Copyright © 2005, Nortel Networks

Policy Controller basics

What's new in the (i)SN09 release?

Virtual Private Network (VPN) functionality has been added to the Nortel Policy Controller for (I)SN09.

Policy Controller customer documentation

The Policy Controller customer documentation suite consists of the following NTPs:

- Policy Controller Basics, NN10427-111
- Policy Controller Configuration Management, NN10432-511
- Policy Controller Fault Management, NN10438-911
- Policy Controller Performance Management, NN10439-711
- Policy Controller Security and Administration, NN10434-611
- Upgrading the Policy Controller, NN10431-461

Overview

The Policy Controller monitors, controls, and enforces use of network resources. It allows for general application maintenance and network topology provisioning. The management function provides tools and interfaces to monitor network resource usage, and defines the relationship between subscriber needs and network resource availability.

The Policy Controller main functions are policy control and management. The primary policy control functions of the Policy Controller are Bandwidth Management and Call Admission Control.

The Policy Controller software application resides on the Service Application Module – eXtremely Thin Server (SAM-XTS) hardware platform and the product is developed and based on the Nortel General-purpose Session Server (NGSS) software platform. The Policy Controller is deployed as two redundant hardware units housed in the SAM-F frame or SAM-CCF frame.

The customer can perform Operations, Administration, Management, and Provisioning (OAM&P) from the Policy Controller Web GUI.

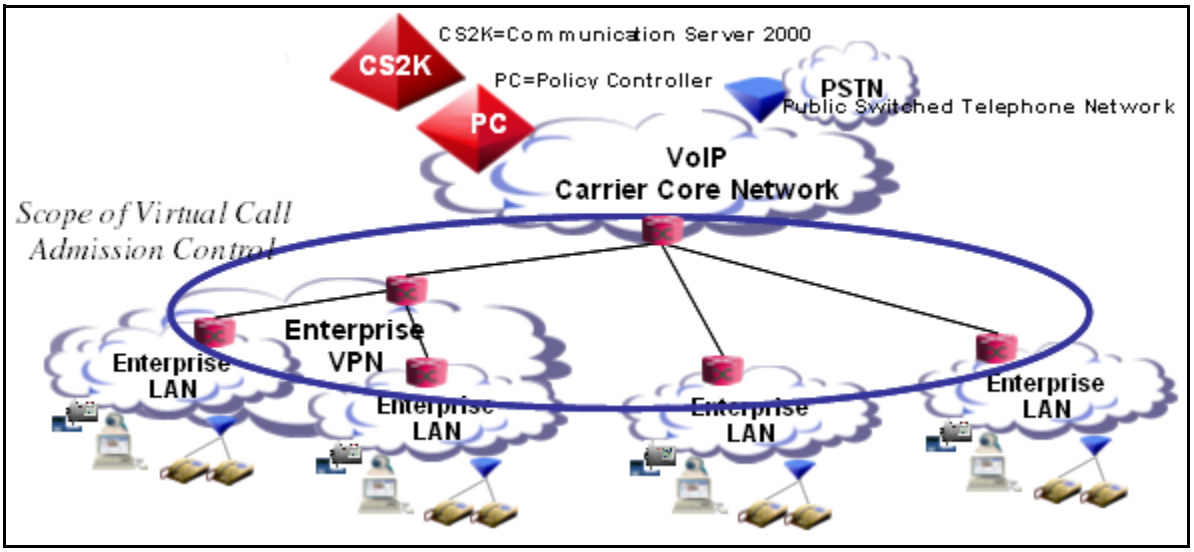
Supported Carrier VoIP solutions

The Policy Controller supports the following Carrier VoIP solutions:

- Carrier Hosted Services (CHS) for North America and International
- Integrated Access Wireline (IAW) for International

The following diagram shows the Policy Controller in a Carrier Hosted Services (CHS) Solution.

Policy Controller in a Carrier Hosted Services (CHS) solution



Policy Control Framework

The Policy Controller has a Policy Control Framework (PCF) that is responsible for processing requests for resources and applying the necessary policy enforcement mechanisms to the requests. All relevant network topology information is retrieved from a Topology Database.

Policy definition

The only policy supported is the Virtual Call Admissions Control (VCAC) Bandwidth Policy. This default policy carries out network resource reservation functions.

Policy enforcement

The Policy Controller applies the default policy to all requests for network resources to enforce call admission control. Resource requests are for flow specifications or an amount of bandwidth requested. VCAC bandwidth usage calculations are used to monitor

the bandwidth usage status and ensure there are enough resources for a new call requests.

When an application server agrees to provide service to a client, it sends a request to the Policy Controller that contains the following information:

- Client identity and location
- FlowSpec specifying traffic requirement for the session

Virtual Call Admissions Control (VCAC)
VCAC is a quality of service (QoS) mechanism that allows the Communication Server 2000 to cancel post-dial, pre-ringing calls that would overload a segment of the packet network.

The Policy Controller is responsible for Virtual Call Admissions Control (VCAC) call/bandwidth so that it can be shared between multiple call agents, applications servers, softswitches, all of which can control VoIP endpoints in the same sites.

VCAC prevents a call from being setup if the media resources required for the call exceed the defined capacity of a limited bandwidth link or set of links associated with the call. If call setup is prevented, the user will receive an appropriate call treatment.

VCAC depends on a logical model of the packet network, starting with the service provider's core packet network and points of bandwidth concentration. These concentration points can occur at customer enterprises comprised of a collection of sites, or at a regional broadband aggregation point. These sites are connected by a mix of limited bandwidth links (LBLs) and network address translators (NATS). The VoIP gateways and the lines are located within the different sites in each enterprise.

