



Carrier VoIP

Core and Billing Manager 850 Basics

Document status: Standard
Document version: 04.04
Document date: 20 October 2006

Copyright © 2006, Nortel Networks
All Rights Reserved.

The information in this document is sourced in Canada, the United States of America, and the United Kingdom.

This is the Way, This is Nortel, Nortel, the Nortel logo, the globemark design, and the NORTEL NETWORKS corporate logo, are trademarks of Nortel Networks. All other trademarks are the property of their respective owners. All rights reserved.

Contents

Core and Billing Manager 850 Basics	5
Dual LAN configuration 8	

4 Contents

Core and Billing Manager 850 Basics

New in this release for Core and Billing Manager 850 Basics in SN09U

Feature changes

The following feature-related changes have been made in the documentation:

- A00010422 - MTX14 CBM Sustaining
 - NN-20000-246: CBM850 Configuration Management for Wireless Networks
 - Updated software download
 - Updated software installation
 - System commissioning with new software
 - NN-20000-248: CBM850 Security and Administration for Wireless Networks
 - Statement on compatibility with MTX13
 - Updates on secure file transfer (SFT) for OMs
 - NN-20000-250: CBM Fault Management for Wireless Networks
 - New warning message for RstorDir.
- A00012465 - CBM User Authorization Integration With A Nortel Central Security Server
- A00012570 - Disabling Non-Secure Network Services in SSPFS
- A00012571 - CBM User Group Improvement
- A00012889 - Pass Phrase Protected Keys For SSH
 - NN-20000-246: CBM850 Configuration Management for Wireless Networks
 - NN-20000-248: CBM850 Security and Administration for Wireless Networks

- A00014576 - CBM Multi-net Support
- A00013193 - Record Count Log Support in SBA

Other changes

The following additional changes have been made in the documentation:

- Q01304841
Changes to MTXSRCH commands.
- Q01310597
Changes to ALM command.

Functional description

The Core and Billing Manager 850 (CBM 850) offers terminal access to the core, the ability to transfer files to and from the core, log delivery service, and applications for managing accounting data and operational measurement (OM) data. The CBM 850 enhances OAM&P functionality by enabling service providers to use their existing LAN resources to create an "operations intranet", with Ethernet connectivity from the core to upstream OSSs, off-loading OAM&P responsibilities from the core.

This document is applicable for both CDMA and GSM/UMTS users. Information that is specific to either CDMA or GSM/UMTS is highlighted where applicable.

CBM 850 hardware

The CBM 850 hardware resides on the carrier-grade, NEBS-compliant Sun Netra 240 server. The Sun Netra 240 server is 2U (3.5 in) high and is designed for high-availability (HA), containing two processors, redundant hot-swap power supplies, and two internal hot-swap RAID-1 mirrored hard disk drives that provide redundant, exact copies of system data. In addition, the server contains a DVD-RW drive, which facilitates easy media exchange for software delivery and backups.

Carrier-grade reliability of the CBM 850 is achieved through local redundancy of hardware components, configuration of redundant servers in an HA cluster, and high-availability software. The HA cluster provides automatic system resource fail-over and network mirrored data on the two servers in the cluster.

To configure SPFS console access, see procedure "Configure SPFS console access" in NN10409-500, *Nortel ATM/IP Solution-level Configuration*.

Network connectivity

Each of the two CBM 850 servers in a cluster is equipped with four Ethernet ports (GigE interfaces, 10/100/1000 auto sensing). Two Ethernet ports on each CBM 850 are directly connected to the mate CBM 850 in the cluster for HA reliability and data replication, creating a redundant, local interconnect LAN. The two remaining Ethernet ports on each CBM 850 are used for connection to the core, other Carrier Voice over IP network elements, managers, customer workstations, and Operation Support Systems (OSS). If a failure occurs on one of the ports in the Ethernet port pair, traffic is automatically routed through the other port and does not cause a fail-over from one CBM 850 to the other. The CBM 850 serves as a physical firewall between the OSS network and the DMS core, and does not allow IP traffic to flow through it.

The Ethernet fabric connecting the CBM 850 to the core and to the OAM LAN is not included as part of the CBM 850 product purchase. It is the responsibility of the customer to procure, engineer, install, and maintain the Ethernet fabric hardware and software components.

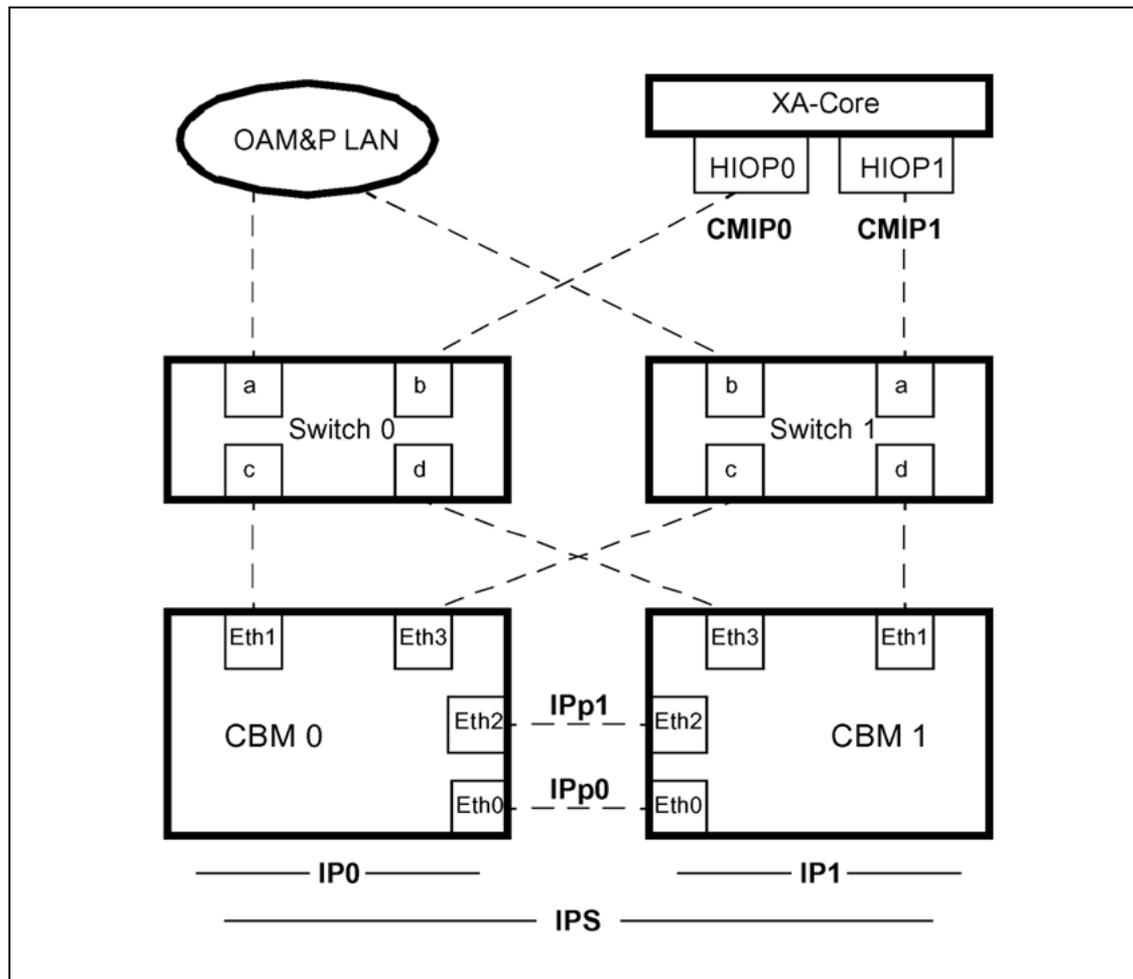
The following are the required characteristics of the Ethernet:

