Carrier VoIP

USP Configuration Management

NN10093-511

Document status: Standard
Document version: 08.02
Document date: 20 October 2006

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

New in this release

The following section details what's new in *USP Configuration Management* for release (I)SN09U.

Features

See the following sections for information about feature changes:

MTP3 User Adaptation (M3UA) RFC compliance for SSG
This feature enhances the USP M3UA RFC compliance according to IETF RFC3332 in order to interwork with SSG. This feature affects the following sections:

- "USP provisioning procedures" (page 7)
- "Configuring Application Server Processes" (page 302)
- "Configuring Application Server Process Paths " (page 304)
- "Configuring Application Servers" (page 308)
- "Configuring Routing Keys" (page 312)

Other changes

See the following section for information about changes that are not feature-related:

- Updated procedure, "Adding routesets" (page 143)

USP Configuration Management

USP configuration management strategy

Once all hardware is in place, and the software is upgraded to the correct software release, you can use the Universal Signaling Point (USP) GUI or Command Line Interface (CLI) to configure the USP.

Logging in to the System

To log into a site, follow these steps:

Step	Action
	At the OAMP workstation
1	Click **File>session-login**.
	ATTENTION If you need to log into a site that is not available from the drop-down menu, see "Configuring USP Sites" (page 35).
2	Select a site from the **Site** drop-down menu.
3	Enter your user ID in the **Login** dialog box. If you don't have a user ID, contact your system administrator.
4	Enter your password in the **Password** dialog box. If you do not have a password, or if you forget your password, contact your system administrator.
5	Click **Login**. The Login Status window displays the progression of the connection.
	—End—

Logging out of the System

To close the USP application:

Step	Action
	At the OAMP workstation
1	Click **File>exit**.
	—End—

Configuring your USP with site-specific datafill

Your Universal Signaling Point (USP) is provisioned with default settings during initial installation. You must modify these settings to enable your USP to operate within your network. The procedures in this section provide the steps necessary for you to take your USP from its default configuration to the configuration that you require.

USP provisioning procedures

The USP Configuration Management manual contains a description of the procedures associated with all tables found under the File and Configuration menu of the USP Java GUI. Perform the procedures as ordered below using the identified panels:

- **File** menu:
  - Adding your Site: **File>site-manager**

    You must add the site information for your USP to the USP GUI to access the system from your alternate boot server.
  - Logging In: **File>session-login**

    Once a site is configured you can log into it using **File>session-login**. For more information on how to login, refer to the Security and Administration guide.

- **Configuration>platform** menu

  The platform menu level provides access to tables associated with the system, shelf, node, port, and channel.
  - System configuration: **Configuration>platform>system**

    Enables the changing of the system name and also the selecting the ATM configuration (direct or with ICCM).
  - Shelf configuration: **Configuration>platform>shelf**

    Shelves can be added with this table.
  - Node configuration: **Configuration>platform>node**

    Nodes on the various shelves can be configured with this table. The graphical view tab provides a graphical view of all the shelves showing alarm indications associated with the various nodes.
  - Port configuration: **Configuration>platform>port**

    The port configuration of the various SS7 interfaces can be modified with this table.
  - Channel configuration: **Configuration>platform>channel**

The channel configuration associated with T1 and E1 channelized interfaces can be modified with this table.

- **Configuration>timer-parm** menu

  The Timer Parameter menu level enables the configuration of the various timers and parameters used by the SS7, SAAL, and SIGTRAN protocols.

  — MTP Level 2 timers: **Configuration>timer-parm>level-2-timer**

  Message transfer part (MTP) Level 2 timers used on SS7 low-speed links and MTP 2 High-speed links are configured using this table.

  — MTP Level 3 timers: **Configuration>timer-parm>level-3-timer**

  MTP Level 3 timers used for all SS7 links are configured using this table.

  — MTP Signaling Link Test timers: **Configuration>timer-parm >slt-timer**

  Signaling test timers used for all SS7 links are configured using this table.

  — SAAL Timers: **Configuration>timer-parm>saal-timer**

  The SAAL parameters are used for ATM High-speed Links.

  ATTENTION
  There are no default SAAL parameter indexes, so an index must be provisioned prior to provisioning an ATM High-speed Link.

  — SAAL Parameters: **Configuration>timer-parm>saal-parm**

  — SCTP Parameters: **Configuration>timer-parm>sctp-parm**

  SCTP is used for IPS7 M3UA paths and M2PA High-speed Links.

- **Configuration>mtp** menu

  Your USP does not contain any MTP provisioning data at the conclusion of the initial installation. You must enter the MTP provisioning data to make your USP part of your SS7 network.

  — Provisioning the System Identity:**Configuration>mtp>system-id**

  A USP supports multiple system identity each specifying a protocol variant and a point code.

  — Provisioning the Capability Codes:**Configuration>mtp>capability-code**

  You can also identify the system with an alternate Point code. This alternate point code, called a capability code, is usually shared with a mated USP to facilitate GTT (global title translation) loadsharing.

— Provisioning Linksets: **Configuration>mtp>linkset**

A linkset is a set of links that carries SS7 signaling information between two nodes in an SS7 signaling network. The maximum number of SS7 links in a linkset is dependent on the link type of the linkset. Linksets can contain up to 16 links each.

Your USP supports six different types of SS7 signaling links. They are as follows:

– A-Links

– B-Links

– C-Links

– D-Links

– E-Links

– F-Links

— Provisioning links: **Configuration>mtp>link**

Links provide the physical connection between two adjacent signaling points in a network.

ATTENTION

To ensure that failure of a SS7 Link system node does not take out an entire linkset, Nortel Networks recommends that the links in your linksets be spread across the SS7 Link system nodes

— Provisioning Combined Linksets:**Configuration>mtp>combined-linkset**

A combined linkset is a set of two linksets which are used equally to loadshare SS7 messages. There should be only one link per combined linkset provisioned on an SS7 Link system node. B- and D-links are typically used in combined linksets. If you do not want to create combined linksets, proceed to the next section, Provisioning Linkset Groups.

— Provisioning Linkset Groups: **Configuration>mtp>linkset-group**

The linkset group is a structure unique to the USP. It is intended to simplify the process of creating routesets. A linkset group contains up to three linksets/combined linksets. The linksets and combined linksets that comprise a linkset group determine normal (primary) and alternate signaling routes.

— Provisioning Routesets: **Configuration>mtp>routeset**

A routeset is a collection of routes that describe the way in which signaling information travels from one node to the next.

— Viewing X-list entries: **Configuration>mtp>x-list**

This feature enables the USP to record the transfer state of individual members of cluster and network routesets. The x-list table enables the viewing of the states of individual members.

- **Configuration>sccp** menu

— Provisioning Remote Point Codes: **Configuration>sccp>remote-pointcode**

Remote Point Codes are routesets that the USP can route SCCP traffic using Global Title Translation.

— Provisioning Remote Subsystem: **Configuration>sccp>remote-subsystem**

Remote Subsystem are subsystem associated with a Remote Point Code that the USP can route SCCP traffic using Global Title Translation.

— Provisioning Remote Subsystem Concerned Point Codes: **Configuration>sccp>remote-subsystem-concerned-pointcode**

The USP routes Subsystem status information about a remote subsystem to Remote Subsystem Concerned Point Codes.

— Provisioning Local Subsystem: **Configuration>sccp>local-subsystem**

Local subsystem are local to the USP System Identity. The subsystem instances can be on local nodes (as in the case of NP) or reside on Application Servers (as in the case of IP Local Subsystem).

— Provisioning Dedicated Local Subsystem Instances: **Configuration>sccp>dedicated-local-subsystem-instance**

Dedicated local subsystem instance are dedicated to a specific system identity. This is the case for IP Local Subsystem. This table enables the provisioning of IP Local Subsystem Instances, by specifying the Application Server associated with the instance.

— Provisioning Shared Local Subsystem Instances: **Configuration>sccp>shared-local-subsystem-instance**

Shared local subsystem instances apply to all system identities. This is the case for NP, Service Location Register (SLR), and Low Layer Control Point (LLCP) Local Subsystems. This table enables the provisioning of NP/SLR/LLCP Local Subsystem Instances, by specifying the node associated with the instance.

— Provisioning Local Subsystem Concerned Point Codes: **Configuration>sccp>local-subsystem-concerned- pointcode**

The USP sends the local subsystem status to all concerned point codes associated with that local subsystem.

— Provisioning NPE Chains: **Configuration>sccp>npe-chain**

Number Portability or Service Location Register can employ chains of NP cards to increase the number of records. The Number Portability Extension (npe) -chain enables the provisioning of the chains of NP cards.

- **Configuration>gtt** menu

SCCP Global Title Translation allows the USP to route SCCP messages using Global Title translation.

— Provisioning GTT results: **Configuration>gtt>gtt-result**

This table enables the provisioning of 3 result types: PC-only, PC-SSN, and SSN-Only. For PC-Only and PC-SSN, up to 16 results can share the same name and therefore the GTT Translation can loadshare across these results.

— Provisioning GTA results: **Configuration>gtt>gta-result**

The Global Title Address (GTA) result table enables the provisioning of GTA that replaces the GTA in the called party address of the message. This GTA result makes use of a provisioned PC-Only result for message routing.

— Provisioning MRGT results: **Configuration>gtt>mrgt-result**

Message Relay global title (MRGT) translation results enables additional field to be modified during the GTT process such Nature of Address (NoA), etc.

— Provisioning GTT Translation: **Configuration>gtt>gtt-translation**

GTT Translation makes use of the results provisioned above to translated the called party address in order to route the incoming messages.

- **Configuration>gws** menu

The Gateway Screening (GWS) menu level enables the provisioning of Gateway Screening and MSU tracing.

— Provisioning GWS control: **Configuration>gws>control**

This table enables the turning on and off of Gateway Screening on specific linksets.

— Provisioning GWS criteria name: **Configuration>gws>criteria-name**

This table enables the provisioning of a Gateway Screening criteria name that can then be used on specific linkset.

— Provisioning GWS criteria set: **Configuration>gws>criteria-set**

This table enables the provisioning of a criteria set for a specific criteria name. A set links the various rows of the Gateway Screening table.

— Provisioning GWS criteria Allowed OPC: **Configuration>gws>criteria-row-alwopc**

Use this table to specify the range of OPC that are allowed.

— Provisioning GWS criteria Blocked OPC: **Configuration>gws>criteria-row-blkopc**

Use this table to specify the range of OPC that should be blocked.

— Provisioning GWS criteria Allowed SIO: **Configuration>gws>criteria-row-alwsio**

Use this table to specify the range of SIOs (Signaling Indicator Octet) that should be allowed.

— Provisioning GWS criteria Allowed DPC: **Configuration>gws>criteria-row-alwdpc**

Use this table to specify the range of Destination Point Codes (DPC) that should be allowed.

— Provisioning GWS criteria Blocked DPC: **Configuration>gws>criteria-row-blkdpc**

Use this table to specify the range of DPC that should be blocked.

— Provisioning GWS criteria Allowed ADF: **Configuration>gws>criteria-row-alwadf**

Use this table to specify the range of Affected Destination Point Code (ADF) that should be allowed. This is with respect to the ADF field of TFx messages.

— Provisioning GWS criteria Allowed CGPA: **Configuration>gws>criteria-row-alwcgpa**

Use this table to specify the range of Calling Party Address (CGPA) that should be allowed.

— Provisioning GWS criteria Allowed TT: **Configuration>gws>criteria-row-alwtt**

Use this table to specify the range of Translation Type (TT) that should be allowed.

— Provisioning GWS criteria Allowed CDPA: **Configuration>gws>criteria-row-alwcdpa**

Use this table to specify the range of Called Party Address (CDPA) that should be allowed.

— Provisioning GWS criteria Allowed PC SSN: **Configuration>gws>criteria-row-alwpcssn**

Use this table to specify the range of Point Code Subsystem (PCSSN) that should be allowed.

— Provisioning GWS criteria Allowed ISUP: **Configuration>gws>criteria-row-alwisup**

Use this table to specify the range of ISUP message types that should be allowed.

— Provisioning MSU Tracing: **Configuration>gws>msu-trace**

The MSU Trace table allows the viewing of the data that was captured during the tracing of message.

- **Configuration>msg-trace** menu

The Message Trace menu enables the provisioning and tracing of message data.

— Provisioning a Message Trace ruleset:**Configuration>msg-trace>msg-trace-ruleset**

Use this window to provision and perform maintenance activities for rulesets.

— Provisioning a Message Trace rule: **Configuration>msg-trace>msg-trace-rule**

Use this window to provision and perform maintenance activities for rules. You can also use this window to create sets of rules that can be applied to any link or path using the Control table.

— Provisioning a Message Trace control: **Configuration>msg-trace>msg-trace-control**

Use this window to provision and perform maintenance activities for rulesets against links or paths.

— Provisioning a Message Trace: **Configuration>msg-trace>msg-trace**

Use this window to view the real time traceback of decoded messages passed through the network.

- **Configuration>np** menu

The NP menu level enables the provisioning of Number Portability information. Refer to the Number Portability section of this manual.

ANSI NP

— Provisioning ANSI NP LSS Misc: **Configuration>np>np-ansi>np-lss-misc**

The Number Portability Local Subsystem Miscellaneous window enables you to define some general characteristics for your ANSI NP system.

— Provisioning ANSI NP Service Name: **Configuration>np>np-ansi>np-service-name**

Use this screen to identify the various services that you are going to support for ANSI Message Relay on the USP.

— Provisioning ANSI NP Service Rules Definition: **Configuration>np>np-ansi>np-service-rules**

Use this screen to set up the rules that will be used by the USP to identify the messages associated with a particular service for ANSI message relay processing.

— Provisioning ANSI NP GTT Override: **Configuration>np>np-ansi>np-gtt-override**

Use this screen to provision an alternate destination for NPAC provided message relay destinations.

— Provisioning ANSI NP Translation Type Mapping: **Configuration>np>np-ansi>np-translation-type-mapping**

Use this screen to provision a new translation type post-message relay processing to the outgoing message to indicate to the next node that a lookup has already been performed (loop prevention).