VCAC is virtual because it does not require interaction with real network elements. It models network elements and tracks the amount of bandwidth consumed by the application flows. When the model indicates that bandwidth is fully utilized and any additional flows would exceed link capacities, no additional flows are authorized.

The VCAC function tracks bandwidth usage as an Explicit or Implicit calculation of encapsulation overhead and link bandwidth. The mechanism depends on the definition of a network zone and associated network link. The Policy Controller topology model allows the customer to either describe a network link by established predefined protocol layers or by a custom link layer type.

Implicit calculation: You can choose to describe a network link as protocol layers (e.g. PPP/Ethernet/ATM) that make up the link. These link layer types are predefined for use by you and are accessible through the Policy Controller provisioning interface. A protocol layer is specified as having either a variable (for example, Ethernet) or fixed (for example, ATM) protocol data unit (PDU). In each case there is an encapsulation overhead, and in the fixed PDU case there is also the unit size & overhead. The Policy Controller implicitly derives the value of the link overhead based on the definition of the predefined link layer type because the encapsulation overhead is associated with the protocol. For example, in the case of a fixed length PDU, you would also specify the unit size (e.g. ATM cellsize=53) and unit overhead amount (e.g. ATM header of 5 bytes).

Explicit calculations: In a simpler approach, you can choose not to model the specific protocol layers of the network link, but instead create a custom link layer and provision the bandwidth available on the link with a single value for the overhead. In this calculation, no assumption is made about multiple link layers and the associated encapsulation overhead of each. It is expected that the operating company personnel explicitly accounts for any overhead required for the link layer. The overall bandwidth is explicitly calculated based on the bandwidth values and overhead provisioned by the customer

Nortel has an established set of subscriber service classes that can be used to map traffic categories, DSCP, and other QoS/CoS parameter designations. Network Service Class (NSC) names can be used to define individual traffic flow policies based on traffic conditions independently of the underlying bearer link protocol or network element resource. This can provide scalability for large networks that interoperate with various policy standards, including: DiffServ, IEEE 802.1p, COPS-PR, and LDAP.

Only voice calls are supported from the CS2000. All voice calls are tagged as Premium.

Nortel components

The Nortel Integrated Element Management System (IEMS) provides proxy connections for Policy Controller OAM functions. The Policy Controller provisioning web client can be launched from IEMS. A secure shell (SSH) connection to the Policy Controller from IEMS is required for OSS operations. The OSS operator position can log into the Policy Controller through IEMS secure proxy and SSH.

IEMS can be used as a:

- web proxy for Policy Controller OAM operations via Web GUI.
- secure proxy for Policy Controller logon.
- secure proxy for Policy Controller OAM operations via OSS.

Refer to the IEMS NTPs for information on how to configure IEMS interfaces for web server proxy and secure proxy for OSS.

Policy Controller hardware platform

The Policy Controller units are deployed in a rack-mounted configuration that houses processing hardware, hard drives, ethernet interface ports (two currently reserved for inter-Policy Controller communication for fault tolerance), and redundant power supplies. This hardware platform uses Network Equipment Building Standards (NEBS) Level 3 compliant hardware designed for telecommunications central offices or data centers, based on the Hewlett Packard™ cc3310 carrier-grade server. With two chassis working together to provide carrier-grade level fault tolerance, this hardware configuration provides the platform for the Policy Controller application.

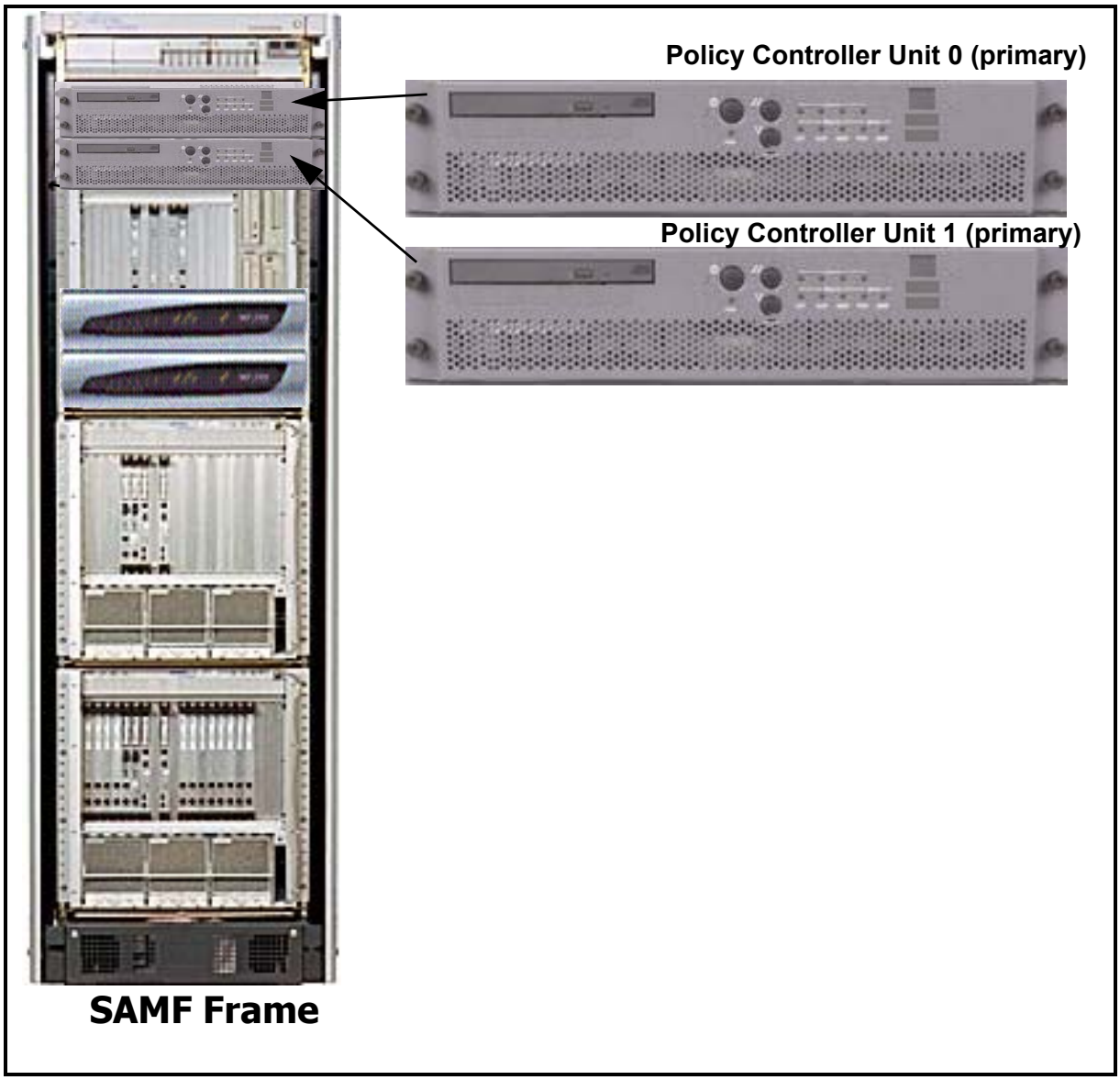
Features of each hardware platform unit include:

- Dual 2.4GHz Xeon Processors
- 4GB DDR Memory
- Dual 73GB Hot Swappable Disk Drives
- CD-RW/DVD-R Drive
- Dual Hot Swappable Power Supplies
- Dual GigE Interface network interface cards
- Service Application Module – eXtremely Thin Server (SAM-XTS) Platform is based on the compact HP cc3310 carrier-grade server.

The following figure shows one Policy Controller node (two units in total) positioned in a SAMF frame (NTRX51HA).

Typically, each Policy Controller unit is labeled for identification to distinguish it from other units in the frame, and to distinguish it from STORM units. The naming identification can be similar to the hostname of the node, made during commissioning of the node.

Policy Controller units in the SAMF frame(NTRX51HA)



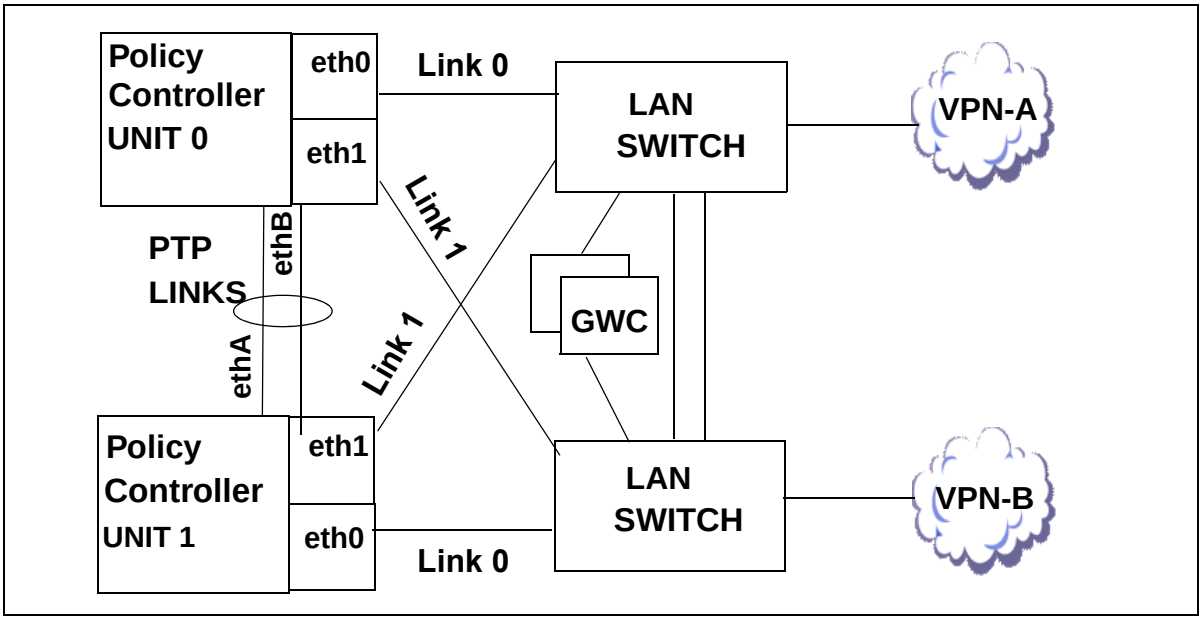
Network interfaces and connectivity

Each Policy Controller unit has two GigE ethernet interfaces, configured as link 0 and link 1, to communicate with CS-LAN switch. In addition, two additional ethernet interfaces interconnect the two hardware units in a Point To Point (PTP) link.