- Network latency/bandwidth of 50 ms
- 10/100/1000 BaseT, auto-negotiation
- Spanning-Tree Protocol (SPT) disabled
- Virtual Router Redundancy Protocol (VRRP)
- Redundant network, path availability greater than 99.999%
- Network management (OAM as required)
- IP Policy Filtering BootP forwarding (Packet CDMA)
 - No routing of messages between the public and private networks
 - The CBM can be the only public destination of messages routed out of the HIOP/CMIC interface (LX17AA) on the XA-Core card

The Ethernet fabric connecting the CBM 850 to the core and to the OAM LAN is not included as part of the CBM 850 product purchase. It is the responsibility of the customer to procure, engineer, install, and maintain the Ethernet fabric hardware and software components.

The following illustration shows the basic CBM 850 network connectivity.

CBM 850 network connectivity



CBM850 also supports an optional second public interface to physically segregate the OAM traffic from the CALLP/Core traffic.

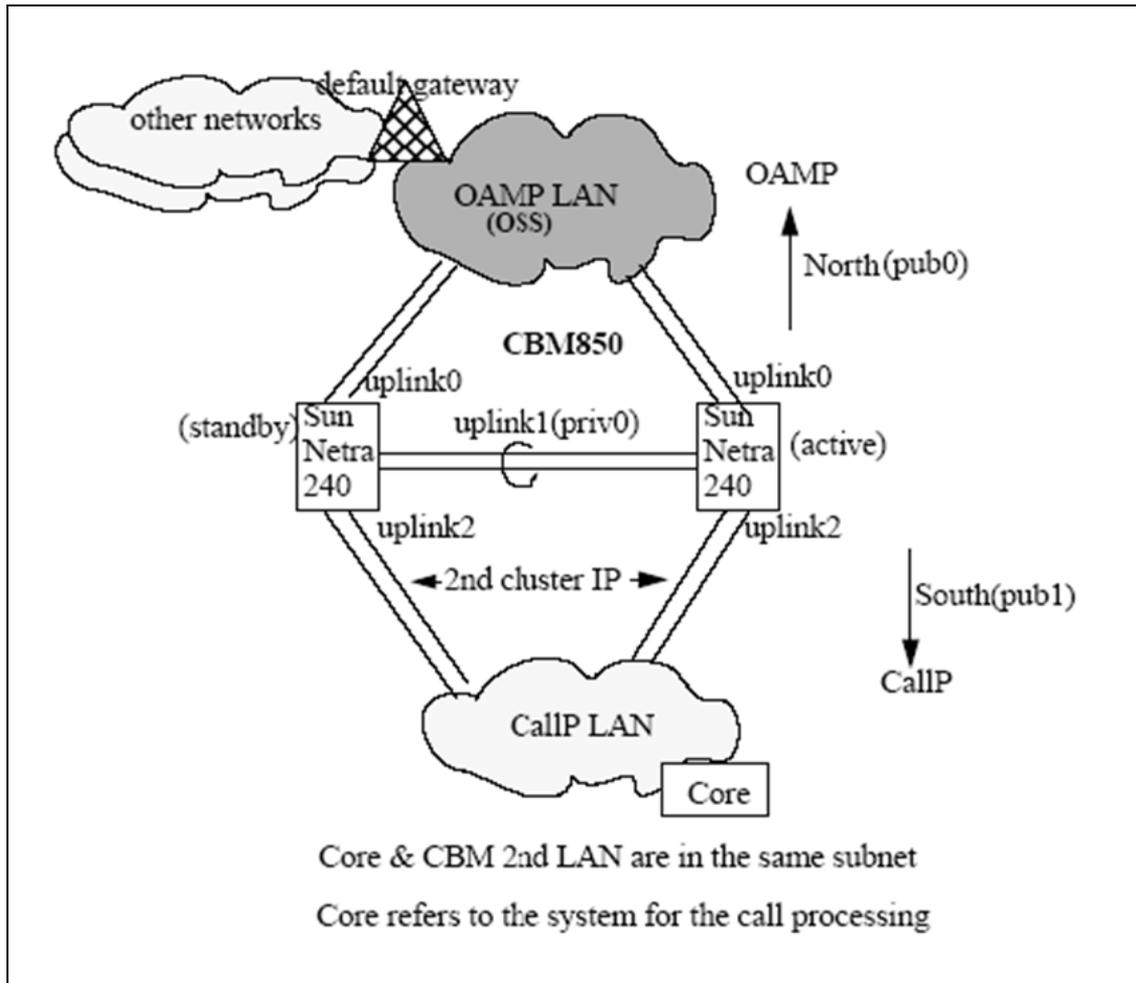
The DUAL LAN CBM requires three network or subnets (as defined by the IP and mask) and 9 IP addresses:

- uplink0- OAM public i/f, customer defined hostname, cluster IP, physical IP for each unit.
- uplink1- private i/f, default hostname, cluster IP, physical IP for each unit
- uplink2- CALLP hostname, customer defined cluster IP, physical IP for each unit.