— Provisioning ANSI NP IN Configuration: **Configuration>np>np-ansi>np-in-config**

Use the NP IN 1.0 Protocol Configuration window to enter carrier identification codes (CIC) and billing indicator information. The provisioned values are used for IN 1.0 query responses.

ITU NP

— Provisioning ITU NP LSS Misc: **Configuration>np>np-itu>np-lss-misc**

The Number Portability Local Subsystem Miscellaneous window allows you to define some general characteristics for your ITU NP system.

— Provisioning ITU NP Service Name: **Configuration>np>np-itu>np-service-name**

Use this screen to identify the various services that you are going to support for ITU Message Relay on the USP.

— Provisioning ITU NP Service Rules Definition: **Configuration>np>np-itu>np-service-rules**

Use this screen to setup the rules that will be used by the USP to identify the messages associated with a particular service for ITU message relay processing.

— Provisioning ITU NP Service Misc: **Configuration>np>np-itu>np-service-misc**

Use this screen to provision some miscellaneous parameters associated with ITU Message Relay processing on the USP.

— Provisioning ITU NP Service Message Relay Looping Prevention: **Configuration>np>np-itu>np-service-message-relay-looping-prevention**

Use this screen to provision the parameters associated with looping prevention functionality for the ETSI/ITU Message Relay services.

— Provisioning ITU NP Service PC/SSN: **Configuration>np>np-itu>np-service-pcssn**

Use this screen to modify the information relating to PC SSN results found in the NP database during ITU non-call related services. The UNPM, by default, uses the same system id and Nature of Address (NoA) values for an outgoing non-call related message as was received in the incoming message. This screen must be datafilled to redirect the message to a destination in a different system id or with a different NoA than the incoming message.

— Provisioning ITU NP INAP Config: **Configuration>np>np-itu>np-inap-config**

Use this screen to provision parameters associated with INAP message processing for ITU call-related messaging.

— Provisioning ITU NP General: **Configuration>np>np-itu>np-itu-general**

Use this screen to provision a set of general attributes for various aspects of ITU NP provisioning for both call and non call-related message handling.

— Provisioning ITU NP Call SRF: **Configuration>np>np-itu>np-call-srf**

Use this screen to provision data for the ITU Call-Related Signal Relay Function capability on the USP. This capability is one method used in wireless networks to support NP.

— Provisioning ITU NP NoA RN: **Configuration>np>np-itu>np-noa-rn**

Use this screen to provision a set of valid nature of address (NoA) and routing number (RN) combinations for each ITU system identity

that has a local subsystem (LSS) provisioned against it. The Nature of Address RN screen is part of the USP's number normalization function for both Message Relay and Call Related SRF.

— Provisioning ITU NP RN to IMSI: **Configuration>np>np-itu>np-rn-to-imsi**

Use this screen to provision International Mobile Subscriber Identity (IMSI) numbers that are used in outgoing Call Related SRF MAP SRI acknowledgement messages against associated RNs or RN ranges. These "generic" IMSIs represent the subscription network corresponding to their associated RNs.

— Provisioning ITU NP Local RN: **Configuration>np>np-itu>np-local-rn**

Use this screen to provision RN number ranges to which the USP is responsible for routing NP SRF messages. The RN ranges are defined by a low and high RN.

- **Configuration>ips7** menu

The IPS7 menu level enables the provisioning of Application Servers and some routing keys to these Application Servers. Communication to the Application Servers is done using M3UA and SCTP.

— Provisioning Application Server Processes: **Configuration>ips7>application-server-process**

An Application Server is made of up to two Application Server Process that are in active/standby mode.

— Provisioning Application Server Process Paths: **Configuration>ips7>application-server-process-path**

Application Server Process paths are provisioned for each application server process. The paths are used for communication between the USP and the Application Server.

— Provisioning Application Server: **Configuration>ips7>application-server**

An Application Server is an IP-based entity that can communicate with the USP using M3UA/SCTP or M3UA/UDP paths. The USP cannot route/distribute traffic to an Application Servers unless a routing key is defined or an ASM is provisioned. Possible routing keys are:

– Destination Point Code: Routing key is provisioned using the Application Server Destination table.

– Local Subsystem: Routing key is provisioned using the Local Subsystem table.

  - Originating Point Code: Routing key is provisioned using the Application Server Assignment table.
  - Route Set: Routing key is provisioned using the Routing key table.

    There are special routing keys associated with an ASM. An ASM is a special Application Server representing the Carrier Voice over IP CS2K Core or the Univity home location register (HLR) Core.

— Provisioning Application Server Destination: **Configuration>ips7>application-server-destination**

This table enables the provisioning of routing keys based on the destination point code of the message. This is similar to routesets in the SS7 domain.

— Provisioning Application Server Assignment: **Configuration>ips7>application-server-assignment**

This table enables the provisioning of routing keys based on the originating point code of the message. The DPC in this case would be the USP system identity's PC (or one of its capability code).

— Provisioning a routing key:**Configuration>ips7>routing-key**

This table enables the provisioning of a routing key that describes a set of SS7 parameters and parameter values that uniquely define the range of signalling traffic to be handled by a particular Application Server (AS).

- **Configuration>rm** menu

The Route Master menu level enables the provisioning of Route Master specific tables.

— Provisioning Route Master System ID Mapping: **Configuration>rm>system-id-mapping**

This table enables the provisioning of the Router Master, Donor, and Host system identity.

— Provisioning Route Master Trunk Mapping: **Configuration>rm>trunk-mapping**

This table enables the provisioning of the trunk mapping specifying if the trunk is owned by the Donor or the Host node.

— Provisioning Route Master Dial Number Mapping: **Configuration>rm>dn-mapping**

This table enables the provisioning of the dial number mapping specifying if the dial number is owned by the Donor or the Host node.

- **Configuration>slr** menu

  The SLR menu level enables the provisioning of SLR-specific information timers and domain name.

  — Provisioning SLR Miscellaneous Information: **Configuration>slr>slr-misc**

  Enables the modification of translation type mapping and country code.

- **Configuration>sip** menu

  The SIP menu level enables the provisioning of SIP application timers and domain name.

  — Provisioning SIP Application timers: **Configuration>sip>application-timers**

  Enables the modification of the TCAP and CALL timeout associated with the USP SIP Application.

  — Provisioning SIP domain names: **Configuration>sip>domain-name**

  Enables the modification of the SS7 and IP Domain name used for the SIP Application.

- **Configuration>llcp** menu

  The Low Layer Control Point (LLCP) menu allows you to provision LCCP functionality.

  — Provisioning the country code: **Configuration>llcp> country-code**

  Enables you to specify the country code to be used as the prefix in the LLCP database.

  — Provisioning overlap outpulse interdigit collection timeout: **Configuration>llcp>overlap-outpulse**

  Enables you to set a timeout value for a specific system identity.

  — Provisioning the abort cause parameters: **Configuration>llcp>abort-cause**

  Enables you to provision the parameters to be returned to the originator when an error condition causes a call to abort.

  — Provisioning release cause parameters: **Configuration>llcp>release-cause**

  Enables you to provision the parameters to be returned to the originator when an error condition causes a call to be released.

  — Provisioning timers: **Configuration>llcp>llcp-timer**

  Enables you to provision values for the timers used by LLCP.

— Provisioning the cgpa replacement entry: **Configuration>llcp>lcgpa-replace**

Enables you to modify the calling party address information in the SCCP portion of messages sent from the LLCP.

— Provisioning AOC bypass: **Configuration>llcp> aoc-bypass**

Enables you to provision calling party numbers that are exempt from the advice of charge (AOC) functionality.

— Provisioning a service key to follow a routing procedure: **Configuration>llcp> tc-relay**

Enables you to associate a service key from the incoming TCAP message with a routing procedure.

— Provisioning callgap criteria: **Configuration>llcp> callgap**

This submenu enables you to provision the parameters used for callgap functionality:

– callgap-criteria

– callgap-profile

– callgap-profile-group

– callgap-traffic-rate

Advanced GUI Features

The JAVA GUI for the USP has several features, tools, and utilities that you can use to configure the system. These features are not associated with any specific user task or procedure.

USP RTC nodes activity status

USP system consists of two Real-time controller (RTC) nodes for redundancy. Each node maintains its activity status by negotiating with its mate node. At any point in time, only one RTC node should be active.

If the RTC nodes are not able to communicate with each other, this may lead to invalid activity states where both nodes are active or none of the nodes are active.

The USP JAVA GUI pops up error dialogs to inform the user about the invalid activity state. The two scenarios are described below.

Scenario 1: No active RTC nodes

Description: The USP JAVA GUI pops up an error dialog stating: "No rtc node is active. No usp commands/real time logs will be processed until an rtc node becomes active. Refer to the USP documents for probable causes and corrective actions". The dialog box disappears automatically once the normal state is restored, or it can be closed by clicking on the "OK" button.

The USP JAVA GUI status bar displays: "Invalid rtc nodes state - No node is active" and this message remains on the status bar until it gets overwritten by another status message.

Probable cause: Communication between RTC nodes is lost. This may be due to failure of both CC nodes.

Corrective action: Restore the communication between the RTC nodes. Bring up the CC nodes on the system.

Scenario 2: Both RTC nodes are active

Description: The USP JAVA GUI pops up an error dialog stating: "An undesirable condition where both rtc nodes are active is detected. Data shown may not be correct and any data provisioning during this condition may get lost. Refer to the USP documents for probable causes and corrective actions". The dialog box disappears automatically once the normal state is restored, or it can be closed by clicking on the "OK" button.

The USP JAVA GUI status bar displays: "Invalid rtc nodes state - Both nodes are active" and this message remains on the status bar until it gets overwritten by another status message.

Probable cause: Communication between rtc nodes is lost.

Corrective action: Restore the communication between the RTC nodes. Bring up the CC nodes on the system.

Real-time alarms

The alarm banner provides a summary of the currently raised alarms in the system by alarm severity: C – critical, M – major, and m – minor. If there are unacknowledged critical alarms, then the critical alarm panel flashes indicating this condition. Critical alarms should be resolved immediately.

The GUI can automatically load the alarm table with a Real-time list of active alarms.

Loading real-time alarms

Step	Action
At the OAMP workstation	
1	Double-click the alarm banner.

—End—

Status panels

The status panel of the main window provides overall session status, including connectivity status and software upgrade status.

- connection status – The connection status panel indicates the current connected site including version information and whether the session is connected in simplex or duplex mode.
- upgrade status – If a software upgrade is in progress, then the upgrade status panel is visible and shows the current software upgrade state.

Monitor mode

The monitor and restore button toggles between full and compact views of the current GUI session. The monitor mode provides a convenient way to switch to a smaller window that displays only alarm and system status information.

Enabling the monitor mode

Step	Action
	At the OAMP workstation
1	Click the Monitor button in the Status bar.
	—End—

Restoring the full JAVA GUI

Step	Action
	At the OAMP workstation
1	Click the Restore button in the Status bar.
	—End—

Short cut keys

The USP JAVA GUI supports shortcut keys for navigating menus. Use the keyboard to access the menu by using Alt+<a>, as an alternative to using the mouse to point and click on the menu item.

Using shortcut keys

Step	Action
	At the OAMP workstation
1	Press the Alt key and the underscored letter of the menu item you want to use.
	—End—

Session lockout

Session lockout secures an OAMP workstation when it is left unattended for a specified period of time (default 15 minutes). If the GUI session is connected to a site and has not been used for the specified timeout value, then the GUI switches to a locked state and displays a password-protected login panel.

The session lock timeout value can be changed from the default value. Perform the following procedure to set the timeout value for the session lockout.

Setting the timeout value for session lockout

Step	Action

At the OAMP workstation

1 Click **Security>session-lockout.**

2 Select a lockout interval:

- lock session now
- 5 minutes of inactivity
- 15 minutes of inactivity
- 30 minutes of inactivity
- disabled

—End—

If the user credentials are updated while the session is locked, the updated credentials must be used to unlock the session.

If the current GUI session is not currently connected, and the session is locked, you must log out and log back in.

Data retrieval features

The following procedures detail the different data retrieval methods. Providing search criteria for data retrieval enables you to refine your search to a smaller set of records. When you select the appropriate table field, search condition, and value, it enables the data retrieval system to filter out records that do not meet the specified criteria, possibly reducing the number of records that are retrieved.

Retrieving records without search criteria conditions

Step	Action

At the OAMP workstation

1 Open the table you want to search.

2 Click the **Search** tab.

3 Click the **Records** combination box and select the number of records to retrieve (the default is 100 records).

Retrieving large record sets can take longer for larger tables. Provide search criteria to restrict the records retrieved based on a set of conditions to reduce the number of records retrieved for larger tables.

4 Click the **Retrieve** button. The progress of the search is indicated in the status bar of the table window.

If the number of returned records is equal to the number of requested records, then there may be more data available for the supplied search criteria. If you click Get **Next**, you can retrieve the next set of records continuing from the last record retrieved. If you select Get **Next**, it enables you to walk through the records in the increment of records that you have selected.

—End—

Retrieving records with search criteria conditions

Step	Action

At the OAMP workstation

1 Open the table you want to search.

2 Click the **Search** tab.

You can enable the **auto refresh** checkbox to automatically re-execute the search using the defined criteria. Auto refresh occurs every sixty seconds.

3 Click the **Records** combination box and select the number of records to retrieve (the default is 100 records).

Retrieving large record sets can take longer for larger tables. Provide search criteria to restrict the records retrieved based on a set of conditions to reduce the number of records retrieved for larger tables.

4 Select the field you want to search conditionally.

5 Select the search condition for the field from the condition drop-down combo box.

6 Type the search value for the selected table field and condition. The value must be valid for the currently selected table field.

Some fields have a predefined list of values. For these fields, the value text field area changes to a drop-down combo box that enables you to more conveniently select the table field search value.

7 Click the **Retrieve** button. The progress of the search is indicated in the status bar of the table window.

If the number of returned records is equal to the number of requested records, then there may be more data available for the supplied search criteria. If you click **Get Next**, you can retrieve the next set of records continuing from the last record retrieved. If you select **Get Next**, it enables you to walk through the records in the increment of records that you have selected.