This configuration allows the Policy Controller to operate like the Gateway Controller in that it supports maintaining active calls over a Warm Switch of Activity (SWACT) from an active to a standby unit. SWACTs can be manually executed or may automatically execute when callp auditing processes determine that there is sufficient cause to SWACT units.

For more detailed information about managing ethernet links for the Policy Controller, refer to the Policy Controller Security and Administration NTP, NN10434-611.

Link Configuration of the Policy Controller with the CS-LAN



Software architecture

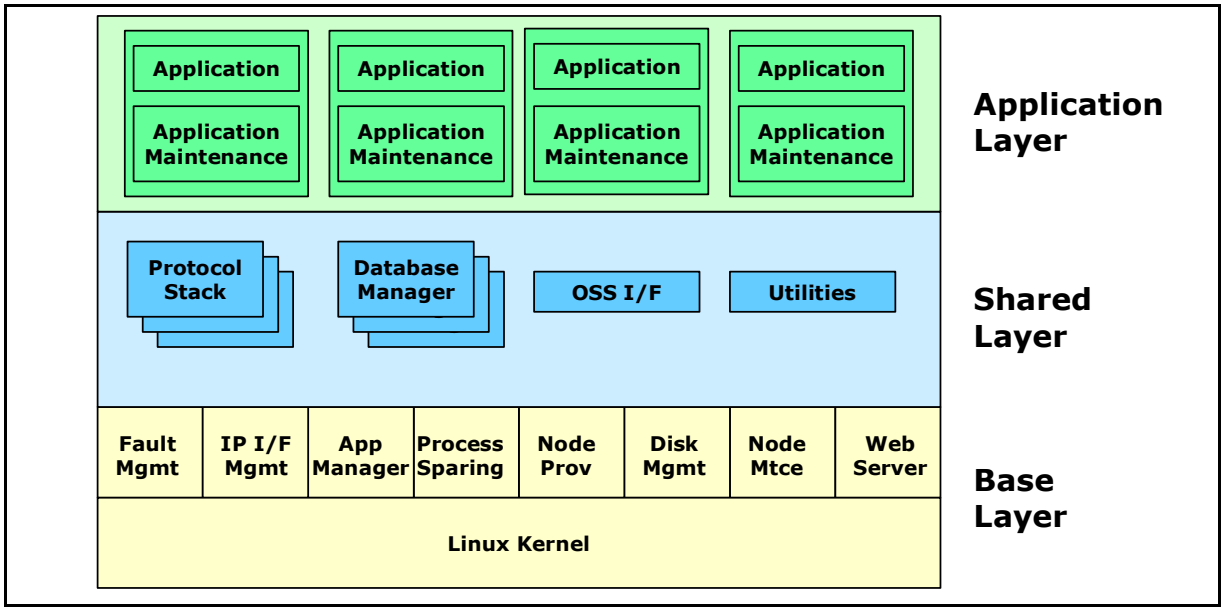
The Policy Controller is developed on the NGSS (Nortel General-purpose Session Server) software platform. The NGSS software platform has a layered architecture, which consists of an application layer, a shared layer, and a Nortel Carrier-Grade Linux base layer. The Policy Controller software resides in the NGSS application layer, and the Session Policy Controller uses the NGSS Application Maintenance Module to interface with the NGSS shared and base layer

functions. The NGSS platform does not support multiple applications. Only one application can be enabled to operate on the platform.

The Policy Controller software layered architecture:

- The base NCGL (Nortel Carrier Grade Linux) layer including the Linux kernel and a carrier-grade software platform that supports fault management, interface management, hardware management and application management
- A shared application layer containing reusable components, such as the Database Manager, that are used by higher level applications such as the Policy Controller application.
- An application layer, which includes a maintenance process for each application which in turn manages the associated application processes, in this case the Policy Controller application processes.

Policy Controller software architecture



Policy Controller application software

The Policy Controller application is responsible for call processing activities. The application runs on the NGCL platform and communicates indirectly with the CS2000 through GWCs.

Client web browser requirements

For provisioning and maintaining the Policy Controller the following client web browsers are supported:

Supported web clients on a Windows 2000, XP, or 2003-based PC:

- Internet Explorer 6.0 SP1and above
- Netscape 6.2.3 and 7.1+

Supported web clients on a Solaris 2.8 and 2.9-based Sun workstations:

- Netscape 6.2.3

For more information about supported Web browsers, refer to the Policy Controller Configuration Management NTP, NN10432-511.

Software ordering and delivery

Refer to the Basics NTP applicable to your Carrier VoIP solution, for more information about software ordering and support options.

Policy Controller software loads

The Policy Controller uses a single load for North America and International markets and all supported IP solutions.

Maintenance release upgrades and patching

The first release of the Policy Controller was SN08. Patching and in-service maintenance release upgrades are supported for the Policy Controller. Consult NTP *Upgrading the Policy Controller*, NN10431-461, for more information.

Upgrading a CS2000 network to support Policy Controller

Upgrading a CS 2000 network-based office to include the Policy Controller is not covered in the Policy Controller NTPs. For initial installation and provisioning of a Policy Controller into an existing network, consult your Nortel service representative and refer to the Policy Controller Installation and Commissioning Installation Method, IM 35-0493.

Operations, administration, maintenance and provisioning

The Policy Controller is a component in the CS 2000 network and it uses operations, administration, maintenance and provisioning (OAM&P) functions for handling fault, configuration, accounting, performance and security (FCAPS) management activities.