Dual LAN configuration

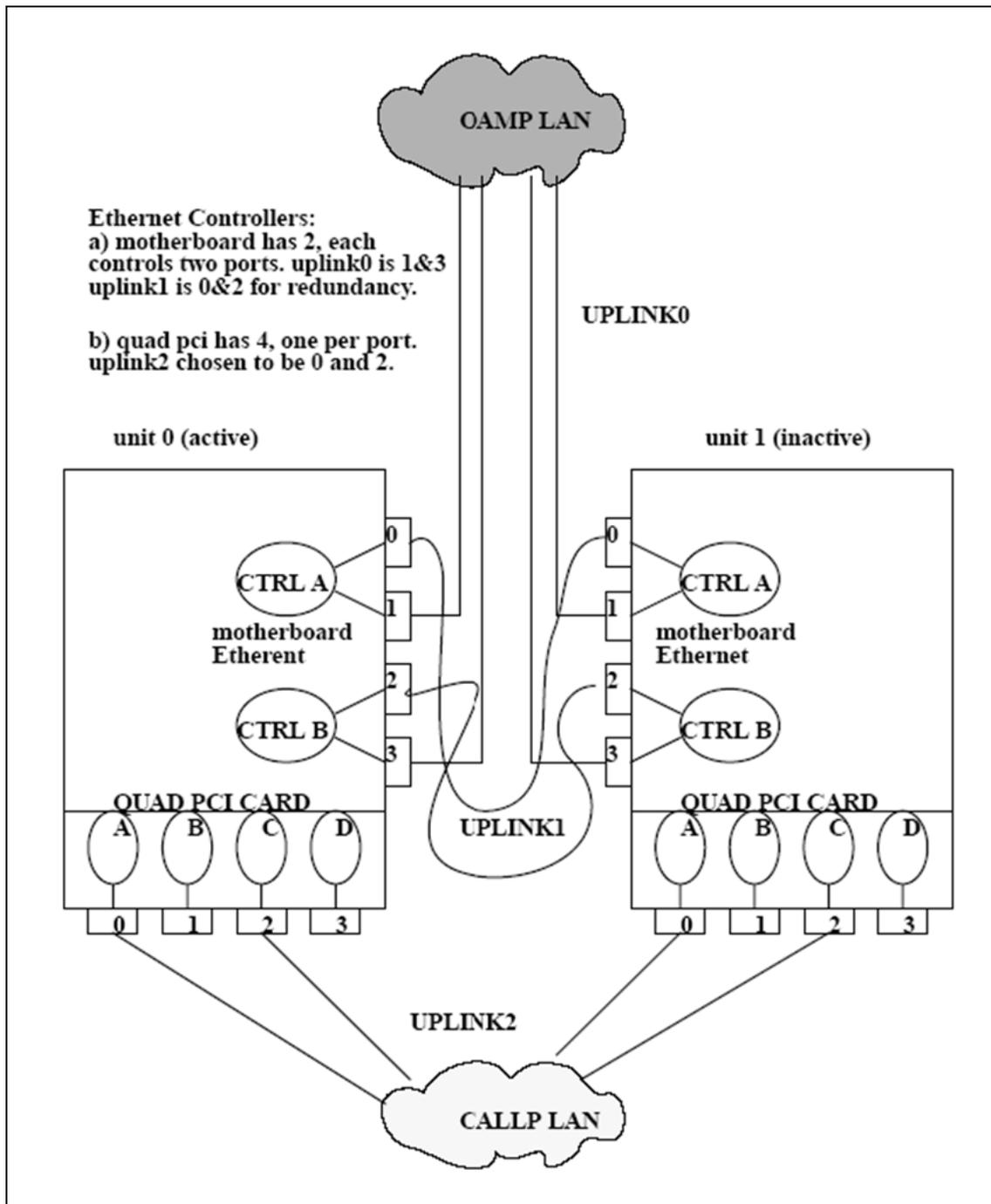
The CBM 850 can be configured into a Dual LAN configuration in order to segregate CALLP/Core traffic from the OAM traffic. Please see the following figure for an illustration of this configuration.

CBM 850 Dual public interface



The following figure illustrates the port assignments for the Dual LAN configuration.

CBM 850 Dual public interface - port assignments



CBM 850 software

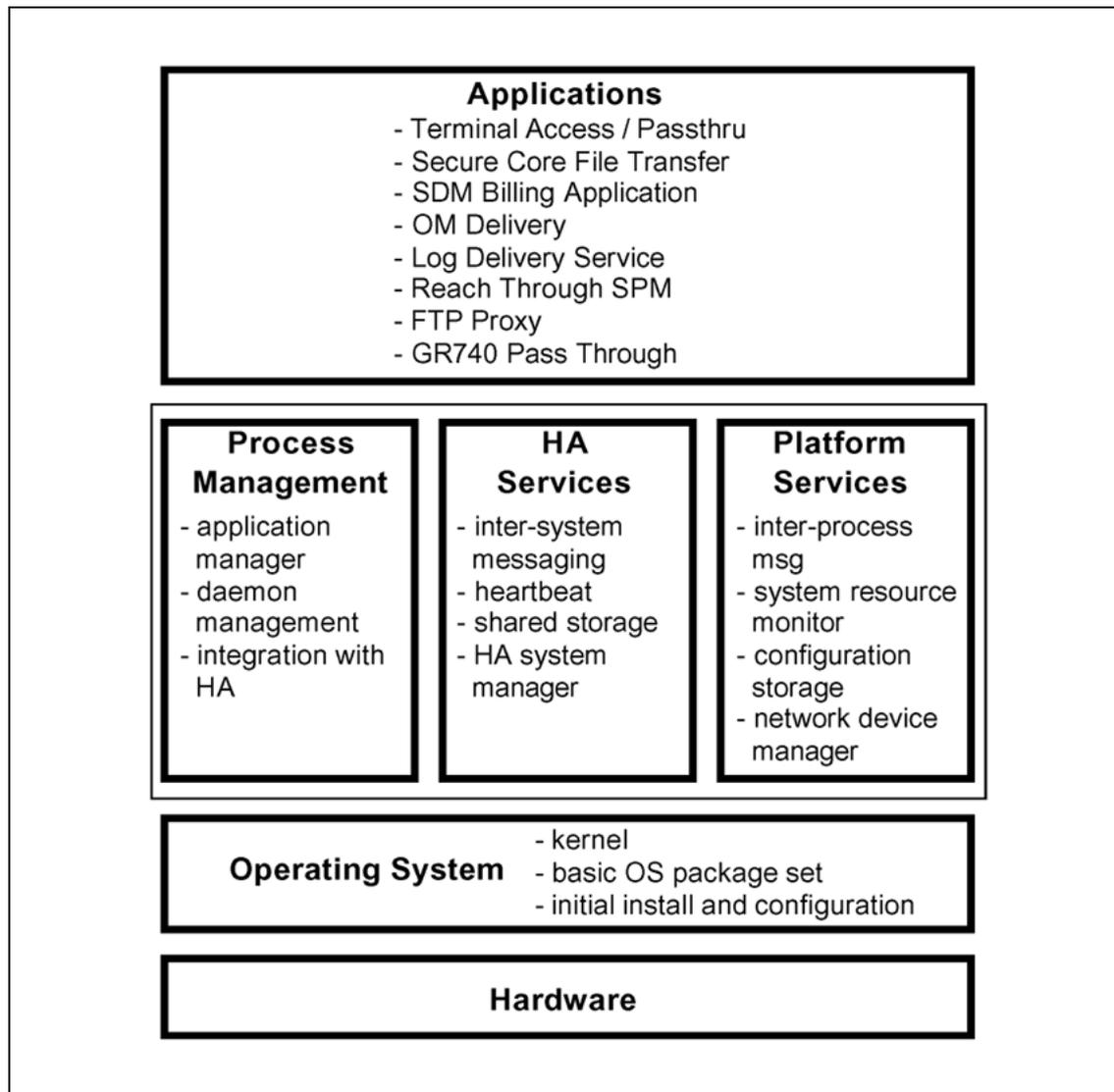
The CBM 850 software is built on top of the Succession Succession Packet CDMA Server Platform Foundation Software (SSPFS), which includes the operating system and several software components, tools, and utilities used