—End—

Retrieving records with additional search criteria conditions (advanced searching)

Step	Action

At the OAMP workstation

1 Open the table you want to search.

2 Click the **Search** tab.

You can enable the **auto refresh** checkbox to automatically re-execute the search using the defined criteria. Auto refresh occurs every sixty seconds.

3 Click the **Records** combination box and select the number of records to retrieve (the default is 100 records).

Retrieving large record sets can take longer for larger tables. Provide search criteria to restrict the records retrieved based on a set of conditions to reduce the number of records retrieved for larger tables.

4 Select the field you want to search conditionally.

5 Select the search condition for the field from the condition drop-down combo box.

6 Add additional search criteria by clicking on the arrow button to expose the additional search criteria table. This enables additional search criteria to be supplied for the data retrieval conditions.

7 Select the additional search condition for the field from the **condition** drop-down combo box and click **Add**.

8 To remove search conditions from the search conditions list, select the desired search condition(s) and click **Remove**. This action removes the selected entries from the list of criteria.

9 If you want to perform a logical OR operation between the two search conditions, then double clicking on the logical operator enables you

to modify (edit) the value between an AND and OR operator. By default, all search conditions are logically ANDed together.

10 Click **Move Up** or **Move Down** to change the search order. All search conditions are applied in the order in which they appear.

11 Click the **Retrieve** button. The progress of the search is indicated in the status bar of the table window.

If the number of returned records is equal to the number of requested records, then there may be more data available for the supplied search criteria. If you click **Get Next**, you can retrieve the next set of records continuing from the last record retrieved. If you select **Get Next**, it enables you to walk through the records in the increment of records that you have selected.

—End—

Data administration

Use the USP JAVA GUI to add, modify, and delete records as detailed in the following procedures.

Adding a new table record

Step	Action

At the OAMP workstation

1 Open the table you want to change.

2 Click the **Administration** tab.

3 Click **New** on the action tool bar if there is already a posted record. If you click **New** again, it ensures all form fields are currently cleared.

4 Enter all the required administrative fields for the specific table.

5 Click **Add** on the action tool bar. Status and progress information of the operation is displayed in the status bar of the table window. The table window is disabled until the command execution is complete (for example, no other commands for this table can be executed while a command is in progress).

6 If command confirmation is required, a confirmation box appears. Select Yes to confirm the command. Some tables and commands have several levels of prompting.

When the change is complete, the table window re-enables and the command status result is displayed in the status bar. If an error occurred during command execution, then an appropriate error message is raised.

—End—

Modifying an existing table record

Step	Action

At the OAMP workstation

1. Open the table you want to modify.
2. Retrieve the table record(s) to modify using the search function.
3. Post the table record(s) to modify.
4. Click the **Administration** tab.
5. Update the record with your changes.
6. Click Modify on the action tool bar to commit your changes. Status and progress information of the operation is displayed in the status bar of the table window. The table window is disabled until command execution is complete (for example, no other commands for this table can be executed while a command is in progress).
7. If command confirmation is required, a confirmation box appears. Select **Yes** to confirm the command. Some tables and commands have several levels of prompting.

   When the change is complete, the table window will re-enable and the command status result is displayed in the status bar. If an error occurred during command execution, then an appropriate error message is raised.

—End—

Deleting an existing table record (from posted record)

Step	Action

At the OAMP workstation

1. Open the table you want to modify.
2. Retrieve the table record(s) to delete using the search function.

3 Post the table record(s) to delete.

4 Click the **Administration** tab.

5 Click **Delete** on the action tool bar to delete the record. Status and progress information of the operation is displayed in the status bar of the table window. The table window is disabled until the command execution is complete (for example, no other commands for this table can be executed while a command is in progress).

6 If command confirmation is required, a confirmation box appears. Select **Yes** to confirm the command. Some tables and commands have several levels of prompting.

When the change is complete, the table window re-enables and the command status result is displayed in the status bar. If an error occurred during command execution, then an appropriate error message is raised.

—End—

Posted sets

You can designate a subset of retrieved records as members of a posted set. This is a convenient way of performing operations on multiple records, as operations performed on the set are applied to all records in the set.

An active record is identified by a right arrow and is highlighted red. The active record is the current record displayed on the Administration panel and can be used during command execution to identify a single specific record of the posted set.

You can perform a modify command against multiple records of a posted set. When you modify the active record, you have the option to select which fields are going to be modified for all table records of the posted set.

The current posted record set can be exported to a local static file using the export function of the table. Click the export button identified by the icon on the table action toolbar.

Related table records from other tables can be retrieved for the currently active posted record

Creating a posted set

Step Action

At the OAMP workstation

1 Select records from the result window.

2 Click **Post**. Posted table records are marked with an **X** next to the table record, and are highlighted yellow.

—End—

Updating a posted set

Step	Action

At the OAMP workstation

1 Select a new record set.

2 Click **Post**. This clears the previous posted set and creates a new posted set consisting of the selected records. Posted table records are marked with an **X** next to the table record, and are highlighted yellow.

—End—

Clearing a posted set

Step	Action

At the OAMP workstation

1 Click **Clear**.

ATTENTION
When you click **Clear** when there are no records posted, it clears the current list of table records.

—End—

Adding and removing single records

Step	Action

At the OAMP workstation

1 Press **Ctrl+** and double-click the selected record to toggle the posted state of the record (adding and removing it from the posted set).

—End—

Changing active records

Step	Action

At the OAMP workstation

1 Double-click on the desired record in the posted set to make it active.

> **ATTENTION**
> When you double-click on a table record that is not part of a posted set, you make it active and posted and it becomes the only record of the new posted set.

—End—

Exporting posted table records

Step	Action

At the OAMP workstation

1 Create a posted set.

2 Click **Export**.

3 Enter the new target file name and select the export format, one of HTML, CSV, or Plain Text.

4 Click **Save**.

5 All currently posted records are exported in the current table field ordering.

The ordering of table field columns can be customized by dragging the column to a new location, or by using the table customization window. This window is accessible by right-clicking the table header and selecting the **Customize** menu item.

—End—

Retrieving related table records

Step	Action

At the OAMP workstation

1 Post the active record to the Administration panel.

2 Click the relation button on the table action toolbar. A list of possible related tables is displayed.

3 Select the tables that contain the related record you want and click **Ok**. All the selected tables open and an automatic search begins, based on the criteria of the currently active table record. If you click Cancel, the operation is aborted.

—End—

Special tables

The following special tables are accessible through the JAVA GUI.

Graphical View of platform-node

The graphical view of the platform-node table presents a visual representation of the current shelf/node status.

The graphical representation of the system nodes displays the current availability status, alarmed states associated with that node, and the current administrative state. If you double-click on a system node, you can post the record to the Administration panel with the currently selected record posted.

Maintenance commands are available from the Graphical View tab by right-clicking on a system node and selecting the command to execute.

Opening the Graphical View tab of the platform-node menu

Step	Action
	At the OAMP workstation
1	Click **Configuration>platform>node.**
2	Click the **Graphical view** tab.

—End—

log/om period search criteria

The log and om tables have special access to log periods and om periods respectively, to enable specific time periods to be retrieved. The log and om period information can be provided as search criteria to select only those table records associated with the selected time periods.

To select specific log or om periods the Search panel has an additional Periods button that brings up a period selection dialog. The current available periods are retrieved from the current connected system and presented in a selectable list of entries. To select multiple periods, highlight the records using the mouse and click **Select**. When the selection is complete, the search criteria will be automatically populated with the selected periods. If you click **Cancel**, then the search criteria will remain unaffected.

user-session table

The user-session table provides access to the currently connected users. The user-session table allows the user to message to chosen users using the internal messaging system.

To message to a single user or to a set of users, perform the following procedure.

Messaging users

Step	Action
	At the OAMP workstation
1	Click **Security>user-session.**
2	Create a posted set of the desired users.
3	Click the **Message** tab.
4	Enter the message to be sent to the posted users.
5	Click **OK**. The user-session table also has a Real-time panel that can be accessed by clicking on the **Realtime** tab of the table window. This provides an up-to-date view of the currently connected users. The user-session table also has a Messages panel that can be accessed by clicking on the Messages tab of the table window. This contains a history of all messages received from other users.

—End—

alarm table Realtime panel

The alarm table has an active real-time list of the currently raised alarms. To view the real-time alarm data, perform the following procedure.

Viewing Real-time alarm data

Step	Action
	At the OAMP workstation
1	Click **Fault>alarm**.
2	Click the **Realtime** tab.

—End—

log table Realtime panel

The log table has the ability to receive generated system logs in real time. To view Real-time log information, perform the following procedure.

Viewing Real-time log data

Step	Action
	At the OAMP workstation
1	Click **Fault>log.**
2	Click the **Realtime** tab.
3	Click **Start** to receive logs in real-time. The maximum number of logs stored locally can be controlled by selecting the current record limit for the **Realtime** panel. The default record limit is 1000 records. The Start and Stop commands are set for the current GUI session. Therefore, the logs are received for any site that is currently connected if the current state is started.

—End—

msu-trace table Realtime panel

The msu-trace table has the ability to receive trapped MSUs in real time. To view MSU captures in Realtime, perform the following procedure.

Viewing Realtime MSU traps

Step	Action
	At the OAMP workstation
1	Click **Configuration>gws.**
2	Click the **Realtime** tab.
3	Click **Start** to receive MSU traps in Realtime. The maximum number of MSUs stored locally can be controlled by selecting the current record limit for the Realtime panel. The default record limit is 1000 records. The Start and Stop commands are set for the current GUI session. Therefore the MSUs are received for any site that is currently connected if the current state is started.

—End—

single entry tables (no search panel)

Several tables are single entry tables and, therefore, do not have associated Search panels.

When invoking a single entry table, the only table record entry is automatically posted to the Administration panel.

Force a reload of supporting data

The USP JAVA GUI enables you to force an unconditional reload of supporting data for a form by holding the **Shift** key while clicking the Reload button.

Configuring USP Sites

USP Sites are provisioned on the USP GUI and represent the physical systems this workstation can access with a GUI session. You must configure the site information for each system that you want to access. The following sections describe how to add, modify, and delete site information from your OAMP workstation.

Deleting a Site

Step	Action
	At the OAMP Workstation
1	Click **File>site-manager**.
2	Click the **site name** list and select the name of the site that you want to delete.
3	Click **Delete**.
4	Click **OK** to close the site-manager window.

—End—

Adding a site

Step	Action
	At the OAMP Workstation
1	Click **File>site-manager** to access the Site Manager window.
2	Click **New**.
3	Enter the name of the site, up to 32 alphanumeric characters, in the **site-name** box. This field is not case-sensitive.

ATTENTION

When you name a site, Nortel Networks recommends you give it the same name as your system. (System names are configured under **Configuration>platform>system**.)

4	In the **rtc-12 ipaddress** box, enter the IP address of the first Real-time Controller (RTC) system node in the Control CAM shelf

5 In the **rtc-15 ipaddress** box, enter the IP address of the second RTC system node in the Control CAM shelf.

6 Select an authentication method:

- For direct connections, choose Standard Authentication to perform authentication at the USP; you can also use Standard Authentication with proxy enabled.
- To perform PAM + Proxy authentication using HTTPS, choose Central Authentication Server.

7 Enter the IP address and port number of the authentication server. For Central Authentication Server, the default port value is 8443.

8 If you are connecting to a proxy, click on the **enable proxy** checkbox.

9 Select either Telnet or SSH as the protocol for the connection.

ATTENTION
The USP 9.0 interface client does not support connections to USP 8.0 sites that are configured to use Telnet proxy.

10 Enter the address of the proxy server in the **proxy-server** box.

11 Enter port of the proxy server in **proxy-port** box. For telnet, the default port is 23. For SSH, the default port is 22.

12 Click **Advanced**... to set up the Host name, Username, and Password. The advanced proxy configuration enables you to customize the prompt and response tokens required to connect through the Telnet proxy. The proxy data stream is scanned for the prompt tokens (expect tokens), and when a pattern match is found, the response value (send value) is sent. The configuration defaults to a typical Telnet proxy configuration, but the prompt values can differ slightly for different Telnet proxies.

The pattern match response values have a few special patterns that are expanded with the appropriate value:

- %h replaced with FQDN of target host
- %a replaced with IP address of target host
- %u replaced with user name
- %p replace with user password or security token

Default values provisioned for proxy token pattern matching are:

- token="Host name:" response="%a"
- token="Username:" response="%u"

- token="Password:" response="%p"

ATTENTION
These are the default values to work with the Carrier Voice over IP Telnet proxy provided by SPFS for CS2K configurations.

13 Click **Apply** to save the information.

14 Click **OK** to close the **site-manager** window.

—End—

Modifying a site

Step	Action

At the OAMP Workstation

1 Click **File>site-manager**.

2 Click the **site name** list and select the site you wish to modify.

3 To change the IP address of the first RTC system node in the Control shelf, enter the new value in the **rtc-12 ipaddress** box.

4 To change the IP address of the second RTC system node in the Control shelf, enter the new value in the **rtc-15 ipaddress** box.

5 To change the authentication method, select either Standard Authentication or Central Authentication Server from the pull-down menu.

ATTENTION
If you choose Central Authentication Server, you must enable remote authentication. For more information about Remote Authentication, see *USP Security and Administration* (NN10159-611).

6 To enable or disable site proxy, check or uncheck the **enable telnet proxy** checkbox.

7 If Site proxy is enabled, you can change/add the **proxy ipaddress** and the **proxy port** in the appropriate boxes.

8 Proxy server advanced settings can be changed by clicking on the **Advanced**... button.

9 Click **Apply** to save the information.

10 Click **OK** to close the site-manager window.

—End—

Deleting a site

Step	Action
	At the OAMP Workstation
1	Click **File>site-manager**.
2	Click the **site name** list and select the name of the site that you want to delete.
3	Click **Delete**.
4	Click **OK** to close the site-manager window.

—End—

Logging into a Site

For more information on how to login, see *USP Security and Administration* (NN10159-611).

Exporting a Site

You can export site configuration files for use in other instances of the JAVA GUI. To do this, perform the following procedure.

Step	Action
	At the OAMP workstation
1	Click **File->site-manager**.
2	Click **Export**.
3	Using the **Save** dialog window, define a path for the exported file.
4	Enter a file name in the **File Name** field.
5	Click **Save**.