The Policy Controller functions as its own element manager. This means that provisioning and maintenance activities for a Policy Controller takes place on the Policy Controller itself. The Policy Controller provision framework provides a web based interface to configure Policy Controller system parameters, provision network topology, perform application mantanence, and display Policy Controller specific OMs, alarms, and logs. An OSS interface is also provided.

The Policy Controller uses a database for persistent data storage of topology data and run-time configuration parameters. There are many components in the Policy Controller that access the database to retrieve, insert, or update data. For example, the Policy Controller Framework (PCF) retrieves topology from the database to construct the topology in the memory and Topology data needs to be input from the OSS into the database. Topology data and system tunable parameters can be changed by system operator or externally while the Policy Controller is running and the internal components of the Policy Controller must be notified of the change. An internal change notification mechanism is used to notify the internal components of the Policy Controller what information has been changed.

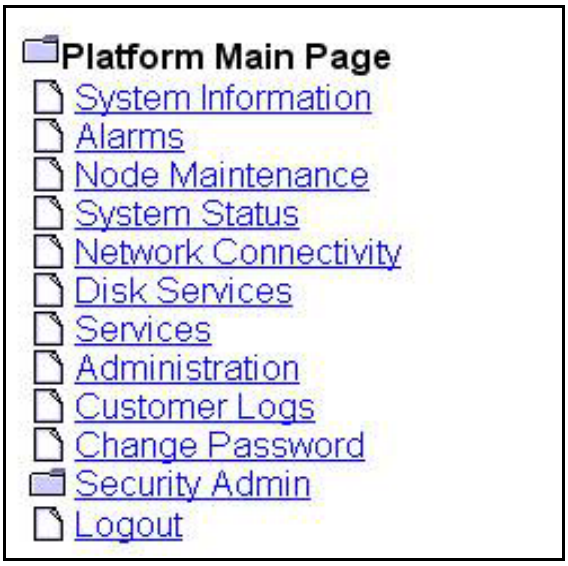
The OSS and web browser are the only interfaces to manage provisioned data. The OMs, Logs, and Alarm information are recorded on the internal hard disk. These subsystems provide an interface to export the data off-board to IEMS. The Web Server can also retrieve active alarms and logs so that they can be displayed on the Web GUI.

Tools, utilities and user interfaces

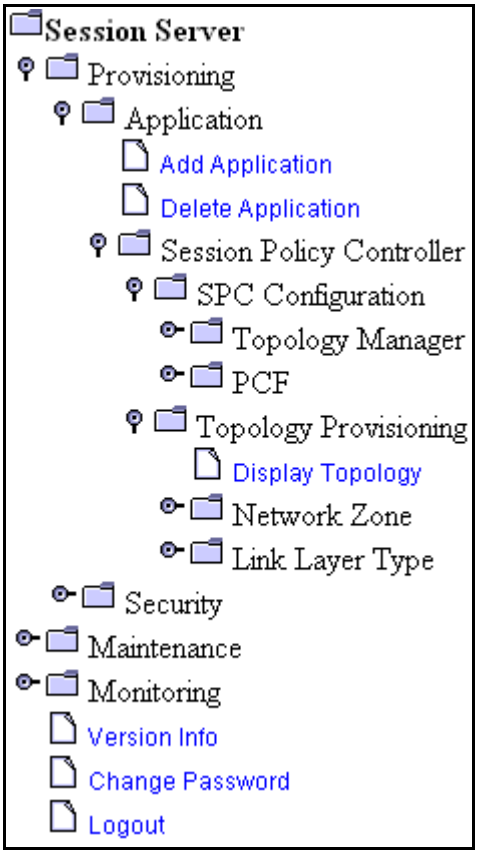
All OAM&P activity on the Policy Controller is performed using one or more of the following user interface tools, accessed through the Integrated EMS system:

- The Policy Controller Manager GUI, a client web browser application
- The CS 2000 NCGL Platform Manager GUI, a client web browser application
- The NCGL command line interface (CLI)

The CS 2000 NCGL Manager GUI main menu used for platform OAM&P



The Policy Controller Manager GUI main menu used for application OAM&P



Accessing Policy Controller GUIs and CLIs

The Policy Controller user interfaces can be configured for access through the Integrated Element Manager System (IEMS). They can also be configured without the Integrated EMS because the Policy Controller uses its own element manager interface. This means that provisioning for a Policy Controller takes place directly on the Policy Controller node itself. This is possible because Policy Controller uses a web-based interface that consists of a web server, running on both Policy Controller units, providing web pages for performing OAM&P activities.

There are three primary methods for accessing Policy Controller user interfaces:

- All GUI and CLI interfaces to the Policy Controller can be accessed by selecting and right-clicking on the active Policy Controller element from the Integrated EMS expanded Network Elements view, as shown in Access the Policy Controller GUI or CLI from the IEMS on page 13.