for managing system equipment and software. SSPFS provides a hardened operating system, routinely exercised with standard security vulnerability detection software.

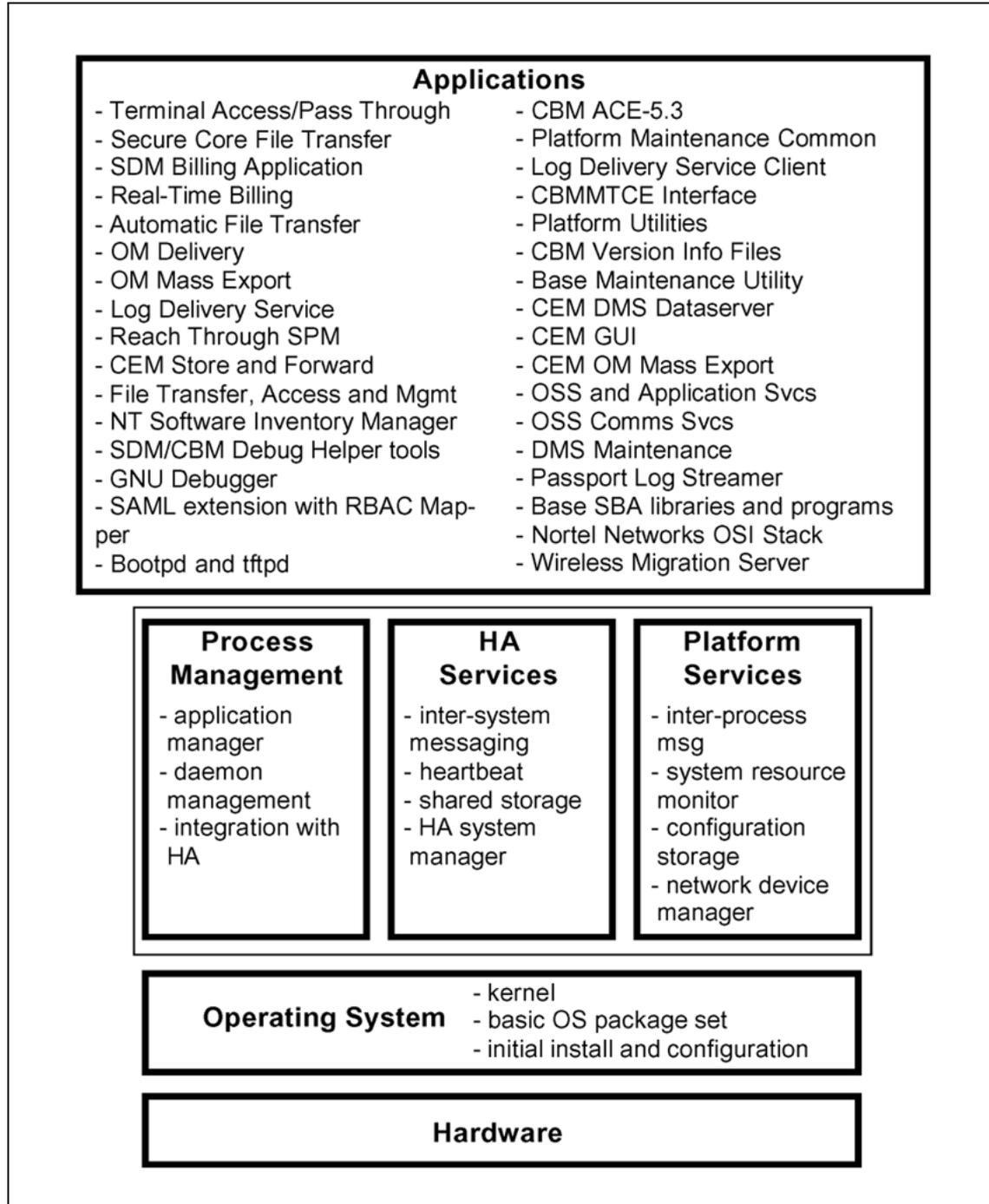
The base components of the CBM 850 software consist of the process management, HA services, and platform services subsystems. The process management subsystem provides control, monitoring, alarming, and recovery of the applications and other system processes. The HA services enable the cluster of CBM 850 servers to appear as one server, providing system-level monitoring, data replication across the servers, and resource migration from one server to the other. The platform services provide general tools used for administration and maintenance of the platform hardware and software.

The CBM 850 software architecture is shown in the following illustration.