—End—

Importing a Site

You can import site configuration files for use in other instances of the JAVA GUI. To do this, perform the following procedure:

Step	Action
	At the OAMP workstation
1	Click **File->site-manager**.
2	Click **Import**.
3	Using the **Save** dialog window, navigate the path to the file to import.
4	Click **Open**. All new site information is added to the list of sites that are available. All existing sites (with the same name) are not affected by this operation.

—End—

Configuring a CAM Shelf

Modifying System Name

Each USP system is identified by a system name. To modify the name of the USP system, perform the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>platform>system**.
2	Enter the name of the USP system in the **system-name** box. The box accepts up to 32 characters.
3	Select the ATM configuration for this USP from the **atm-configuration** drop-down list. *Direct* is used for single or dual shelf system and indicate that no ICCMs (Inter CAM Controller Modules) are used. *ICCM* indicates that USP shelves are interconnected with an ICCM ATM switch.
4	Click **Modify** to save the new system name. A confirmation dialog box appears.
5	Click **Yes**. The new system name is updated in the title bars of all the windows that contain the system name in their titles.

—End—

CAM Shelf Information

Each CAM shelf in your USP system is identified by a shelf name and a brief shelf description. The following sections describe how you can identify and modify the CAM shelf information and the various logical elements of the CAM shelf that can be acted upon from the USP GUI.

Modifying CAM Shelf Information

The CAM shelf contains default information populated by the initial load. You can customize the name of the shelf as well as its description.

To modify CAM shelf information, perform the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>platform>shelf**.

2 Click the **Search** tab.

3 Click the **Retrieve** button.

4 Double-click the record you want to modify to populate the administration panel.

5 To modify the shelf name, enter a new name in the **shelf-name** box. The box accepts up to 32 characters.

> **ATTENTION**
> Nortel Networks recommends that the shelf name contain the system name and the number of the shelf.

6 To modify the shelf description, enter a new description of the shelf in the **shelf-description** box. You can enter up to 32 characters.

7 Click **Modify** to save the changes. A confirmation dialog box appears.

8 Click **Yes** to confirm the change.

—End—

Adding a CAM Shelf

CAM shelves can be added to the system by performing the following steps.

Step	Action
	At the OAMP workstation
1	Click **Configuration>platform>shelf**.
2	Click **New**.
3	Enter the shelf number in the **shelf** box.

> **ATTENTION**
> Shelf numbers 0 to 7 are supported, but you must provision shelves sequentially staring with 0.

4 Enter the shelf name in the **shelf-name** box. The box accepts up to 32 characters.

> **ATTENTION**
> Nortel Networks recommends that the shelf name contain the system name and the number of the shelf.

5 Enter a description of the shelf in the **shelf-description** box. You can enter up to 32 characters.

6 Click **Add** to save the changes. A confirmation dialog box appears.

7 Click **Yes** to confirm the change.

—End—

Configuring an Extension CAM Shelf

When adding an extension CAM shelf to your USP, you must provision the system to include the new shelf and its components.

ATTENTION

The NTST02AA CC card is supported in a single-shelf system only. If you have NTST02AA card and are upgrading your system to a dual or multi-shelf configuration, then you must upgrade your CC cards to either NTST02AB or NTST02BA .

To add an extension CAM shelf, you must perform the following procedures.

ATTENTION

If your system configuration will have three or more shelves, you must install and provision two ICCMs. You have the option to add ICCMs in two-shelf systems. An ICCM is the ATM switch required for adding more than two shelves to your USP. If you attempt to add a third shelf without first adding the ICCMs, the system sends an error message.

Adding ICCMs

Step	Action
	At the OAMP Workstation
1	If you are adding two ICCMs to your system configuration, perform the following steps. If you are not adding two ICCMs, skip this procedure and proceed to Provisioning the Extension Shelf.
2	Click Configuration>platform>system.
3	Change the atm-configuration from direct to iccm.
4	Click Modify. A confirmation dialog box appears.
5	Click Yes to confirm the change.

—End—

Adding Cable Connections for an Extension Shelf

Step	Action
	At the USP Chassis

1 Use an OC-3 cable to connect the CC in slot 1 of the extension CAM shelf to the correct line on the line card of the first ICCM. Refer to the table in Step 4for the correct line number for the cable attachment.

2 Check the LED for the line on the first ICCM. A green light indicates that the connection is correct. A red light indicates a line error. If the red LED is lit, refer to the USP In-service introduction of ICCMs in the Upgrade guide.

3 Use an OC-3 cable to connect the CC in slot 18 of the extension CAM shelf to the correct line on the line card of the second ICCM. Refer to the table in Step 4for the correct line number for the cable attachment.

4 Check the LED for the line on the second ICCM. A green light indicates the connection is correct. A red light indicates a line error. If the red LED is lit, refer to the USP In-service introduction of ICCMs in the Upgrade guide.

Connections for Extension Shelves

Extension Shelf	Link for CC1	Link for CC18
First extension shelf	line 1 (link card 0, ICCM 0)	line 1 (link card 0, ICCM 1)
Second extension shelf	line 2 (link card 0, ICCM 0)	line 2 (link card 0, ICCM 1)
Third extension shelf	line 3 (link card 0, ICCM 0)	line 3 (link card 0, ICCM 1)
Fourth extension shelf	line 4 (link card 0, ICCM 0)	line 4 (link card 0, ICCM 1
Fifth extension shelf	line 5 (link card 0, ICCM 0)	line 5 (link card 0, ICCM 1
Sixth extension shelf	line 6 (link card 0, ICCM 0)	line 6 (link card 0, ICCM 1
Seventh extension shelf	line 7 (link card 0, ICCM 0)	line 7 (link card 0, ICCM 1

5 Follow the steps in the section Provisioning the Extension Shelf before you add the physical connections for the next extension CAM shelf.

—End—

Provisioning the Extension Shelf

Step	Action

At the OAMP Workstation

1 Click **Configuration>system>shelf**.

2 Enter the shelf number in the shelf box. Shelf numbers 0 to 7 are supported.

3 Enter the shelf name in the shelf-name box. The box accepts up to 32 characters.

ATTENTION
Nortel Networks recommends that the shelf name contain the system name and the number of the shelf.

4 Enter the shelf description in the shelf-description box. The box accepts up to 32 characters.

5 Click **Add** to save the changes.

6 Repeat this procedure for each extension shelf that you want to add to your USP, up to a maximum of seven extension shelves.

—End—

Deleting an Extension CAM Shelf

Step	Action

At the OAMP workstation

1 Before deleting an extension CAM shelf, you must delete all provisioned application system nodes (Link, CAM Controller (CC), Number Portability Server (NPS), or Number Portability Controller (NPC) system nodes) from the extension shelf, and then delete the CC system nodes. For information on how to perform those procedures, refer to:

- "Deleting a Node" (page 84)
- "Performing Maintenance Activities on NP or LL Nodes" (page 85)

2 After deleting all the system nodes on the extension CAM shelf, perform the following steps to delete the shelf:

a. Click Configuration>platform>shelf.

b. Click the Search tab.

c. Click Retrieve and locate the shelf to delete. Double click on the shelf to go to the Administration view for this shelf.

d. Click Delete. A confirmation dialog box appears

e. Click Yes to confirm the change.

—End—

Deleting an ICCM

In a multi-shelf system, if you want to convert your system back to a single or dual shelf configuration, you can delete the ICCMs from your system. After deleting the unneeded shelves from your system, perform the following steps to delete the ICCMs:

ATTENTION

The USP requires two ICCMs for multi-shelf configurations. The system does not support configurations with only one ICCM except during software upgrade.

Step	Action
	At the OAMP Workstation
1	Click Configuration>platform>system.
2	Change the atm-configuration from iccm to direct.
3	Click Modify. A confirmation dialog box appears.
4	Click Yes to confirm the change.

—End—

Configuring an RTC System Node

You can perform provisioning and maintenance operations for an RTC system node from the platform node window.

The platform node window contains data such as the name of the RTC system node, a description of the RTC system node, PECs for the related hardware, and the names of the related boot image and boot data snapshot. It also contains the external IP address, external subnet mask, and external gateway address. In addition, you can edit the provisioning data and view the serial numbers and manufacturer information for the related hardware.

The platform node window also displays the state and status information for the RTC system node, identifies the currently running image file and data snapshot, and provides status messages.

ATTENTION

RTC system nodes reside only on control CAM shelves. If you have a dual-shelf system, the RTC system nodes on the control CAM shelf also serve as the Real-time Controllers for the extension CAM shelf.

The following table indicates the availability of the maintenance operations buttons in relation to the operational and administrative status and availability status (offline only) settings of an RTC system node.

Maintenance operation buttons availability

	Enabled		Disabled		
Maintenance Button	**Locked**	**Unlocked**	**Locked**	**Locked and offline**	**Unlocked**
SWACT	Yes	Yes	No	No	No
Diagnostics	N/A	N/A	N/A	N/A	N/A
Load	Yes	No	Yes	Yes	Yes
Lock	No	Yes	No	No	Yes
Unlock	Yes	No	Yes	No	No
Offline	Yes	No	Yes	No	No

Viewing RTC System Node Provisioning Data

RTC system node data cannot be viewed until the node has been loaded for the first time.

Viewing RTC System Node Provisioning Data

Step	Action
	At the OAMP Workstation
1	Click **Configuration>platform>node**.
2	Click **Graphical view**.
3	Double-click the RTC 12 or RTC 15 card on the control CAM shelf to open the RTC in the Administration panel.

—End—

Modifying RTC System Node Provisioning Data

Do not make any provisioning changes to the RTC system nodes while the inactive RTC system node is disabled. This can cause software errors or loss of data. In addition, do not make provisioning changes to the RTC system nodes when the system has critical alarms.

The following sections describe procedures for modifying different types of provisioning data for the RTC system nodes.

Modifying RTC System Node Name or description

Modifying RTC System Node Name or Description

Step	Action
	At the OAMP Workstation
1	Click **Configuration>platform>node**.
2	Click **Graphical view**.
3	Double-click the RTC 12 or RTC 15 card on the control CAM shelf to open the RTC in the Administration panel.
4	To change the name of the RTC system node, highlight or double-click the **slot-name** box and enter the new name, up to 32 characters.

ATTENTION

Nortel Networks suggests that the RTC system node name should contain information that indicates the system name, shelf name, function (RTC system node), and slot number.

5 To change the description of the RTC system node, highlight the contents of the **slot-description** box and enter a new description. This can be any useful information, up to 32 characters.

6 Click **Modify** to save the changes. A confirmation dialog box appears.

7 Click **Yes** to confirm the change.

—End—

Modifying RTC System Node PECs or Boot Image File

Modify the PECs when you replace an element of the current RTC system node with a new RTC system node element that has a different PEC (for example, NTST11BA instead of NTST11AB). Modify the boot image file when you receive a new version of the RTC system node boot image file.

Modifying RTC System Node PECs, Boot Image File,

Step	Action
	At the OAMP workstation
1	Click **Configuration>platform>node**.
2	Click **Graphical view**.
3	Double-click the RTC 12 or RTC 15 card on the control CAM shelf to open the RTC in the Administration panel.
4	Perform "Modifying the RTC Mission Card PEC" (page 53), then continue to execute this procedure.
5	To change the PEC of the PSE transition module, click the **tm-pec** list and select the appropriate PEC for the PSE transition module.
6	To change the boot image file for the RTC system node, click the **boot image** list and select an image file. These files are stored on the SCSI disk drive associated with this RTC system node.

ATTENTION

You cannot change the boot image file if the RTC system node is disabled.

If you have changed the PEC of the RTC card, you may need to change the boot image file.

7	To change the PEC of the SCSI disk card, click the **scsi-front-pec** list and select the appropriate PEC for your SCSI disk card.

ATTENTION
If you are also changing the SCSI disk card from a dual-slot SCSI to a single-slot SCSI, perform the procedure in the section Changing a Dual-slot SCSI to a Single-slot SCSI.

8 To change the PEC of the transition module for the SCSI disk, click the SCSI Disk TM PEC list and select the appropriate PEC for your SCSI disk transition module.

9 Click **Modify** to save the changes. A confirmation dialog box appears .

10 Click **Yes** to confirm the change.

11 If the RTC system node is locked, proceed to the next step. If the RTC system node is not locked, click **Lock** in the Maintenance portion of the window and proceed to the next step. A confirmation dialog box appears.

12 Click **Yes** to confirm the change.

13 Click **Load**. A confirmation dialog box appears.

14 Click **Yes** to confirm the change.

15 Click **Unlock**. A confirmation dialog box appears.

ATTENTION
If you changed your boot image file for a new release, Nortel Networks recommends that you delete the out-of-date image file from your system using the file manager function. For more information about the File Manager function, see *USP Security and Administration* (NN10159-611).

16 Click **Yes** to confirm the change.

—End—

Changing a SCSI

Use this procedure to replace a Single-slot SCSI, replace a Dual-slot SCSI, or change a Dual-slot SCSI to a Single-slot SCSI.

ATTENTION

The RTC performs an alternate boot because there is no data on the new SCSI. As a result, you must take the latest snapshot, copy it to the Alternate boot server (ABS), and set this snapshot to **Active**. Perform an ABS test on **Administration>alternate-boot-server**, and ensure the connection to the ABS is working properly.

CAUTION

Perform this procedure on each SCSI card to be replaced one at a time. An attempt to perform this procedure on more than one SCSI card simultaneously can result in service degradation.

CAUTION

Wear wrist straps and use standard antistatic precautions.

ATTENTION

Before you start this procedure, change the RTC to the latest data snapshot of the system.

Changing a SCSI

Step	Action

At the OAMP Workstation

1 Before replacing any cards, press all the Lamp Test buttons on the front and rear of the CAM shelf to ensure all the LEDs are working properly.

2 Click **Configuration>platform>node**.

3 Click **Graphical view**.

4 Double-click the slot of the first RTC mission card associated with the SCSI that you are changing. The platform node window appears.

5 If the card is active, click **Swact** to change the **activity-state**. After the Switch of activity (SWACT) is complete, wait at least 15 minutes before proceeding to the next step.

