Core and Billing Manager 850 Basics

What's new in Core and Billing Manager 850 Basics for (I)SN09

Feature changes

There are no feature changes in this release.

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.

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.

Network connectivity

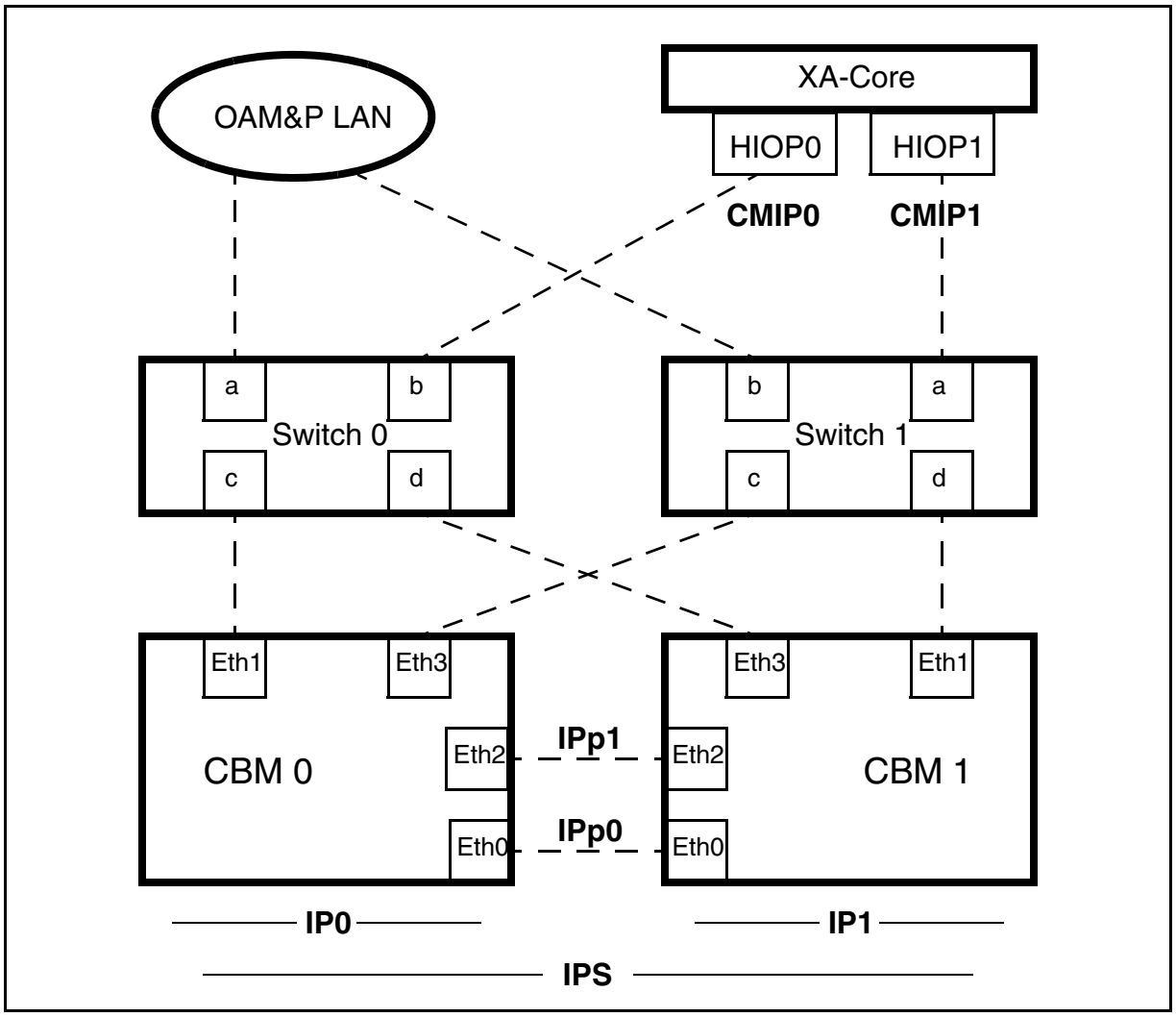
Each of the two CBM 850 servers in a cluster is equipped with four Ethernet ports (GigE interfaces, 10/100/1000 auto sensing). Two Ethernet ports on each CBM 850 are directly connected to the mate CBM 850 in the cluster for HA reliability and data replication, creating a redundant, local interconnect 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.