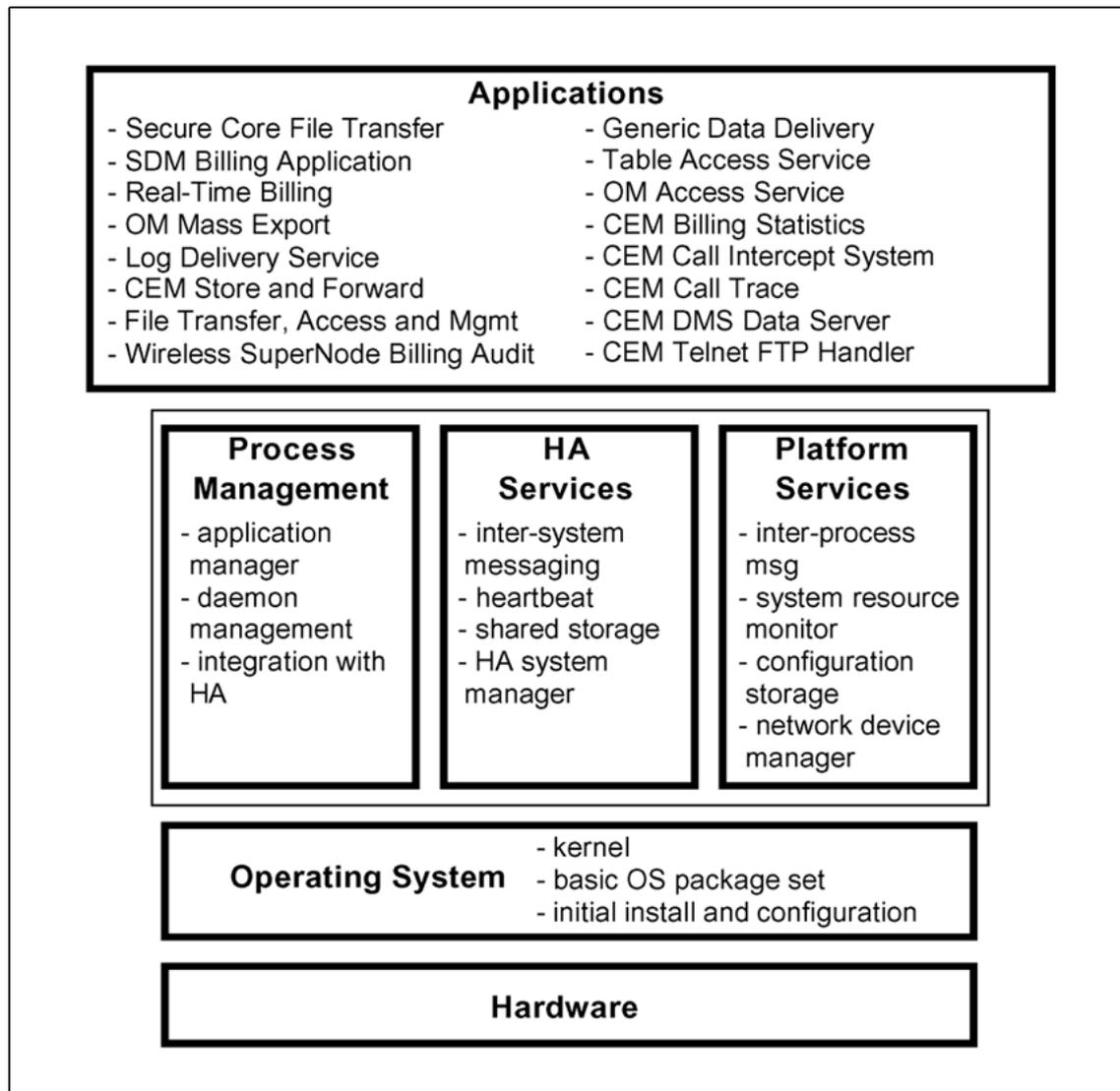
CBM 850 software architecture



CBM 850 software architecture



CBM 850 software architecture



CBM 850 applications and services

The following applications and services are supported on the CBM 850.

Terminal Access / Pass Through

The CBM 850 can be accessed through standard terminal access client software: telnet and ssh. These access methods can be individually enabled or disabled. Any ssh client that interoperates with OpenSSH 3.4 can be used.

The CBM 850, as the call server manager, provides terminal access to the core through terminal access clients running either on the CBM 850 or through the "Passthru" mechanism. Passthru users are immediately transferred to a terminal access session to the core upon login to the CBM

850. A Passthru user can be configured to require a local (CBM 850) password. Without a local password, the Passthru user is forwarded to the core login process, where the core userid and password are required.

The maximum number of simultaneous users directly logged into the CBM 850 is 64. This number is limited, however, by the computing capacity required to carry out all of the actions initiated by users who are logged in.

ATTENTION

The Terminal Access/Pass Through application is supported by CDMA only.

More complete information about the Terminal Access/Pass Through application can be found in NN-10017-111, *SDM Product Overview*.

File transfer

This application provides the ability to transfer files to and from the CBM 850, and to and from the core through the CBM 850. Since the CBM 850 platform provides ftp service and the OpenSSH software, the following methods for file transfer are available:

- ftp, which provides standard file transfer service; passwords are transferred in clear text across the network
- scp, which provides a "command line" encrypted file transfer service. This service is well suited for machine-to-machine interface.
- sftp, which provides interactive encrypted file transfer service

The CBM 850 also extends file transfer capabilities of ftp and ssh to allow a user direct access to the core file systems in order to transfer files to and from the user's client machine and the core.

File Transfer Protocol Proxy (FTPP) The FTTP application provides the ability to transfer files between the core and client machines through the CBM 850, without the need for files being stored on the CBM 850. This capability is provided through a special daemon running on the CBM 850 that is accessed by CBM pass-through users, or users who are members of the "passthru" user group. Through this application, a member of a Passthru user group will not have access to the CBM 850 file system and a CBM 850 user will not have access to the core file system.



WARNING

When the FTP Proxy is installed on the CBM 850 it disables the proftpd services provided with the SPFS platform on both the active and inactive node.

The FTP Proxy runs only on the active node.

SSH Core File Transfer (SCFT) SSHCore File Copy allows an ssh user to execute standard ftp commands on the core, through an ssh tunnel from the client machine and the CBM 850. The path from the client machine to the CBM 850 is fully ssh-secured (that is, authenticated, authorized, and encrypted). Files are transferred between the client machine and the core without the need for the files being stored on the CBM 850. The user interface is similar in form and function to the "scp" ssh command. An appropriate CBM 850 userid and password or static ssh user key setup is required, to provide the authentication and authorization information. An audit log records the operation of this application, including the identification of the user executing commands and the commands being executed.

SuperNode Billing Application (SBA)

The SBA provides a data server to collect billing records from the core, in compliance with the AMA Data Networking System (AMADNS) design described in GR-1343. Billing data retrieved from the core is stored on the two RAID-1 mirrored disks of the CBM 850. Files can then be sent from the CBM 850 to downstream systems for processing. More complete information about the SBA application can be found in *Core and Billing Manager 850 Accounting*, NN10363-811.