6 Select the correct SCSI PEC from the **scsi-front-pec** list. Click **Modify** to add the change. A confirmation dialog box appears.

7 Click **Yes** to confirm the change.

8 If the RTC system node is not locked, click **Lock**. A confirmation dialog box appears.

9 Click **Yes** to confirm the change.

10 Click **Offline**. A confirmation dialog box appears.

11 Click **Yes** to confirm the change.

12 Prior to replacing the SCSI disk, you must first remove the associated processor card.

Perform steps a - c to unseat the RTC system node:

a. Before you unseat an RTC, remove the screws that fasten it to the slot in the shelf.

b. Press outward on the top and bottom latches of the RTC card to release it from the CAM shelf.

c. Grasp the top and bottom latches of the RTC card and gently pull it toward you to remove it from the CAM shelf.

13 Repeat step 12 to remove the SCSI card you want to replace.

14 Perform the following steps to replace the SCSI:

a. Position the top and bottom latches of the new SCSI card facing you, and gently slide the SCSI card into the card guide of the one you removed, seating the bottom of the SCSI card into the card guide and then the top.

b. Apply pressure to the faceplate near the latches until you feel resistance.

c. Snap the top and bottom latches of the SCSI card inward, toward one another. Two audible clicks can be heard when the SCSI card is seated properly.

The next step depends on the action you are performing.

If you are replacing	Go to
a Single-slot SCSI with another Single-slot SCSI or a Dual-slot SCSI with another Dual-slot SCSI	step e
a Dual-slot SCSI with a Single-slot SCSI	step d

d. Insert a filler card or a replacement card in the empty slot not used by the SCSI card. Slot 14 or 17 becomes empty, depending on the RTC you are changing. Then go to step e.

e. Reseat the RTC mission card.

f. On the front and rear of the CAM shelf, press Lamp Test. If the LEDs do not light for the SCSI you just replaced, ensure the SCSI and RTC are seated properly by unseating each and completing step 14 again.

15 On the system node window, click **Load**. Click **Yes** to confirm. After three to five minutes, the **operational-state** on the RTC provisioning and maintenance window displays "enabled". The LED under the RTC flashes green on the front of the CAM shelf.

16 Click **Unlock** to unlock the RTC. A confirmation dialog box appears.

17 Click **Yes** to confirm the change.

18 At the front of the CAM shelf, ensure the LED under the RTC is a solid green light.

19 Wait at least 15 minutes before proceeding to the next step. Monitor all logs and alarms. Ensure all alarms are cleared before proceeding.

20 If necessary, repeat this procedure to replace the second SCSI disk card.

—End—

RTC Mission Card PEC

Modification of the RTC mission card PEC for the RTC system nodes should be performed from the OAMP workstation that is configured as an alternate boot server. Changing the RTC mission card PEC requires that you update the BOOTP server, which can be done only from the alternate boot server.

Modifying the RTC Mission Card PEC

Step	Action
	At the OAMP Workstation
1	Before replacing any cards, press all the Lamp Test buttons on the front and rear of the CAM shelf to ensure all the LEDs are working properly.
2	Click **Configuration>platform>node**.
3	Click **Graphical view**.
4	Click the RTC 12 or RTC 15 card on the control CAM shelf to open the RTC in the Administration panel.

5 Ensure that the RTC system node is enabled. This information is displayed in the Operational Data portion of the RTC system node Administration window.

If the RTC system node is enabled, proceed to step 9. Otherwise, proceed to step 6.

6 If the RTC system node is locked, proceed to step 7. Otherwise, click **Lock** and proceed to step 7. (The Lock button is located in the top bar of the window.)

7 Click **Load** to download the boot image and re-initialize and enable the RTC system node. (The Load button is located in the top bar of the window.)

ATTENTION
If the RTC system node does not enable, the PEC information for the RTC card can still be modified.

8 If the RTC system node is locked, proceed to step 9. Otherwise, click **Lock** and proceed to step 9.

9 Ensure that the RTC is inactive. This information appears in the Operational Data portion of the window.

If the RTC system node is inactive, proceed to step 10. Otherwise, click **SWACT**.

10 Click on the RTC Card list and select the appropriate PEC from the pull-down list. If you need to type in a PEC, place your cursor inside the box.

11 Click **Modify** to save your changes. A confirmation dialog box appears.

12 Click **Yes**.

13 Perform a backup operation. To do this, complete the following steps:

a. Click **Administration>backup**.

b. Enter a description of the data snapshot in the **`snapshot-description`** box. You can enter up to 32 characters.

You can have the snapshot automatically transferred to the Alternate Boot Server and set as the active snapshot. You can also automatically delete snapshots on the RTC and Alternate Boot Server when the maximum is reached. See *USP Security and Administration* (NN10159-611).

c. Click **Create** to create the data snapshot. An hourglass appears while the current system configuration is being saved.

The Backup Status box at the bottom of the panel indicates when the data snapshot has been successfully saved on the active RTC system node. The data snapshot is named for the date and time of its creation.

14 Return to the RTC Card window. If the RTC system node is offline, proceed to step 16. If the RTC system node is not offline, click **Offline**. A confirmation dialog box appears.

15 Click **Yes** to confirm the change.

16 Ensure that the LED below the slot for the RTC card to be replaced is not illuminated.

CAUTION
Wear wrist straps, and use standard antistatic precautions.

17 Replace the old RTC mission card with the new RTC mission card. To do this, perform the following steps:

a. Press outward on the top and bottom latches of the RTC mission card to be replaced. Two audible clicks can be heard when the RTC mission card is released completely.

b. Grasp the top and bottom latches of the RTC mission card and gently pull it toward you to remove it from the shelf.

c. Gently slide the new RTC mission card into the empty slot, seating the bottom of the RTC mission card into the channel, and then the top.

d. Apply pressure to the faceplate until you feel resistance.

e. Snap the top and bottom latches of the new RTC mission card inward, toward one another. Two audible clicks can be heard when the RTC mission card is seated properly.

18 In the RTC system node provisioning and maintenance window for the affected RTC system node, click **Load** to reload the RTC system node. A confirmation dialog box appears.

19 Click **Yes** to confirm the change.

20 Ensure that the LED is flashing for the slot containing the new RTC mission card.

21 Click **Unlock** to make the affected RTC system node available to the system. A confirmation dialog box appears.

22 Click **Yes** to confirm the change.

—End—

Modifying Boot Data configuration

Modify the boot data configuration when you need to perform a restore operation. Restore operations should be performed only in emergency situations where you need to recover a system configuration stored in an old data snapshot.

Modifying Boot Data configuration

Step Action

At the OAMP Workstation

1 Click **Administration>file-manager**.

2 From the Alternate Boot Server section, select the Snapshot folder, Version folder (for example, v11.0.0). Select the snapshot file with the latest timestamp for the required system configuration.

3 From the right side of the window, select the RTC system node.

If you are working with	Select the RTC node in
slot12	slot12
slot15	slot15

4 From the right side of the window, select the Snapshot folder, and the Version folder (the same version folder as selected in step 2).

The Version folder may not exist if a snapshot has never been stored on the RTC system node.

5 View the content of the Version folder on the right side of the window. If the data snapshot to be restored from the Alternate Boot Server is not listed or the Version folder does not exist, proceed to step 6. If the data snapshot to be restored is listed in the field, proceed to step 8.

6 From the Alternate Boot Server section, select the data snapshot to be restored.

7 Initiate a copy operation by clicking the arrow icon. An hourglass is displayed while the snapshot is being copied.

When the copy operation is complete, the fields in the Destination portion of the window update with the information for the copied snapshot.

8

If the boot image	Go to
needs to be changed	step 9
doesn't need to be changed	step 14

9 From the Alternate Boot Server section, select the load folder, Version folder (for example, v11.0.0) and the load file for the required system configuration.

10 From the right side of the window, select the load folder, and the Version folder (the same version folder as selected in step 9).

The Version folder may not exist if a load has never been stored on the RTC system node.

11 View the content of the Version folder on the right side of the window. If the load to be restored from the Alternate Boot Server is not listed or the Version folder does not exist, proceed to step 12. If the data snapshot to be restored is listed in the field, proceed to step 14.

12 From the Alternate Boot Server section, select the load to be restored.

13 Initiate a copy operation by clicking the arrow icon. An hourglass is displayed while the load is being copied.

When the copy operation is complete, the fields in the Destination portion of the window update with the information for the copied load.

14 Open the RTC system node administration tab for the RTC system node you are working with: slot12 or slot15. To do this, click **Configuration>platform>node**. Click the **Graphical view** tab, then double-click the slot you are working with: slot12 or slot15, to transfer the Administration panel.

15 Click the button next to the **boot-snapshot** field to change the boot data snapshot setting for the RTC system node. The system displays the data snapshots window. Select the data snapshot to be restored. The data snapshots window closes.

16

If the boot image	Go to
needs to be changed	step 17
doesn't need to be changed	step 18

17 To change the boot image setting for the RTC system node, select the boot image file for the node from the **boot-image** drop-down list.

18 Click **Modify** to save the changes and click **Yes** to confirm the changes if a confirmation dialog box is displayed.

When you change the boot snapshot, a minor alarm is generated that indicates that the running snapshot is different from the boot snapshot. This alarm is cleared when you perform a COR on your system or if you change the boot snapshot back to match the running snapshot.

When you change the boot image, a minor alarm is generated that indicates that the original image is different from the RTC boot image. This alarm is cleared when you perform a COR on your system or if you change the boot image back to match the running original image.

19 This procedure is complete. If applicable, return to the higher-level procedure or task flow that directed you to this procedure.

—End—

Modifying RTC System Node External IP Address

Modification of the external IP address for the RTC system nodes should be performed from the OAMP workstation that is configured as an alternate boot server. Changing the external IP address requires that you update the BOOTP server, which can be done only from the alternate boot server.

ATTENTION

Changing the IP address information for a piece of equipment can result in that equipment becoming unavailable. Nortel Networks recommends that this procedure be performed by persons with a clear understanding of subnets and IP LANs. If you are changing any IP address settings, use the procedures in the General System Provisioning section of this document.

Modifying RTC System Node External IP Address

Step Action

At the OAMP Workstation

1 Click **Configuration>platform>node**.

2 Click **Graphical view**.

3 Double-click the RTC 12 or RTC 15 card on the control CAM shelf to open the RTC in the Administration panel.

4 Verify whether the RTC system node to be modified is inactive. If the RTC system node is inactive, proceed to step 6. If the RTC system node is not inactive, click **Swact** to make this RTC system node inactive. A confirmation dialog box appears.

5 Click **Yes** to confirm the change.

6 Enter the new external IP address in the **ext-ip-address** box.

7 Click **Modify**. A confirmation dialog box appears.

8 Click **Yes** to confirm the change.

9 In order for the changed IP address to be used, you must re-load the RTC system node. Perform the following steps to re-load the RTC system node:

a. If the RTC system node is locked, proceed to the next step. If the RTC system node is not locked, click **Lock**. A confirmation dialog box appears.

b. Click **Yes** to confirm the change.

c. Click **Load**. A confirmation dialog box appears.

d. Click **Yes** to confirm the change.

10 Exit the GUI.

11 Update your site information with the modified external IP address for the RTC system node. To do this, perform the following steps:

a. Double-click the USP GUI icon to restart the GUI. The Login window appears.

b. Click **File>site-manager**.

c. Click the **site-name** list. A list of the valid site names appears.

d. Select the name of your system.

e. Enter the new external IP address in the **rtc-12-ipaddress** box.

f. Click **Modify** to save your modifications to the site information. A confirmation dialog box appears.

g. Click **Yes** to confirm the change.

12 Locate the LED beneath the slot that contains the RTC system node that you modified. When it turns green, log into your system. To do this, perform the following steps:

a. From the session-login screen (under **File>session-login**), select your system site from the Site list.

b. Enter your user account name in the **Login** box.

c. Enter your user account password in the **Password** box.

d. Click **Login**. The Login Transcript window appears, and logs the actions performed during the login operation.

13 Click **Configuration>platform>node**

14 Click **Graphical view**.

15 Double-click the RTC 12 or RTC 15 card on the control CAM shelf to open the RTC in the Administration panel.

16 Click **Unlock**. A confirmation dialog box appears.

17 Click **Yes** to confirm the change.

18 If you do not want to change the external IP address of the other RTC system node, proceed to step 19. If you want to change the external IP address of the other RTC system node, repeat steps 1 to 17 for that RTC system node. Once you have completed modification of the other RTC system node, proceed to step 19.

19 Perform a backup operation. To do this, perform the following steps:

a. Click **Administration> backup**.

b. Enter a description of the data snapshot in the **snapshot-description** box. You can enter up to 32 characters.

You can have the snapshot automatically transferred to the Alternate Boot Server and set as the active snapshot. You can also automatically delete snapshots on the RTC and Alternate Boot Server when the maximum is reached. See *USP Security and Administration* (NN10159-611).

c. Click **Create** to create the data snapshot. An hourglass appears while the current system configuration is being saved.

The Backup Status box at the bottom of the panel indicates when the data snapshot has been successfully saved on the active RTC system node. The data snapshot is named for the date and time of its creation.

ATTENTION
These files are large and can take several minutes to copy from an RTC to your alternate boot server.

d. Select the new snapshot with the ABS manager. See the Security and Administration guide for more information.

20 Log into your system.

21 Nortel Networks recommends that you delete any data snapshots from your system that were created before your modification of the RTC system node(s) to prevent the possibility of restoring your system using one of these older data snapshots. If you were to restore your system using one of these older data snapshots, you would lose communication with your OAMP workstations.

If you want to delete the older data snapshots, proceed to step 22. If you do not want to delete the older data snapshots, the procedure is complete.

22 Click **Administration>File-manager**.

23 Select a data snapshot that was created before your changes to the RTC system node(s) from the Snapshot folder in the Alternate Boot Server section of the window.

24 Click **Delete** to delete the data snapshot.

25 Repeat steps 23 and 24 for each data snapshot that was created before your changes to the RTC system node(s). Once you have deleted all the older data snapshots from the alternate boot server, proceed to step 26.

26 Select a data snapshot that was created before your changes to the RTC system node(s) from the Snapshot folder in the Destination portion of the window.