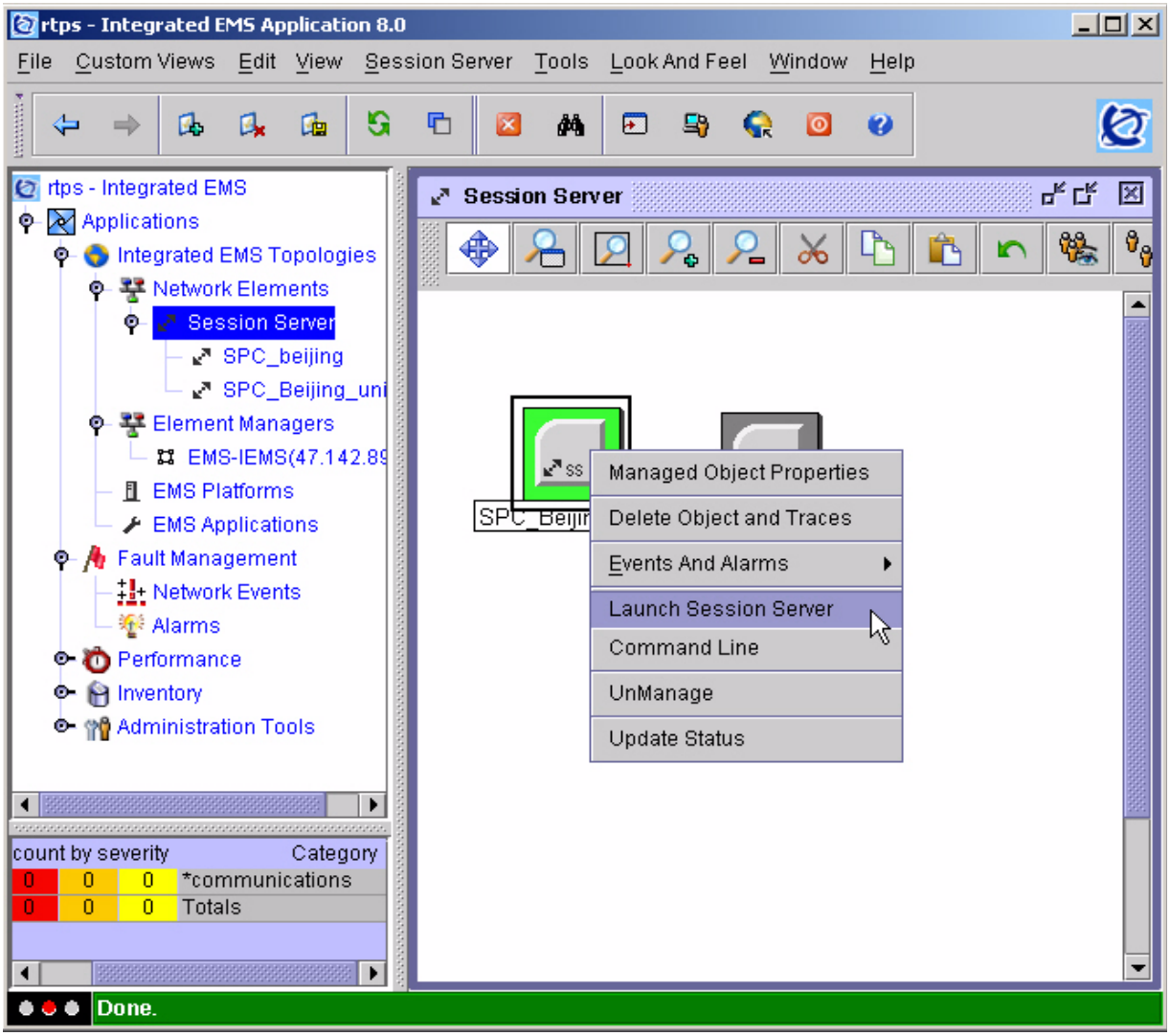
  For more information, refer to procedure *Access the CS 2000 Policy Controller GUIs from the Integrated EMS*, found in the Policy Controller Security and Administration NTP, NN10434-611. For more information about using the Integrated EMS service, refer to the Integrated EMS Basics NTP, NN10329-111.

- All GUI interfaces to the Policy Controller can be accessed from a remote system known to the proxy server (running on CS 2000 Management Tools server) on the CS-LAN.

- The CLI interface can be accessed through a secure shell (SSH) connection from a remote client to the Policy Controller by way of SSH/telnet access through the SSPFS server.

For commissioning purposes, the CLI can also be accessed using a console connected to the rear of the Policy Controller active unit.

Access the Policy Controller GUI or CLI from the IEMS



Configuration management

Nortel installation personnel, or its contracted agents, initially install and commission the Policy Controller. The customer can then configure, manage, and provision the Policy Controller with the help of the procedures documented in the Policy Controller Configuration Management NTP, NN10432-511.

Fault management

Alarm and Logging capabilities span the Policy Controller application and NGSS software platform. The Policy Controller derives its Alarm

and Logging functionality from the NGSS software platform and a majority of these key functions are provided by the capabilities of the underlying NGSS platform. Refer to the Policy Controller and NGSS Fault Management NTPs for more detail concerning NGSS logs and alarms.

The Policy Controller uses self-testing, automated diagnostics and log reporting systems to support maintenance activities and to manage and report faults. These systems raise alarms and generate logs when the following types of hardware or software events occur:

- fault or failure conditions
- correction or resolution of fault or failure conditions
- when a preset operating performance or resource capacity threshold such as CPU usage is crossed or exceeded
- a condition occurs that is transient or cannot be repaired and causes a system SWACT

Fault management for the Policy Controller platform encompasses the following functions:

- Set up and manage resource thresholds, such as monitoring disk usage and file system usage
- Monitor alarms at either the CS 2000 NCGL Platform Manager or the CS 2000 Policy Controller Manager GUI
- Review log reports using the CS 2000 NCGL Platform Manager or CS 2000 Policy Controller Manager GUIs or view the logs directly from their log files using the NGCL CLI (command line interface)

  Note: If the Policy Controller is configured to transfer log reports to the OSS network rather than the Policy Controller GUIs, log reports may only be available to Integrated EMS or other 3rd party OSS applications rather than on the logs view of the Policy Controller GUIs. Regardless of the logs configuration, logs are always directly accessible from the log files located on the disk drives of either unit.