SuperNode Billing Application (SBA)

The SBA provides a data server to collect billing records from the Call Server. Billing data retrieved from the Call Server is stored on the two RAID-1 mirrored disks of the CBM 850 platform. Files can then be sent from the CBM 850 to the customer's downstream servers for processing. More complete information about the SBA application can be found in NN-20000-247, *Core and Billing Manager Accounting for Wireless Networks*.

SBA Real-time Billing

The Real-time Billing (RTB) application enables transfer downstream of billing data as the data is also being written to the CBM 850 disk. The downstream system can thereby process the billing records received by the CBM 850 in near real-time. This application can be used for billing streams configured to store the received billing records in DIRP file format on the CBM 850. More complete information about the SBA application can be found in *Core and Billing Manager 850 Accounting*, NN10363-811.

SBA Real-time Billing

The Real-time Billing (RTB) application enables transfer downstream of billing data as the data is also being written to the CBM 850 disk. The downstream system can thereby process the billing records received by the CBM 850 in near real-time. This application can be used for billing streams configured to store the received billing records in DIRP file format on the CBM 850. More complete information about the SBA application can be found in NN-20000-247, *Core and Billing Manager Accounting for Wireless Networks*.

SBA Automatic File Transfer

The Automatic File Transfer (AFT) application transfers billing files from the CBM 850 to a downstream system. It transfers all available billing files in chronological order using the Nortel proprietary AFT protocol, a subset of the DMS AFT protocol. More complete information about the SBA application can be found in the Accounting NTP in the CBM 850 NTP suite

ATTENTION

The SBA Automatic File Transfer (AFT) application is supported by CDMA only.

File Transfer, Access, and Management (FTAM)

The FTAM application provides the transfer of billing files using two main components: the initiator and the responder. The initiator resides on the downstream processor, and is responsible for initiating all file transfer and query requests between the downstream processor and the SBA. The responder, resides on the CBM 850, and acts upon the individual request sent to it from the initiator.

OM Delivery

The OM Delivery application transfers operational measurement data to downstream destinations. The application provides the ability to:

- group related OMs together into report elements so that they can be monitored easily
- format into comma-separated value (CSV) format
- delivered to a customer operations support system (OSS)
- select a subset of registers in an OM group
- set the report interval to five minutes or to Office Transfer period (15 or 30 minutes) for each report element
- specify when to collect OM data using data collection schedules, when to rotate the report file using report collection schedules, and when to transfer report files to a downstream system using file transfer schedules
- store OM data files on disk where they are available for regularly scheduled, automated transfer to a downstream system by way of FTP
- schedule an unattended file transfer to a maximum of 16 downstream destinations (per schedule)

ATTENTION

The OM Delivery application is supported by CDMA only.

OM Mass Export

The OM Mass Export application provides the collection, accumulation, and delivery of OM data to the customer's downstream processors. The OM Mass Export has two main functions: switch export and accumulation export. The switch export function provides OM data to the customer in the readable switch (ASCII) format. Accumulation export provides OM data to the customer in tab-delimited format.

Log Delivery Service

The log delivery system collects core logs and CBM 850 logs, formats them in either Nortel-standard or SCC2 format, and routes them to remote hosts printers and to UNIX files. The Log Delivery Service provides high-speed log delivery, using TCP/IP protocol to transfer logs from the CBM 850 to the OSS. The applications supporting Log Delivery Service allow flexible configuration options such as log filtering.

Passport Log Streamer

Alarms generated on Passports are received by the MDM and are then sent to the CBM 850. The Passport Log Streamer application parses the data received from the MDM and feeds this data into the customer syslog. The logs can then be retrieved through the Log Delivery Service application.

ATTENTION

The Passport Log Streamer application is supported by CDMA only.

Log Consolidation

Non-core network element managers running on the SSPFS platform generate logs into their local log systems. These local log systems are configured to forward the logs to the CBM 850. Log Consolidation aggregates these additional logs received from the managers into the SCC2/Nortel Standard log streams.

GR740 Pass Through

The GR740 Pass Through application enables the CBM 850 to both receive GR740-compliant messages from and send GR740-compliant messages to a network data collection operations system (NDC OS) on the operating company's LAN/WAN. The messages are transferred over a TCP/IP link, in accordance with the Telcordia specification GR-740.

The CBM 850 version of GR740 Pass Through can be configured in SSH mode (secure mode) or standard mode. SSH secured tunnels are used to secure the communication from the OSS to the core through the CBM 850. The tunnels are initiated from the OSS and require local CBM authentication.

Reach Through SPM

The Reach Through SPM 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 application provides transport network access to the SPM through the CBM 850. A customer Network Element uses Transaction Language 1 (TL1) to retrieve OC-3 performance parameter information from the SPM.

ATTENTION

The Reach Through SPM application is supported by CDMA only.

DMS Maintenance

The DMS Maintenance application (DMA) is used for communicating trunk and line maintenance messages to the computing module (CM) through the core manager maintenance interface. The DMA translates the Operation Support System Data Interface (OSSDI) trunk and line maintenance messages into a format that the core manager maintenance interface understands and can forward to the CM.

Core Element Manager (CEM) Store-and-Forward (SAF)

processes The CEM server is an element manager for the DMS node, providing fault, performance, and configuration management toolsets. The server works in conjunction with the CEM browser, which is accessed through the Integrated Element Management System (IEMS).

Three CEM client applications run on the CBM 850 to provide the CEM server with access to core OAM&P data. These applications include:

- CEM Data server
- CEM Telnet Ftp Handler
- CEM Store and Forward

CEM Data Server The CEM Data Server service provides a conduit between the Call Server (core) and the CEM server for performance and configuration information. This service depends on the base Table Access and OM Access services. The CEM Data Server forwards operational measurements (OM) and configuration data to the performance manager or configuration manager in the CEM server, respectively.

CEM Telnet Ftp Handler This service provides the pass-through capability for the Call Server (core) terminal access and file transfer components of the CEM server/browser. This allows terminal access and file transfers to the Communications Server (core) to be initiated within the CEM server/browser.

CEM Store and Forward The Store and Forward (SAF) processes are responsible for storing and forwarding operational measurements (OM) and logs from the SDM/CBM to the CEM server. This service provides the upstream interface to the CEM server and additional reliability by storing data to handle disruption in communications between the SDM/CBM and the CEM server.