27 Click **Delete** to delete the data snapshot. This removes the data snapshot from the active RTC system node.

28 Repeat steps 26 and 27 for each data snapshot that was created before your changes to the RTC system node(s). Once you have deleted all the older data snapshots from the active RTC system node, proceed to step 29.

29 In the **RTC** list, select the inactive RTC system node.

30 Select a data snapshot that was created before your changes to the RTC system node(s) from the Snapshot folder in the **rtc** portion of the window.

31 Click **Delete** to delete the data snapshot. This removes the data snapshot from the inactive RTC system node.

32 Repeat steps 30 and 31 for each data snapshot that was created before your changes to the RTC system node(s). Once you have deleted all the older data snapshots from the inactive RTC system node, the step is complete.

If	Then
your system Remote Access Sever (RAS) is a Shiva LAN Rover	this procedure is complete
your system RAS is a Contivity 100	perform the procedure in step 33

33 Update the network address translation (NAT) tables on the Contivity 100. To do this, perform the following steps:

a. Establish a telnet connection to the Contivity 100.

b. Enter the administrator password and press the Enter key.

c. To update the NAT tables, type

```
nat add <ipaddressRTC12>:*
<ipaddressRTC12>:* ip
nat add <ipaddressRTC15>:*
<ipaddressRTC15>:*ip
commit
```

and press the Enter key. In this case, <ipaddressRTC12> and <ipaddressRTC15> are variables that should contain the new IP address.

d. Log out of the telnet session to the Contivity 100.

—End—

Modifying RTC System Node External Subnet Mask

When you modify the external subnet mask setting in the RTC system nodes, you must modify the subnet mask settings in your OAMP workstations and the Shiva Net Manager application.

ATTENTION

Changing the IP address information for a piece of equipment can result in that equipment becoming unavailable. Nortel Networks recommends that this procedure be performed by persons with a clear understanding of subnets and IP LANs. If you are changing any IP address settings, use the procedures in the General System Provisioning section.

Modification of the external subnet mask for the RTC system nodes should be performed from the OAMP workstation that is configured as an alternate boot server. Changing the subnet mask settings requires that you update the BOOTP server, which can only be done from the alternate boot server.

Modifying RTC System Node External Subnet Mask

Step	Action
	At the OAMP Workstation
1	Click **Configuration>platform>node**.
2	Click **Graphical view**.
3	Click the RTC 12 or RTC 15 card on the control CAM shelf to open the RTC in the Administration panel.
4	Enter the external subnet mask in the **ext-subnet-mask** box
5	Click **Modify** to save your modifications to the site information. A confirmation dialog box appears.
6	Click **Yes** to confirm the change.
7	You must load the RTC system node to re-initialize the site information. To do this, perform the following steps: a. If the RTC system node is inactive, proceed to step c. If the RTC system node is active, click **Swact**. A confirmation dialog box appears. b. Click **Yes** to confirm the change. c. If the RTC system node is locked, proceed to step e. If the RTC system node is not locked, click **Lock**. A confirmation dialog box appears. d. Click **Yes** to confirm the change. e. Click **Load**. A confirmation dialog box appears. f. Click **Yes** to confirm the change. g. Click **Unlock**. A confirmation dialog box appears. h. Click **Yes** to confirm the change.

8 Click **SWACT**. A confirmation dialog box appears.

9 Click **Yes** to confirm the change.

10 Repeat steps 1-9 for the newly inactive RTC system node.

11 To modify the subnet mask settings for the remote access server (RAS), perform the following steps:

a. Double-click the Shiva Net Manager icon on your desktop. The Device List window appears.

b. Double-click the device name for your local RAS in the list. The Enter Administrator Password window appears.

c. Enter the password in the Administrator Password box and click OK. The Configuration window appears.

d. In the Configure list, select IP General. The window changes to display the general IP address data for your local RAS.

e. Highlight the contents of the IP network mask box and enter the new subnet mask setting (it should match the subnet mask setting entered in step 4).

f. Click the Actions menu and select Set Configuration to save your changes to the IP address data.

A confirmation window may appear informing you that you must reset the RAS for all the changes to take effect. If this occurs, click OK. You may have to wait for a few minutes for the RAS to reset.

ATTENTION
Any active remote access sessions are terminated when you reset the local RAS.

g. Click the File menu and select Exit to close the Shiva Net Manager application.

ATTENTION
Steps 11 a-11 g must be repeated for any other OAMP workstations that use the local RAS.

12 To modify the subnet mask settings in your alternate boot server, perform the following steps:

a. Click BOOTP Server on the taskbar. The BOOTP Server window appears.

b. Log in to the server as the administrator by clicking the Configure menu, selecting Administrator, and then selecting Login. The BOOTP Login window appears.

c. Enter the administration password and click OK.

d. Click the Configure menu and select Server to display the Configure BOOTP window.

e. Select the Networks tab window.

f. Modify the setting in the Subnet Mask box by clicking the sliding scale below the box and adjusting the value (it should match the setting entered in step 4).

g. Click Modify to save the change.

h. Click OK to return to the BOOTP Server window.

i. End your administrative session on the BOOTP server. To do this, click the Configure menu, select Administrator, and then Logout.

j. Right-click the Network Neighborhood icon on your desktop and select Properties. The Network window appears.

k. In the Configuration tab window, select the TCP/IP network component for the Ethernet card in your alternate boot server.

l. Click Properties to display the TCP/IP Properties window.

m. In the IP Address tab window, select the contents of the Subnet Mask box and enter the new external subnet mask (Note: it should match the setting in step 4).

n. Click OK to close the TCP/IP Properties window and return to the Network window.

o. Click OK to close the Network window. You will be prompted whether you want to restart your computer to make the new settings take effect.

p. Click Yes to restart your alternate boot server.

ATTENTION

Steps 12 j-12 p must be repeated for each OAMP workstation configured for your system.

13 Once you have completed the re-configuration of your OAMP workstations, return to your alternate boot server and double-click the USP GUI icon to display the Login window.

14 Log in to your system.

15 Perform a backup operation. To do this, perform the following steps:

a. Click **Administration> backup**.

b. Enter a description of the data snapshot in the **Snapshot-description** box. You can enter up to 32 characters.

You can have the snapshot automatically transferred to the Alternate Boot Server and set as the active snapshot. It is also possible to automatically delete snapshots on the RTC and Alternate Boot Server when the maximum is reached. See *USP Security and Administration* (NN10159-611).

c. Click **Create**.

d. Select the new snapshot with the ABS manager. See the Security and Administration guide for more information.

16 Nortel Networks recommends that you delete any data snapshots from your system that were created before your modification of the subnet mask settings to prevent the possibility of restoring your system using one of these older data snapshots.

If you were to restore your system using one of these older data snapshots, you would lose communication with your OAMP workstations.

If you want to delete the older data snapshots, proceed to step 17. If you do not want to delete the older data snapshots, the procedure is complete.

17 Click **Administration>File-manager**.

18 Select a data snapshot that was created before your changes to the subnet mask settings from the Snapshot box in the Source portion of the window.

19 Click **Delete** to delete the data snapshot.

20 Repeat steps 18 and 19 for each data snapshot that was created before your changes to the subnet mask. Once you have deleted all the older data snapshots from the alternate boot server, proceed to step 21.

21 Select a data snapshot that was created before your changes to the subnet mask settings from the Snapshot folder in the **rtc** portion of the window.

22 Click **Delete** to delete the data snapshot. This removes the data snapshot from the active RTC system node.

23 Repeat steps 21 and 22 for each data snapshot that was created before your changes to the subnet mask. Once you have deleted all

the older data snapshots from the active RTC system node, proceed to step 24.

24 In the **rtc** list, select the inactive RTC system node.

Select a data snapshot that was created before your changes to the subnet mask settings from the Snapshot folder in the rtc portion of the window.

25 Click **Delete** to delete the data snapshot. This removes the data snapshot from the inactive RTC system node.

26 Repeat steps 24 and 25 for each data snapshot that was created before your changes to the subnet mask settings. Once you have deleted all the older data snapshots from the inactive RTC system node, the procedure is complete.

If	Then
your system RAS is a Shiva LAN Rover	this procedure is complete
your system RAS is a Contivity 100	perform the procedure in step 27

27 Update the network address translation (NAT) tables on the Contivity 100. To do this, perform the following steps:

a. Establish a telnet connection to the Contivity 100.

b. Enter the administrator password and press the Enter key.

c. To update the subnet, type

```
ifconfig eth1 ipaddress <ipaddressRAS> <subnetmask>

commit
```

and press the Enter key. In this case, <ipaddressRAS> and <subnetmask> are variables that should contain the IP addresses for the Contivity 100 and subnet mask.

d. Log out of the telnet session to the Contivity 100.

—End—

Modifying RTC System Node External Gateway Address

When you modify the external gateway address setting in the RTC system nodes, you must modify the gateway address settings in your OAMP workstations, the Shiva Net Manager or Contivity 100 application, and the

network ping initialization file. Modification of the external gateway address for the RTC system node should be performed from the OAMP workstation that is configured as an alternate boot server.

ATTENTION

Changing the IP address information for a piece of equipment can result in that equipment becoming unavailable. Nortel Networks recommends that this procedure be performed by persons with a clear understanding of subnets and IP LANs. If you are changing any IP address settings, use the procedures in the General System Provisioning section of this document.

Modifying RTC System Node External Gateway Address

Step	Action
	At the OAMP Workstation
1	Click **Configuration>platform>node**.
2	Click **Graphical view**.
3	Double-click the RTC 12 or RTC 15 card on the control CAM shelf to open the RTC in the Administration panel.
4	Enter the new external gateway address in the **ext-gateway** box.
5	Click **Modify** to save your modifications to the site information. A confirmation dialog box appears.
6	Click **Yes** to confirm the change.
7	You must load the RTC system node to re-initialize the site information. To do this, perform the following steps: a. If the RTC system node is inactive, proceed to step e. If the RTC system node is active, click **Swact**. A confirmation dialog box appears. b. Click **Yes** to confirm the change. c. If the RTC system node is locked, proceed to step e. If the RTC system node is not locked, click **Lock**. A confirmation dialog box appears. d. Click **Yes** to confirm the change. e. Click **Load**. A confirmation dialog box appears. f. Click **Yes** to confirm the change. g. Click **Unlock**. A confirmation dialog box appears. h. Click **Yes** to confirm the change.

8 Repeat steps 1-7 for the newly inactive RTC system node.

9 Modify the gateway address settings for the RAS. To do this, perform the following steps:

If	Go to
your system RAS is a Shiva LAN Rover	step 10
your system RAS is a Contivity 100	step 11

10 If your system RAS is a Shiva LAN Rover, perform the following steps. When you finish the procedure in step 10, continue to step 12.

a. Double-click the Shiva Net Manager icon on your desktop. The Device List window appears.

b. Double-click the device name for your local RAS in the list. The Enter Administrator Password window appears.

c. Enter the password in the Administrator Password box and click OK. The Configuration window appears.

d. In the Configure list, select IP General. The window changes to display the general IP address data for your local RAS.

e. Highlight the contents of the IP address of device and IP address of default router boxes and enter the new gateway address setting (it should match the gateway address setting entered in step 4).

f. If the IP addresses for the ports have changed as well proceed to step 10 g. If the IP addresses for the ports have not changed, proceed to step 10 m.

g. Select IP Addresses from the Configure list. The window changes to display the IP address assignment and pool data for your local RAS.

h. Click the IP address in the list in the IP Address Pool portion of the window.

i. Click Remove.

j. Enter the new IP address of the first port on the local RAS in the Starting address box.

k. Enter the number of ports equipped on the RAS in the Range count box.

l. Click Add.

m. Click the Actions menu and select Set Configuration to save your changes to the IP address data. A confirmation window may appear informing you that you must reset the RAS for all the changes to take effect. If this occurs, click OK. You may have to wait for a few minutes for the RAS to reset.

ATTENTION
Any active remote access sessions are terminated when you reset the local RAS.

n. Click the File menu and select Exit to close the Shiva Net Manager application

ATTENTION
Steps 10 a-10 n must be repeated for any other OAMP workstations that use the local RAS.

11 If your system RAS is a Contivity 100, perform the following procedure. When you complete the procedure in step 11, continue to step 12.

a. Establish a telnet session to the Contivity 100.

b. Enter the administrator password and press **Enter**.

c. To change the gateway, enter the following command:

```
route add default eth1 <gateway>

commit
```

and press the Enter key. In this case <gateway> is a variable that should contain the name of the new gateway.

ATTENTION
The routing changes can take up to two minutes. During this time, workstations on other subnets may not be able to access the RTC. Workstations on the same subnet are not affected.

d. Quit the telnet session.

12 Modify the gateway address settings in your alternate boot server. To do this, see the Security and Administration guide for the procedure to modify Gateway IP addresses.

13 Once you have completed re-configuring your OAMP workstations, return to your alternate boot server and double-click the USP GUI icon.

14 Log in to your system.

15 Click **Configuration>platform>node**.

16 Click **Graphical view**.

17 Double-click the RTC 12 or RTC 15 card on the control CAM shelf to open the RTC in the Administration panel.

18 Perform a backup operation. To do this, perform the following steps:

a. Click **Administration> backup**.

b. Enter a description of the data snapshot in the **snapshot-description** box. You can enter up to 32 characters.

You can have the snapshot automatically transferred to the Alternate Boot Server and set as the active snapshot. It is also possible to automatically delete snapshots on the RTC and Alternate Boot Server when the maximum is reached. See *USP Security and Administration* (NN10159-611).

c. Click **Create**.

d. Select the new snapshot with the ABS manager. See the Security and Administration guide for more information.

19 Nortel Networks recommends you delete any data snapshots from your system created before your modification of the gateway address to prevent the possibility of restoring your system using one of these older data snapshots. If you were to restore your system using one of these older data snapshots, you can affect communication with your local RAS.

To delete the older data snapshots, proceed to step 20. If you do not want to delete the older data snapshots, the procedure is complete.

20 Click **Administration>file-manager**.

21 Select a data snapshot created before your changes to the gateway address from the Snapshot box in the Source portion of the window.