- Perform routine and preventative maintenance tasks
- Replace faulty equipment

Monitoring and managing alarms

Alarm notifications are sent to the IEMS NMS in the form of SNMP traps. The standard Nortel Alarm MIB is used for this purpose. Alarms notifications are also distributed to the web server and can be viewed from the Web GUI.

Information about alarms includes the alarm type, identifier, time-stamp, the unit generating the alarm, the severity and description of the alarm. Refer to the graphic View of the CS 2000 Policy Controller Manager alarms page on page 15 for a view of the alarms page. Active alarms are refreshed automatically every 45 seconds. Alarms are cleared automatically when the issue that raised the alarm has been corrected. If the problem is not corrected, the audit alarm reappears.

The Policy Controller captures all system events in the customer log which can be viewed from the web GUI as shown in the graphic Logs viewed from the Policy Controller Manager GUI. The log files are automatically rotated so that the log file system is never filled through logging activity.

View of the CS 2000 Policy Controller Manager alarms page

Unit	Activity	Jam	State	Connectivity	Host Name	Last Update Time
0	Active	no	simplx 4M+	LnkCon M	SPC2	10:35:40

The Alarms panel updates every 45 seconds
Datestamp of last update: Monday May 09th 2005 10:35:22 PM CST

Type	ID	Timestamp	Host	Severity	Description
Communications	Communications Protocol Error	Thursday March 10th 2005 03:58:57 PM	SPC2	Major	Host is not communicating with any NTP server(s); No. of configured server(s): 1; No. of accessible server(s): 0.
Processing error	Application Subsystem Failure	Thursday March 10th 2005 03:51:54 PM	SPC2	Major	The state is Standby Disabled.
Processing error	Underlying Resource Unavailable	Thursday March 10th 2005 03:51:54 PM	SPC2	Major	Mate unit is unavailable.

Alarm severity codes indicate the impact of events on the Policy Controller or other network elements. There are three levels of alarm: critical, major and minor. Based on the alarm severity, each alarm has

a specific color. Critical and major alarms are red and minor alarms are orange.

For details on Policy Controller alarms as well as procedures on viewing alarms and associated logs, refer to the Policy Controller Fault Management NTP, NN10438-911.

Monitoring Logs

The Policy Controller application or the platform generate logs associated with alarms. These logs are written to the local custlog file. Stored as ASCII-based text, in CSV format, the log data can be reviewed, copied, printed, saved to a remote system and loaded into a spreadsheet application for further analysis.

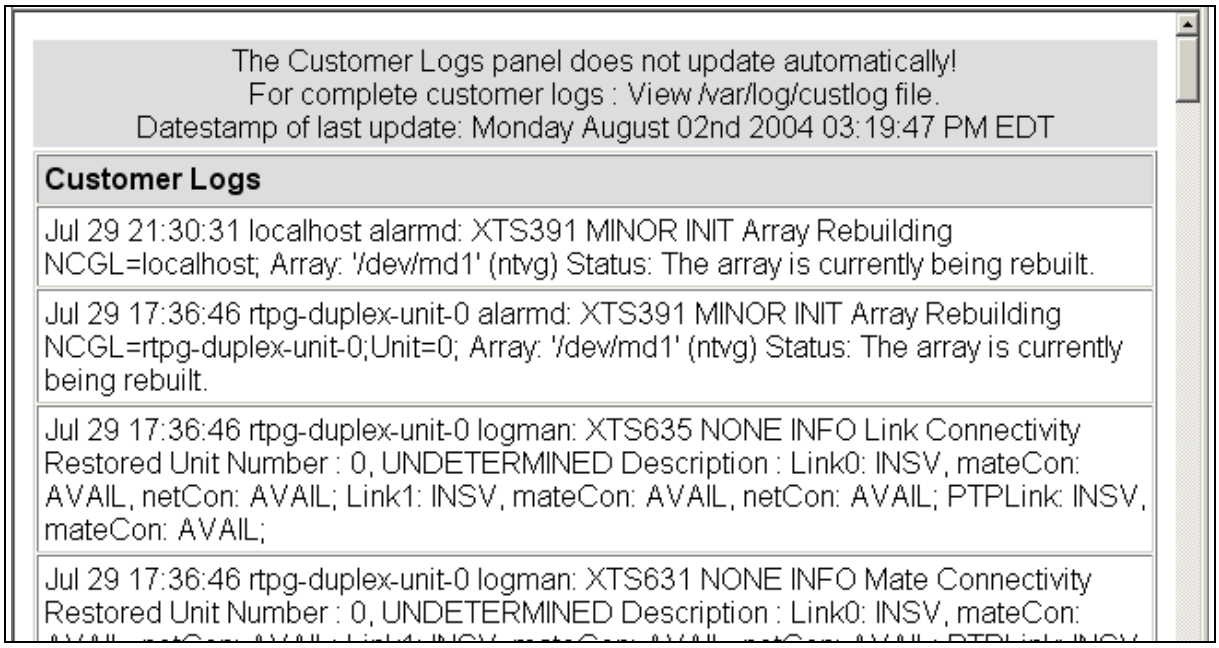
The Policy Controller can be configured to alter what log information is written to the local custlog file by redirecting log information to a remote log server and SNMP server using the NCGL commissioning tool.