Note: 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



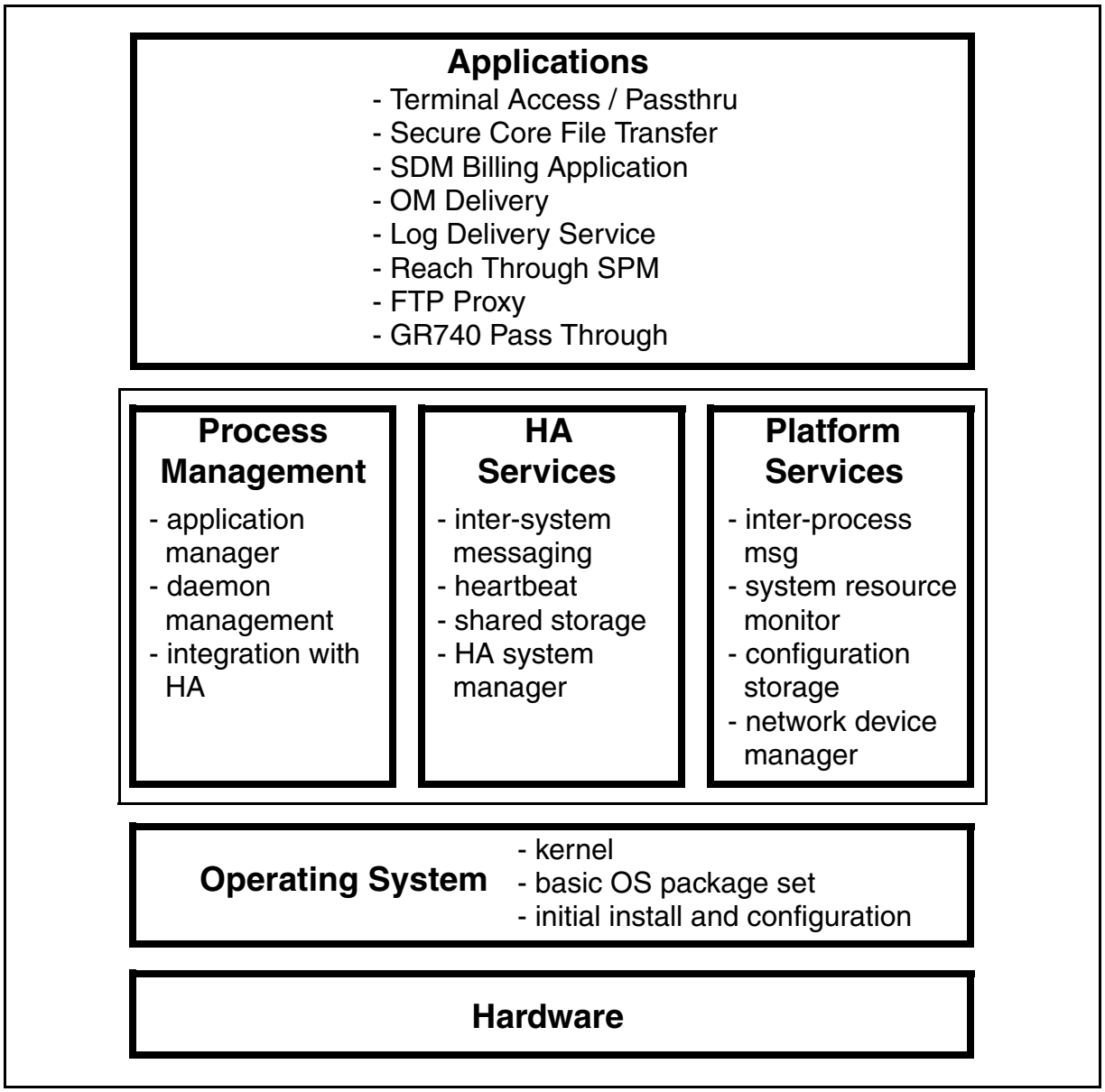
CBM 850 software

The CBM 850 software is built on top of the Carrier Voice over IP Server Platform Foundation Software (SPFS), which includes the operating system and several software components, tools, and utilities used for managing system equipment and software. SPFS 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 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.

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 FTPP 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.

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.

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 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.

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
- 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)

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.

Nortel Multiservice Switch Log Streamer

Alarms generated on a Nortel Mulitservice Switch are received by the MDM and are then sent to the CBM 850. The Nortel Multiservice Switch 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.

Log Consolidation

Non-core network element managers running on the SPFS 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.

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 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.

SPFS services

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

Through SPFS, 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 SPFS 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.

Network Time Protocol

A Network Time Protocol daemon included in the SPFS 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. SPFS 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 SPFS. 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 SPFS platform and software, and upgrading the CBM 850 software. The SPFS upgrade consists of two processes; upgrading the Solaris operating system and upgrading the SPFS 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 SPFS upgrade.

CBM 850 emergency access

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

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.

- CBM 850 users are authenticated through the 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.