22 Click **Delete** to delete the data snapshot.

23 Repeat steps 21 and 22 for each data snapshot created before your changes to the gateway address. Once you have deleted all the older data snapshots from the alternate boot server, proceed to step 24.

24 Select a data snapshot created before your changes to the RTC system node(s) from the Snapshot folder in the **rtc** portion of the window.

25 Click **Delete** to delete the data snapshot. This removes that data snapshot from the active RTC system node.

26 Repeat steps 24 and 25 for each data snapshot created before your changes to the gateway address.

Once you have deleted all the older data snapshots from the active RTC system node, proceed to step 27.

27 In the **rtc** list, select the inactive RTC system node.

28 Select a data snapshot created before your changes to the gateway address from the Snapshot folder in the **rtc** portion of the window.

29 Click **Delete** to delete the data snapshot. This removes that data snapshot from the inactive RTC system node.

30 Repeat steps 28 and 29 for each data snapshot created before your changes to the gateway address. Once you have deleted all the older data snapshots from the inactive RTC system node, the procedure is complete.

—End—

Replacing an RTC card

Use this procedure to replace an RTC mission card. Configuration of the BOOTP settings for the new RTC card should be performed from the OAMP workstation or Solaris machine that is configured as an alternate boot server.

A USP snapshot should be taken prior to any maintenance activity to ensure that a most recent backup of the data is available.

Backing up the system and ABS testing

Step	Action

At the OAMP Workstation

1 Click **Administration>backup**.

2 Enter a description of the data snapshot in the **snapshot-description** box. You can enter up to 32 characters.

ATTENTION

You can have the snapshot automatically transferred to the Alternate Boot Server and set as the active snapshot. This is recommended. If this option is not available proceed to the File Manager menu to copy the snapshot to the ABS. See the *USP Security and Administration* (NN10159-611) for more information.

3 Click **Create** to create the data snapshot. An hourglass appears while the current system configuration is being saved.

The Backup Status box at the bottom of the panel indicates when the data snapshot has been successfully saved on the active RTC system node. The data snapshot is named for the date and time of its creation.

4 Click **Close** to close the Backup Active RTC window and return to the Administration window.

5 Select the new snapshot with the ABS manager. See the *USP Security and Administration* (NN10159-611) for more information.

6 Click **Administration>alternate-boot-server**.

7 Click **Test** to perform the ABS test.

8 Click on **Logs** from the Fault menu to retrieve the results of the ABS test. A successful test message will prove that the connection to the alternate boot server was established correctly.

—End—

Configuring the BOOTP settings if using Windows ABS

Step	Action

At the OAMP Workstation

1 Click **Distinct BootP Server** on the taskbar. The Distinct BOOTP Server window appears.

2 Log in to the server as the administrator by clicking the Configure menu, selecting Administrator, and then selecting Login. The BOOTP Login window appears.

3 Enter the administration password and click OK.

4 Click the **Configure** menu and select **Server** to display the Configure BOOTP window.

5 Click on the MAC address for the card to be replaced and remove it.

6 Click **Add** and enter the new MAC address and the boot file location in the Boot File field.

7 End your administrative session on the BOOTP server. To do this, click the Configure menu, select Administrator, and then Logout.

—End—

Configuring the BOOTP settings if using Solaris ABS

Step	Action

From an xterm or telnet prompt

> ***ATTENTION***
> *Ensure that your Telnet client supports the use of the backspace key, which is required in the event of a typing error. An option is to enter "stty erase <Backspace>" after logging into the CMT.*

1 Type the following to access commands for the ABS server:

```
cli
```

2 From the menu displayed, select **2** for configuration.

3 Select 11 for BOOTP configuration.

4 Select **3** for a list of BOOTP entries.

5 Select **2** to delete a BOOTP entry.

You are prompted to enter the hardware address [ha] associated with the BOOTP entry to be deleted.

6 Type the MAC address of the card to be removed and press Enter.

7 Type **ok** to confirm and press Enter.

The following message appears

```
==="bootp_del" completed successfully
```

8 Select **3** to list the BOOTP entries and ensure the entry deleted is no longer on the list.

9 Select **1** to add a BOOTP entry.

You are prompted for the hardware address (ha) of the RTC card to be added.

10 Enter the hardware address (MAC address) of the card to be added/replaced.

11 Enter the location of the boot file [bf] for the BOOTP entry. For example:

```
/data/usp/ntssgusp/abs/sites/<sitename>/rtc 1/rtcboot
```

12 Enter the gateway [gw] IP address for the BOOTP entry.

13 Enter the home directory [hd] location for the BOOTP entry.

ATTENTION
Typing a period (.) makes the current directory the default. This is recommended.

14 Enter the hardware type [ht] for the BOOTP entry.

If you have an Ethernet cable connected to the RTC, the [ht] is usually Ethernet.

15 Enter the MAC address of the RTC card as the [ha] for the BOOTP entry.

16 Enter the IP address of the RTC being replaced as the host IP address [ip] for the BOOTP entry.

17 Enter the IP address of the Solaris ABS machine as the server IP address [sa] for the BOOTP entry.

18 Enter the subnet mask [sm] value for the BOOTP entry. For example:

```
255.255.255.0
```

The settings are printed on the screen.

19 If all the settings are correct, type **ok** to confirm the settings and press Enter.

The following message appears:

```
==="bootp_add" completed successfully
```

—End—

Replacing the RTC card

Step Action

CAUTION
Wear wrist straps and use standard antistatic precautions.

1

At the OAMP workstation

2 Before replacing any cards, press all the Lamp Test buttons on the front and rear of the CAM shelf to ensure all the LEDs are working properly.

3 Click **Configuration>platform>node**.

4 Click **Graphical view**.

5 Double-click the slot of the card to be replaced on the control CAM shelf.

6 Check the **activity-state** to ensure the card to be replaced is inactive.

7 If the card is active, click **Swact** to change the **activity-state**. After the SWACT is complete, wait at least 15 minutes before proceeding to the next step.

8 If Swact was performed, check the status again to ensure that the card is now inactive.

9 Lock the RTC system node by clicking the **Lock** button. A confirmation dialog box appears.

10 Click **Yes** to confirm the change.

11 Click **Offline**. A confirmation dialog box appears.

12 Click **Yes** to confirm the change.

13 Click **Graphical View** from Configuration>platform>node. The RTC to be replaced should now have an amber light, not green.

14 Remove the offline RTC card from the slot and insert the replacement RTC card.

   a. Before you unseat an RTC, remove the screws that fasten it to the slot in the shelf. Ensure that if a separate SCSI card is being used in slot 16, the SCSI light is not lit at the time the RTC card is pulled.

   b. Press outward on the top and bottom latches of the RTC card to release it from the CAM shelf.

   c. Grasp the top and bottom latches of the RTC card and gently pull it toward you to remove it from the CAM shelf.

   d. Insert the new card into the CAM shelf and use the screws to fasten it to the slot.

15 In the Graphical View (under Configuration>platform>node), click on the slot for the newly replaced card and click **Load**. Click **Yes** to confirm.

16 Watch the USP logs for beginning and ending "RTC Database Synchronization" logs that should appear in 10 minutes time. If you do not see these logs in this time frame, an alternate boot may be necessary.

17 If activity state on RTC changes to enabled, click **Unlock** to unlock the RTC. A confirmation dialog box appears.

18 Click **Yes** to confirm the change.

19 At the front of the CAM shelf, ensure the LED under the RTC is a solid green light.

20 You have completed this procedure.

—End—

Configuring a Network Element System Node

You can perform provisioning and maintenance operations for nodes in the node provisioning and maintenance window. This window has three sections: Provisioning data, Operational data, and Boot data.

The Provisioning data section contains:

- type and name of the system node
- a description of the system node
- product engineering codes (PECs) for the related hardware (Front and TM [Transition Module]) and other card specific values

  For the node having a Ethernet Interfaces (e.g. RTC, NPC, etc.) the following information is also included:

  — external IP address

  — external subnet mask

  — external gateway IP address

ATTENTION

The serial numbers and manufacturer information for the related hardware is available using the Search tab. By right clicking in the grid, select customize... From there you can add additional fields that are displayed for the hardware. Serial number of Front and TM can be selected.

The Operational Data section provides you with the state and status information for the system node.

The Boot Data section contains the following information:

- name of the related boot image
- name of the related HA boot image (if applicable)
- currently running image file
- status messages

Adding a System Node

CAUTION

Do not provision a new system node while the inactive RTC system node is disabled. You can cause software errors to be reported or data to be lost. You should not provision a new system node while the USP system has critical alarms active.

ATTENTION

To add an extension CAM shelf to your system, you need to initially provision the CC system nodes on the extension CAM shelf. You must provision both CC system nodes before you can provision any application system nodes on an extension CAM shelf. To provision an extension CAM shelf, the CC system nodes on the control CAM shelf must be provisioned with the correct CC card type for a dual-shelf system. The correct PEC is NTST02AB or NTST02BA.

To add a system node, perform the following steps:

Step	Action
	At the OAMP Workstation
1	Click **Configuration>platform>node**.
2	Click **Graphical view**.
3	Double-click the desired empty slot to open it in the administration panel.

ATTENTION

RTC nodes are restricted to slot 12 and 15 of the CAM Control Shelf. Slot 13 and 16 of the CAM Control Shelf are reserved for the RTC Disk drive, and they are provisioned when the RTCs are provisioned.

Slot 1 and 18 of any shelves are reserved for the CAM Controller (CC) nodes.

All other Nodes can occupy slot 2 to 11, 14 and 17 of the CAM Control shelf or slot 2 to 17 of an Extension shelf.

4 Select the slot type from the slot-type drop-down list. A confirmation dialog box appears. The available slot types are:

- rtc: See the RTC System Node Provisioning and Maintenance section of this document for information about how to provision a Real Time Controller.
- usp-compact: This node is used in Carrier Voice over IP CS2K compact applications and is not supported on the USP.
- cc: CAM Controller node
- lslink: Low-speed Link node, either DS-0A or V.35
- Iplink: IPS7 Gateway Node used for M3UA applications
- ss7iplink: IP High-speed Link node using M2PA, M3UA, and M2UA over SCTP
- atmhslink: ATM High-speed Link over T1 or E1 interfaces
- chanlslink: Channelized E1 supporting up to 4 SS7 channels

- multi-chanlslink: Channelized E1 or T1 supporting up to 8 SS7 channels
- mtp2hslink: MTP Level 2 High-speed Links
- npc: Number Portability Controller
- nps: Number Portability Server
- npe: Number Portability Extension
- llc: Low Layer Controller
- lls: Low Layer Server

NPC, NPS, LLC, and LLS nodes cannot be provisioned in slots 14 and 17 of the control shelf because their SCSI disk must exist in an adjacent slot.

NPC and LLC system nodes work in mated pairs. Both the NPC system nodes must be provisioned in the same CAM shelf. The USP has a limit of two NPC or LLC system nodes per system.

NPC, NPS, LLC, and LLS system nodes require two adjacent slots. The slot in which you attempt to provision an NPC, NPS, LLC, or LLS system node must have an empty slot to its immediate right in order for the system to permit you to perform provisioning.

NPS system nodes can be provisioned when your USP already has two NPC system nodes provisioned. The USP has a limit of four NPS system nodes per system.

NPE system nodes are configured in logical chains that are associated with NPC, NPS, LLC, or LLS cards. The USP supports four NPEs for each chain and one chain for each card, for a maximum of 24 NPE nodes for each system.

5 Click **Yes** to confirm the change.

6 Enter the name of the system node, up to 32 characters, in the **slot-name** box.

ATTENTION

Nortel suggests that the system node name should contain information that indicates the system name, shelf name, function (CC system node), and slot number.

7 Enter the description of the system node in the **slot-description** box. You can enter up to 32 characters.

The shelf and slot box are automatically filled when entering the Administration panel by double clicking a slot from the Graphical View.

8 For iplink, ss7iplink, npc, llc, or lls, enter the **ext-ip-address**, **ext-subnet-mask**, and **ext-gateway**. The external gateway address is the address of the gateway to use when the destination IP address is not in the IP link system node subnet.

9 For multi-chanlslink or atmhslink, select either **t1** or **e1** mode from the **t1-e1-mode** drop-down list.

10 Select the PEC for the mission card from the **front-pec** drop-down list.

11 Select the PEC of the TM from the **tm-pec** drop-down list.

The **tm-type** box shows the type of TM based on the tm-pec selection.

12 For npc and nps node, select the SCSI disk front pec in the **scsi-front-pec** drop-down list.

13 Select the boot image file for the node from the **boot-image** drop-down box. These files are stored on the SCSI disk drive associated with the active RTC system node.

14 For lslink, atmhslink, chanlslink, multi-chanlslink, and mtp2hslink, select the **HA boot image** file for the system node from the **ha-boot-image** drop-down list.

15 Click **Add**.

—End—

Loading a Node

You must load the system node to download the boot image file.

Step	Action
	At the OAMP workstation
1	Click **Configuration>platform>node**.
2	Click **Graphical view**.
3	Double click the slot to open it in the administration panel.

ATTENTION

Any local subsystem (LSS) instances associated with an NPx system node must be deactivated before you can lock an NPx system node.

4 If the system node is locked, proceed to step 6. If the system node is not locked, click **Lock**. A confirmation dialog box appears.

5 Click **Yes** to confirm the change.

6 If the system node is offline, proceed to step 8. If the system node is not offline, click **Offline**. A confirmation dialog box appears.

7 Click **Yes** to confirm the change.

8 Click **Load**. A confirmation dialog box appears.

9 Click **Yes** to confirm the change.

10 Once the card is loaded, click **Unlock**. A confirmation dialog box appears.

11 Click **Yes** to confirm the change.

—End—

Viewing Node Provisioning Data

To view node provisioning data, perform the following steps:

Step	Action
	At the OAMP Workstation
1	Click **Configuration>platform>node**.
2	Click **Graphical view**.
3	Double click the desired slot to open it in the administration panel and view the node configuration data.

—End—

Modifying Node Provisioning Data

CAUTION
Do not make any provisioning changes to a node while the inactive RTC system node is disabled. You can cause software errors to be reported or data to be lost.

Do not make provisioning changes to system nodes while the USP system has active critical alarms.

