tools, to interact with the Passport-based network element manager. No further user authentication is needed.

The CS 2000 Core Manager and Preside MDMs connect through a redundant Ethernet LAN that consists of two Passport 6480s with fault-tolerant connections to the CS 2000 Core Manager side through 10baseT ports and simplex connections to a pair of redundant Preside MDMs. Pre-existing LAN connectivity monitoring mechanisms on the CS 2000 Core Manager provide tools to monitor the CS 2000 Core Manager's physical connectivity to the LAN and its IP connectivity to the Preside MDMs.

Limitations and restrictions

The following limitations and restrictions apply to this configuration of CS 2000 Core Manager-to-Preside MDM connectivity.

- Existing CS 2000 Core Manager and Preside MDM connectivity monitoring agents cannot pinpoint the exact location of a physical break in the common LAN, other than a fault directly in one of the Ethernet cards (or its related link).
- Management of the common LAN occurs through the NMS software that runs on the Preside MDMs.
- Faults in the LAN beyond the scope of the CS 2000 Core Manager are detected and reported by the Preside MDMs. Fault notifications are relayed to the CS 2000 Core Manager through a log stream. The element manager does not perform any explicit fault correlation.

- The CS 2000 Core Manager monitoring agent also checks the quality of the link and produces a customer log if excessive Cyclic Redundancy Check (CRC) errors occur in incoming Ethernet frames. The corresponding monitoring agent on the Preside MDM side also produces customer logs for excessive CRC errors in its Ethernet cards. No other link quality tests occur.
- The CS 2000 Core Manager-to-Preside MDM connection is not used for software loading on the Preside MDM. All Preside MDM software loading must be done directly with the machine.

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 CS 2000 Core Manager:

- Ethernet REX
- CPU REX

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

Log report SDM630 is generated when a REX test is invoked to indicate the start time. The same log report is generated when a REX test has completed 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 procedure “Performing a REX test” in the Fault section 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 CS 2000 Core Manager 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 impact 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 the “maxuproc” value is set to “500”
  - verifies the “maxmbuf” value is set to “0”
  - verifies the “maxpout” value is set to “31”
  - verifies the “minpout” value is set to “15”
  - verifies the “cms_notify_meth” value is set to “/sdm/mtce/smm/smm_cms_notify”
  - verifies the “cms_notify_attr” value is set to “condition,req_condition”
  - verifies the DAT drive block size is set to “512”
  - verifies no runaway processes exist
  - checks for excess CPU usage
  - verifies that the appropriate SDM processes are running
  - verifies the autorestart flag is set to “true”

The system audit is set by default to run all checks 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 section.

Related procedures

Refer to the following procedures to perform tasks related to the system audit:

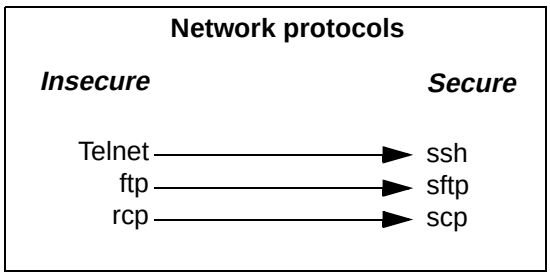
- “Performing a system audit” in the Fault section
- “Viewing the system audit report and taking corrective action” in the Fault section
- “Disabling or enabling/changing the time of a system audit” in the Fault section
- “Clearing a system audit alarm” in the Fault section

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 URL 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 CS 2000 Core Manager from a remote system or log in to a remote system from the CS 2000 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 CS 2000 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 sources for SSH clients.

Sources for SSH clients

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

a.Sources for SSH clients are not limited to those listed in this table.

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

  Using scp, you can securily copy files to and from the CS 2000 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 CS 2000 Core Manager provides the following 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 the second or third method.

The basic utilities of OpenSSH are as follows:

- 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 procedure “Installing OpenSSH” in the Upgrades section 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 CS 2000 Core Manager component product and customer support includes the following areas:

- 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 either an answer to the problem or corrective action.

Corrective action can include the following:

- 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 CS 2000 Core Manager 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 CS 2000 Core Manager 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