If the Policy Controller is configured to transfer SNMP alarm traps to an OSS network, log reports related to the raising or clearing of alarms is only available on the Integrated EMS or other 3rd party OSS application, rather than on the logs view of the Policy Controller GUIs.

If the Policy Controller is configured to transfer logs to a remote log server, all logs that are ordinarily viewable from the Policy Controller GUI or local log file on the disk drive are sent to the log server.

The following sample logs view is displayed by the CS 2000 Policy Controller Manager. This view displays a maximum of the most recent 2000 line entries from the current custlog file. When viewing logs from an Integrated EMS system, log headers may differ slightly from what is shown in this view.

Logs viewed from the Policy Controller Manager GUI



Customer log histories can be only viewed by directly accessing the custlog file using the Policy Controller CLI (command line interface). Log files can also be downloaded using FTP to a PC or other system capable of connecting to the Policy Controller on the secure CS-LAN.

For details about Policy Controller logs and procedures on viewing logs, refer to the Policy Controller Fault Management NTP, NN10438-911.

Performance management

The Policy Controller records operational measurements (OMs) for various performance related events and stores them in CSV format. These OMs are information sources for determining preventive and corrective maintenance actions, and identifying provisioning problems or capacity limitations.

Policy Controller OMs are defined the following areas:

- Requests for resource reservation, resource commit and resource delete.
- CAC attempts, successes, failures, and usage summaries for each network zone.
- Topology changes/modification
- Half call attempts, successes

OMs are viewed through the Integrated EMS, using the command line interface (CLI) to the Policy Controller or through a direct, secure shell (SSH) connection to the Policy Controller. OMs cannot be viewed directly from the Integrated EMS.

OM data recorded on one unit of a Policy Controller node is completely independent of OM data recorded on its mate unit. Data is not transferred from one unit to another during Policy Controller application database synchronization activities.

When more than one Policy Controller node is installed in the network, OM data recorded by the first node is independent of that recorded by other Policy Controller nodes.

Service monitoring
Some operational measurements can indicate service level degradation for the Policy Controller when combined with alarms, indicating that resources are running low. This information helps to determine the corrective action which may include equipment repair.

Security monitoring
Some operational measurements can indicate security degradation or possible intrusion. When combined with alarms, this information helps to determine the corrective action which may include generating new security certificates or disconnecting suspicious remote servers.

Security and Administration

The NGSS software platform provides security functionality to the Policy Controller.

The platform provides the following security functions:

- User login and password authentication
- Web based security user access using HTTPS
- Secure shell environment (SSH)
- Transport Layer Security (TLS)

For the Policy Controller web GUI pages, there are some privileges which can be assigned to specific operating personel. For example, some operating personel may only have read-only privileges, and someone with administrator privileges can write and modify the Policy Controller configuration.

The UID/Password is used to determine the user access level, and privileges are based on user access level. The authentication of the user is done during the login process. For each topology configuration

command, the access privilege is checked and based on the user group. If the user does not have sufficient privilege to execute a command, an error message "Insufficient Security Privileges to perform this action" is returned as part of the response.

The Policy Controller uses access groups for configuration, provisioning, and maintenance commands. The access group levels are: mgcadm, mgcrw, mgcprov, mgcmtc, mgcro.

The Policy Controller is deployed on the CSLAN. The signaling between the CS2000-GWC and Policy Controller takes place on a subnet of the CSLAN. The Policy Controller provisioning web client can be launched from IEMS. The OSS operator can log into the Policy Controller through IEMS/SSPFS secure proxy and SSH. SSH is used to secure the connection between IEMS and Policy Controller.

Lawful Intercept (LI) enables law enforcement agencies to monitor the communication content of a subscriber. LI is not implemented on the Session Policy Controller. It is offered on the CS2000-GWC as a regular Carrier VoIP feature.

The Policy Controller provides a uniform topology provisioning interface for OSS and Policy Controller Web GUI. This interface is responsible for creating server sockets, listening ports, setting up a new connection when a client (OSS or GUI) is connected, authenticating users, and receiving client (OSS or GUI) requests. Since the management interface can process multiple connections at the same time, the Policy Controller implements a delayed IP address holder function to prevent any one user from abusing these connections. If a user sets up a connection and does nothing but immediately closes the connection, the IP address of the client is recorded and any connections from that IP address are rejected until the delay-time for that IP address has expired. The delay timer is configurable and default value is 10 seconds.

For more information on security for the Policy Controller, refer to the Policy Controller Security and Administration NTP, NN10434-611.

Operation Support Systems (OSS)

The Policy Controller provides an XML based provisioning interface that can be reused for OSS purposes.

The Policy Controller supports an OSS interface for topology provisioning. The OSS interfaces are programmed to process XML command requests as service orders are sent. Separate commands are required for multiple operations. For example, in order to add multiple Network Segments, an XML command request would be

needed for each Network Segment. The Policy Controller XML command schema is published as part of the OSSGate User's Guide, NE10004-512. Policy Controller XML configuration commands are in the Policy Controller Configuration Management NTP, NN10432-511.

Operational administration

User administration is controlled through the CS2000 Sesssion Server GUI, the Policy Controller GUI, and the CLI. Procedures for managing users are found in the Policy Controller Security and Administration NTP, NN10434-611.

Upgrading the Policy Controller

The NCGL platform software and the Policy Controller application can be patched or upgraded by way of an MR (maintenance release) upgrade. Refer to the Upgrading the Policy Controller NTP, NN10431-461, for more information.

Customer support

Refer to the Basics NTP applicable to your Carrier VoIP solution to find information about support options and to Policy Controller order software.