Core Element Manager (CEM) Store-and-Forward (SAF)

processes The CEM server is an element manager for the DMS node, providing fault, performance, and configuration management toolsets. The server works in conjunction with the CEM browser, which is accessed through the Integrated Element Management System (IEMS).

Three CEM client applications run on the CBM 850 to provide the CEM server with access to core OAM&P data. These applications include:

- CEM Data server
- CEM Telnet Ftp Handler
- CEM Store and Forward

CEM Data Server The CEM Data Server service provides a conduit between the Call Server (core) and the CEM server for performance and configuration information. This service depends on the base Table Access and OM Access services. The CEM Data Server forwards operational measurements (OM) and configuration data to the performance manager or configuration manager in the CEM server, respectively.

CEM Telnet Ftp Handler This service provides the pass-through capability for the Call Server (core) terminal access and file transfer components of the CEM server/browser. This allows terminal access and file transfers to the Communications Server (core) to be initiated within the CEM server/browser.

CEM Store and Forward The Store and Forward (SAF) processes are responsible for storing and forwarding operational measurements (OM) and logs from the SDM/CBM to the CEM server. This service provides the upstream interface to the CEM server and additional reliability by storing data to handle disruption in communications between the SDM/CBM and the CEM server.

SSPFS services

The CBM 850 shares with other tools built on top of SSPFS a common platform of hardware, operating system, and third party services and tools. SSPFS provides the services for managing the hardware and system health.

Through SSPFS, the CBM 850 provides services such as booting, load imaging, and Network Time Protocol for other Carrier Voice over IP network elements, and provides interfaces into core data for higher-level applications.

Bootp/TFTP/NFS

The CBM 850 serves as a load server for other Carrier Voice over IP nodes. The SSPFS services, Bootp, TFTP, and/or NFS are used by Carrier Voice over IP nodes, such as the Gateway Controller and MG9K, to put loads and images on the CBM 850 and to retrieve loads and images from the CBM 850.

Bootp/TFTP/NFS

The CBM 850 serves as a load server for other Succession nodes. The SSPFS services, Bootp, TFTP, and/or NFS are used by Succession nodes, such as the Gateway Controller and MG9K, to put loads and images on the CBM 850 and to retrieve loads and images from the CBM 850.

ATTENTION

The Bootp/TFTP/NFS services are supported in the CDMA Packet network only.

Network Time Protocol

A Network Time Protocol daemon included in the SSPFS provides a mechanism for synchronizing the CBM 850 time-of-day to one or more external sources (NTP servers). The health of this daemon and the precision of the time-of-day on the CBM 850 is monitored. Alarms are raised and logs are generated when the time-of-day accuracy or the availability of servers is compromised.

CBM 850 maintenance

Maintenance user interfaces

CBM 850 administration and maintenance is performed through a local interface called the "CBM 850 maintenance interface (cbmmtc)." This interface provides:

- a hierarchical set of screens or levels
- a dynamic alarm banner with state nomenclature that reports overall CBM 850 state, application states, core connectivity status, NTP health status, platform (hardware) status, system resources status, and file system resources status and health
- context-sensitive fault reporting and help
- administration functions such as user pass-through functionality, terminal access configuration, and software installation and maintenance

The status of the CBM 850 and of its components is available also through command line query commands.

Logs

CBM 850 applications and services generate customer logs, which are written to persistent storage in a simple text file. SSPFS logs identifying platform issues are also generated on the CBM 850. Core logs are also generated for state changes.

Visual hardware indicators

The general product state of the CBM 850 is also reflected in the server LEDs for critical, major, and minor alarms, as well as through the office alarm unit of the frame in which the CBM 850 is installed.

Geographical survivability

The CBM 850 physical architecture allows support for geographical survivability. Since the physical storage on each redundant server is completely, and continually, copied to the other server using high availability network replication software, the two servers can be physically separated by great distances.

The IP addresses and default gateway for each server must remain in the same subnet in the distributed configuration. This is accomplished by connecting the point-to-point inter-server connections through a WAN (optical network) specially engineered for this purpose.

Geographical survivability is accomplished through a coordinated effort and cooperation of all the elements in an office. The CBM supports geographical survivability as part of the larger solution where all elements are split across two physical locations.

CBM 850 upgrades and patching

Software upgrades for the CBM 850 are delivered in the form of software packages and software patches:

- Software packages are delivered by way of the electronic software delivery (ESD) method through a high-speed internet connection. The packages can be deposited either on an intermediary machine or directly onto the node when access to the node is available.
- Software patches are applied and managed through the Network Patch Manager (NPM). The NPM is packaged with SSPFS. The NPM is equipped to manage patches both manually through a command line interface or graphical user interface (GUI) and through scheduled automatic application. Any patching failures raise alarms within the NPM. The NPM treats the servers in a CBM 850 cluster individually as a separate devices and ensures that only one device is restarted at a time.

Upgrading the CBM 850 with a new software release involves upgrading both the SSPFS platform and software, and upgrading the CBM 850 software. The SSPFS upgrade consists of two processes; upgrading the Solaris operating system and upgrading the SSPFS software. The CBM upgrade also consists of two processes: preparing the CBM upgrade media and applying and patching the new CBM software. The CBM upgrade is automatically initiated during the SSPFS upgrade.

CBM 850 emergency access

The console port is a standard RS-232 port with an RJ-45 connector.

Use an RJ-45 cable and adaptor to connect to a dumb terminal or laptop. Connection to the Sun N240 is established using a RJ-45 serial cable and a RJ-45-DB9 adapter. Connect one end of the RJ-45 serial cable to the N240 Serial MGT port (located on the rear of the Netra). Connect the other end to the adapter and then to the client PC/FT laptop.

Use the Sun Part 530-2889 SunBox Serial Adapter (RJ-45 to dB25) for modem connection, if provided.

CBM 850 security

Since the CBM 850 acts as a gateway and firewall for the CS 2000, and because it hosts accounting records and call-related personal information from CS 2000 subscribers, maintaining system security is of critical importance. The following are some of the basic characteristics of the security framework provided by the CBM 850:

- The Solaris operating system of the CBM 850 has been hardened by following Unix good practices and by the removal from the initial system configuration of most unnecessary services that could provide exploitable back doors to the system.
- The CBM 850 protects network traffic using SSH protocol. This service is available for most applications either through SSH terminal access, SFTP inbound or outbound file transfer, or SSH port forwarding. The CBM 850 also supports IPsec protocol.

For the SBA and OMDD applications on the SDM/CBM that use OpenSSH SFTP to perform secure outbound file transfers, the user can select either password-based authentication, or key-based (public key) authentication.

- CBM 850 users are authenticated through the Integrated element Management System (IEMS).
- The CBM 850 restricts the commands and files that a user can access, based on the role of the user.

- The CBM 850 generates security and audit logs for certain critical operations. Security and audit logs are stored in permanent storage, and can also be routed to external systems that host a syslog server.

CBM 850 to SDM comparison

The following table outlines the major differences between the SDM and the CBM.

SDM to CBM 850 comparison

	CBM	SDM
Hardware		
OEM supplier	Sun Netra 240	Motorola Fault-Tolerant Hardware
Footprint	two 2U servers for CBM 850/860	Space for E28 cabinet
CPU	two Ultra SPARC IIII at 1.28 GHz (loadsharing and redundant)	400 MHz Arthur processor
Memory	4 Gbytes	512 Mbytes
Removable media	DVD-RW drive	DAT
Physical storage	two internal 73-Gbyte or one internal 146-Gbyte, 15K RPM hot-swappable disks—RAID mirrored (four copies of data on CBM850)	Up to 72 Gbytes of redundant data plus separate disks for program store
Power supplies	two redundant hot-swappable power supplies	two redundant hot-swappable power supplies
Interfaces/connectivity		
OSS interfaces	four 10/100/1000-Mbps BaseT Ethernet ports for CBM 850	two 100/10 Ethernet interfaces
Core connectivity	CBM 850 - two GigE interfaces (10/100/1000 auto sensing) (shares OSS ports)	DS512
Console port	The console port is a standard RS-232 with an RJ-45.	The console port is a standard RS-232 with an RJ-45.
Frames	COAM cabinet and MISC frame	E28 cabinet
Maintenance		
Audio alarms	Available on office alarm unit	Available on office alarm unit
Visual alarms	No MAP visibility on CBM 850	MAP and LED
Electronic Software Delivery	Available	Available
Patching	Scheduled automatic patching (includes auto reboot/SWACT)	Scheduled automatic patching

	CBM	SDM
MAP maintenance evolution		
Maintenance interface	CBM 850 uses local maintenance interface	Core CI is principal SDM maintenance interface
MAPCI presence	No MAPCI presence for XA-Core	MAPCI presence
Control from Core	CBM 850 is standalone, not controlled from Core	SDM node and link (DS512) tightly integrated and controlled from Core
OAM interface	CBM 850 is EMS of Core	SDM is peripheral of Core
Log/alarm reports	CBM alarms and logs are reported locally and not to the Core. SDM report name is maintained for CBM for back-office compatibility.	Logs and alarms sent from the SDM to the Core and reported at the Core.
SDMRLOGIN	SDMRLOGIN is not available for access to the CBM from the Core	SDMRLOGIN can be used to access the SDM from the Core
Upgrades		
Upgrade time (best case - 5 Gbytes data)	3.5 hrs or more (with OS upgrade)	3–5 hrs
Time in Billing Backup (including SBA Upgrade)	< 5 min	60–90 min
Core inaccessibility time via SDM/CBM	0 sec	60–90 min
Other applications outage (worst case)	< 5 min Data reformat will have impact	2–3 hrs
Additional loss or redundancy	60 min during active side clone (estimated)	N/A
Automatic fallback capability	No	May require S-tape restore
Upgrade success rate	Extremely high (expected)	97%
Complete upgrade within maintenance window (4 hr)	Comfortable if you use three windows	Requires full maintenance window

	CBM	SDM
Complexity (number of steps and potential for operator error)	Low (improvements)	Medium
Vulnerability to hardware failures	Very low	Medium

CBM 850 implementation sequence

The following sequence provides the activities required for the complete implementation of the CBM 850, from hardware installation to final cutover.

CBM implementation sequence

	Activity	Reference
1	Order IPs	CIQ
2	Physical install of CBM hardware	This activity is performed by Nortel personnel.
3	Upgrade Core to latest release; upgrade software on SDM to latest release	NTP 411-2131-371, <i>SDMX Deployment Guide</i> , for CDMA or NTP 411-8111-233, <i>GSM/UMTS Voice Core Network OAM Upgrades</i> , for GSM/UMTS
4	Install NTLX17AA (HCMIC)	This activity is performed by Nortel personnel.
5	Bring NTLX17AA on line	This activity is performed by Nortel personnel.
6	Decommission RTIF/CMIC packets	This activity is performed by Nortel personnel.
7	Datafill core to assign local IP address for HCMIC	This activity is performed by Nortel personnel.
8	Physical connection of CBM to NTLX17AA via network	This activity is performed by Nortel personnel.
9	Install SSPFS software, if needed	This activity is performed by Nortel personnel.
10	Install UCBM software	This activity is performed by Nortel personnel.
12	Install applicable patches on CBM and/or DMS-MTX	This activity is performed by Nortel personnel.
13	Activate Transition Mode Billing (TMB)	NTP NN-20000-243, <i>Wireless Transition Mode Billing Guide</i>

	Activity	Reference
14	Verify billing from the CBM	NTP NN-20000-243, Wireless Transition Mode Billing Guide
15	Reconfigure Succession products to accommodate CBM	This activity is performed by Nortel personnel.
16	SDM to CBM cutover	NTP NN-20000-243, Wireless Transition Mode Billing Guide
17	Physical uninstall of SDM	This activity is performed by Nortel personnel.

Carrier VoIP

Core and Billing Manager 850 Basics

Copyright © 2006, Nortel Networks
All Rights Reserved.

Publication: NN10355-111
Document status: Standard
Document version: 04.04
Document date: 20 October 2006

To provide feedback or report a problem in this document , go to <http://www.nortel.com/documentfeedback>

The information in this document is sourced in Canada, the United States of America, and the United Kingdom.

The information contained herein is the property of Nortel Networks and is strictly confidential. Except as expressly authorized in writing by Nortel Networks, the holder shall keep all information contained herein confidential, shall disclose it only to its employees with a need to know, and shall protect it, in whole or in part, from disclosure and dissemination to third parties with the same degree of care it uses to protect its own confidential information, but with no less than reasonable care. Except as expressly authorized in writing by Nortel Networks, the holder is granted no rights to use the information contained herein.

This is the Way, This is Nortel, Nortel, the Nortel logo, the globemark design, and the NORTEL NETWORKS corporate logo, are trademarks of Nortel Networks. All other trademarks are the property of their respective owners. All rights reserved.