If you modify the external IP address setting for IPlink, SS7iplink, NPC, LLC, or LLS system nodes, you must update the settings on the external provisioning system (for example, LSMS).

If you modify the external subnet mask setting for IPlink, SS7iplink, NPC, LLC, or LLS system nodes, you may have to update the settings on the external provisioning system, if it is on the same subnet.

To modify system nodes, perform the following steps:

ATTENTION
To modify an NP or LL system node, refer to the Modifying NPx or LLx Node Provisioning Data.

Step	Action

At the OAMP Workstation

1 Click **Configuration>platform>node**.

2 Click **Graphical view**.

3 Double click the desired slot to open it in the administration panel and view the node configuration data.

Fields that cannot be modified are grayed out.

ATTENTION
Any LSS instances associated with an NPx or LLx system node must be deactivated before you can lock the system node.

4 Make the required changes to the fields associated with this node.

5 Click **Modify**. A confirmation dialog box appears.

ATTENTION
If you have selected a new boot image file, PEC, SCSI PEC, IP address, Subnet mask, or gateway you must perform the procedure, "Loading a Node" (page 81). If you did not select any of these items, the procedure is complete.

6 Click **Yes** to confirm the change.

—End—

Deleting a Node

To delete a node, perform the steps below:

Any provisioning data (e.g. links) using this node must be deleted prior to deleting a node. To determine if a link is associated with this node, you can use Retrieve related records button (located in the command bar to the immediate left of the Help button) and select the mtp link table. This will bring you to the Search panel of mtp link table and will display any links associated with this node.

Before you can delete an NPx or LLx system node, you must delete any NPx or LLx local subsystem instances that refer to that system node. For an NPE system node, you must also remove that NPE from the NPE chain and perform a bulk load to redistribute the records in the NPx database.

Step	Action
	At the OAMP Workstation
1	Click **Configuration>platform>node**.
2	Click **Graphical view**.
3	Double-click the card that you want to delete. This brings you to the Administration panel.
4	If the node is locked, proceed to step 6. If node is unlocked, click **Lock**. A confirmation dialog box appears.
5	Click **Yes** to confirm the change.
6	If the node is offline, proceed to step 8. If node is not offline, click **Offline**. A confirmation dialog box appears.
7	Click **Yes** to confirm the change.
8	Click **Delete**. A confirmation dialog box appears.

ATTENTION
The system does not allow you to delete CC system nodes on your control CAM shelf.

9	Click **Yes** to confirm the change.

—End—

Performing Maintenance Activities on NP or LL Nodes

The following system nodes are part of the hardware that supports the Universal Number Portability Master (UNPM) and Service Location Register (SLR) applications:

- Number Portability Controller (NPC)
- Number Portability Server (NPS)
- Number Portability Extension (NPE)

ATTENTION

Throughout this procedure, an NPx means NPC, NPS, or NPE system node. LLx means LLC or LLS.

The following system nodes are part of the hardware that supports the Low Layer Control Point (LLCP):

- Low Layer Server (LSS)
- Low Layer Controller (LLC)

This section provides the state and status information for the NPx or LLx system node. It also contains fields that identify the currently running image file and provide status messages. In addition, this section contains buttons that you can use to perform various maintenance operations

The table that follows indicates the availability of the NPx or LLx system node maintenance buttons in relation to the node states.

Maintenance operations buttons available

	Enabled		Disabled		
Button	**Locked**	**Unlocked**	**Locked**	**Locked & Offline**	**Unlocked**
Diagnostics	N/A	N/A	N/A	N/A	N/A
SWACT (NPC and LLC only)	Yes	Yes	No	No	No
Load	Yes	No	Yes	Yes	Yes
Lock	No	Yes	No	No	Yes
Unlock	Yes	No	Yes	No	No
Offline	Yes	No	Yes	No	No

You can perform the following maintenance activities on an NPx or LLx system node:

- switch activity (SWACT) NPC or LLC only
- lock

- unlock
- offline
- load
- viewing NPx or LLx system node alarms

ATTENTION
You cannot perform maintenance activities on an NPx or LLx system node on an extension CAM shelf while the extension CAM shelf is in isolation.

Manual SWACT Operation on the NPC or LLC System Nodes

The active NPC or LLC system nodes handle all system processing and store a record of all system data. The inactive NPC or LLC system node acts as a backup, and when it is enabled, it is ready to assume the active role at any time. The SWACT operation switches the active and inactive system nodes.

The system performs automatic SWACT operations when

- you lock the active NPC or LLC while the inactive system node is unlocked and enabled
- the active NPC fails

To perform a manual SWACT operation, both NPC and LLC system nodes must be in the same availability state (locked or unlocked) and enabled.

To switch the active NPC or LLC system node manually, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>platform>node**.
2	Click the **Graphical View** tab.
3	Double-click the slot for the system node you wish to Swact.
4	Click **Swact**. A confirmation dialog box appears.
5	Click **Yes** to confirm the change.

—End—

Lock Operation

You must lock an NPx or LLx system node in order to perform system node maintenance operations, except for SWACT.

ATTENTION
Any LSS instances associated with the NPx or LLx system node must be deactivated before you can lock the system node.

CAUTION
To lock an NPC or LLC system node, the mated system node in the CAM shelf must be unlocked and enabled. Locking the active system node causes an automatic SWACT operation to be performed.

To lock an NPx or LLx system node, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>platform>node**.
2	Click the **Graphical View** tab.
3	Double-click the slot for the system node you wish to lock.
4	Click **Lock**. A confirmation dialog box appears.
5	Click **Yes** to confirm the change.

—End—

Unlock Operation

To unlock an NPx or LLx system node, at least one of the CC system nodes in the same shelf must be unlocked and enabled. A locked system node can be unlocked, as long as it is not offline as well.

To unlock an NPx or LLx system node, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>platform>node**.
2	Click the **Graphical View** tab.
3	Double-click the slot for the system node you wish to unlock.
4	Click **Unlock**. A confirmation dialog box appears.
5	Click **Yes** to confirm the change.

—End—

Offline Operation

You must take an NPx or LLx system node offline before replacing any of its hardware.

To take an NPx or LLx system node offline, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>platform>node**.
2	Click the **Graphical View** tab.
3	Double-click the slot for the system node you wish to Offline.

If the NPx system note is	Go to
locked	step 6
unlocked	step 4

4	Click **Lock**. A confirmation dialog box appears.
5	Click **Yes** to confirm the change.
6	Click **Offline**. A confirmation dialog box appears.
7	Click **Yes** to confirm the change.

—End—

Load Operation

Perform a load operation to download the boot image and re-initialize an NPx or LLx system node. Only a locked system node can be loaded.

To load an NPx or LLx system node, complete the following steps:

Step	Action
	At the OAMP workstation:
1	Click **Configuration>platform>node**.
2	Click the **Graphical View** tab.

3 Double-click the slot for the system node you wish to Load.

If the NPx system node is	Go to
locked	step 6
unlocked	step 4

4 Click **Lock** in the Maintenance portion of the window. A confirmation dialog box appears.

5 Click **Yes** to confirm the change.

6 Click **Load** to download the boot image and re-initialize and enable the NPx system node. A confirmation dialog box appears.

7 Click **Yes** to confirm the change.

—End—

Configuring Ports

Port configuration represents configuration of the physical port terminating on a link node (e.g. V.35, DS-0A, E1, T1, etc.). Port configuration is automatically provisioned when the node is provisioned.

Change the V.35 mode between DTE and DCE

Each of the four ports on a V.35 Transition Module can be configured as either DTE (data terminal equipment) or DCE (data communications equipment) by changing the orientation of the hardware plug-in module associated with each port. A V.35 signaling link configured as DCE provides the clocking for link data at either 56Kbps or 64Kbps. A V.35 signaling link configured as DTE derives clocking from the V.35 interface signals. That means that the setting of the data transmission rate of a V.35 port configured as DTE has no effect on the actual link speed. The data transmission rate setting of a V.35 port configured as DTE is used by the system for computations based on link speed, such as BERT. If the data transmission rate setting is incorrect for a V.35 port configured as DTE, it does not affect the operation of the port. However, it can result in inaccurate BERT calculations.

CAUTION
Wear wrist straps, and use standard antistatic precautions.

Modifying the V.35 mode between DTE and DCE

Step	Action
	At the OAMP workstation
1	Click **Configuration>platform>node**.
2	Click **Graphical view**.
3	Double-click the icon for the V.35 link system node you are changing. Note the slot and shelf you are changing.
4	Click **Lock**. A confirmation dialog box appears.
5	Click **Yes** to confirm the change.
6	Click **Offline**. A confirmation dialog box appears.

7 Click **Yes** to confirm the change.

8 Before you remove the TM, remove the connector(s) attached to it by unscrewing the thumbscrews on the top and bottom of each connector. Gently pull off the cable connector(s) for the TM.

9 Press outward on the top and bottom latches of the TM to release it from the shelf. Two audible clicks can be heard when the TM is released completely.

10 Grasp the top and bottom latches of the TM and gently pull it toward you to remove it from the shelf.

11 Locate the plug-in module on the TM associated with the port that you want to configure.

ATTENTION
The default settings for a V.35 TM are DTE with a data transmission speed of 56Kbps.

12 The lower edge of the TM card contains the text DTE/DCE and an arrow. Each plug-in module is labelled DCE on one end and DTE on the other end. The orientation of each plug-in module with respect to the arrow on the TM card determines the operational mode of the associated port. Unplug the module associated with the port that you want to configure. Plug the module back into the TM card. Keep the correct end, DTE or DCE, aligned with the arrow on the TM card.

13 Position the top and bottom latches of the V.35 TM and gently slide the TM into the card guide, seating the bottom of the TM into the card guide and then the top.

14 Apply pressure to the faceplate until you feel resistance.

15 Snap the top and bottom latches of the TM inward, toward one another. Clicks are audible when the TM is seated properly.

16 After you reseat the TM, plug in its TM connector(s) and turn the thumbscrews on the top and bottom of the connector(s) to tighten.

17 From the front or rear of the CAM shelf, press the Lamp Test button. If the LEDs do not turn on for the system node you just configured, ensure the TM is seated properly by completing steps 8-16 again.

18 Click **Load**. A confirmation dialog box appears.

19 Click **Yes** to confirm the change.

20	Once loaded click **Unlock**. A confirmation dialog box appears.
21	Click **Yes** to confirm the change.

—End—

V.35 ports

Perform the following steps to change the configuration of a V.35 port.

Configuring V.35 ports

Step	Action
	At the OAMP workstation
1	Click **Configuration>platform>port**.
2	Click the **Search** panel tab, click the **Retrieve** button (located in the command bar to the immediate left of the **Help** button), and locate the V.35 port you want to modify. Double-click the V.35 port to open it in the Administration panel.
3	Click **Configuration>platform>node**. (You can leave the port window open in the background.)
4	Click **Graphical View**.
5	Double-click the icon for the link system node you are changing.
6	Click **Lock**. A confirmation dialog box appears.
7	Click **Yes** to confirm the change.
8	Click **Offline**. A confirmation dialog box appears.
9	Click **Yes** to confirm the change.
10	In the port window, select the new port speed in the **port-speed** drop-down list. Port speeds of 56 kb/s and 64 kb/s are supported.
11	Click **Modify**. A confirmation dialog box appears.
12	Click **Yes** to confirm the change.
13	In the node window, click **Load**. A confirmation dialog box appears.
14	Click **Yes** to confirm the change.

15 Click **Unlock**. A confirmation dialog box appears.

16 Click **Yes** to confirm the change.

—End—

DS-0 ports

DS-0 port configuration cannot be modified since there is only one supported configuration for this type of link. It can be viewed by performing the following steps.

Viewing DS-0 ports

Step	Action
	At the OAMP workstation
1	Click **Configuration>platform>port**.
2	Click the **Search** panel tab, click the **Retrieve** button (located in the command bar to the immediate left of the Help button), and locate the DS-0A port you want to modify. Double-click the DS-0A port to open it in the Administration panel.

—End—

4 channelized link ports

Perform the following steps to change the configuration of the E1 port used for the 4 channelized link node (node defined as chanlslink).

ATTENTION
There is also an 8-channel option with a multi-chanlslink node type.

Configuring 4 channelized link ports

Step	Action
	At the OAMP workstation
1	Click **Configuration>platform>port**.
2	Click the **Search** panel tab, click the **Retrieve** button (located in the command bar to the immediate left of the **Help** button) and locate the 4 channelized link port you want to modify. Double-click the port to open it in the Administration panel.

3 Click **Configuration>platform>node**. (You can leave the port window open in the background.)

4 Click **Graphical View**.

5 Double-click the icon for the link system node you are changing.

6 Click **Lock**. A confirmation dialog box appears.

7 Click **Yes** to confirm the change.

8 Click **Offline**. A confirmation dialog box appears.

9 Click **Yes** to confirm the change.

10 In the port window, the only field that can be changed is the clocking mode field. Select a new clocking mode value from the **clocking-mode** drop-down list.

11 Click **Modify**. A confirmation dialog box appears.

12 Click **Yes** to confirm the change.

13 In the node window, click **Load**. A confirmation dialog box appears.

14 Click **Yes** to confirm the change.

15 Click **Unlock**. A confirmation dialog box appears.

16 Click **Yes** to confirm the change.

—End—

8 channelized link ports

Perform the following steps to change the configuration of the E1 or T1 port used for the 8 channelized link node (node defined as multi-chanlslink).

ATTENTION
There is also a 4-channel option with a chanlslink node type.

Configuring 8 channelized link ports

Step	Action
	At the OAMP workstation

1 Click **Configuration>platform>port**.

2 Click the **Search** panel tab, click the Retrieve **button** (located in the command bar to the immediate left of the **Help** button), and locate the 8 channelized link port you want to modify. Double-click the port to open it in the Administration panel.

3 Click **Configuration>platform>node**. (You can leave the port window open in the background.)

4 Click **Graphical View**.

5 Double-click the icon for the link system node you are changing.

6 Click **Lock**. A confirmation dialog box appears.

7 Click **Yes** to confirm the change.

8 Click **Offline**. A confirmation dialog box appears.

9 Click **Yes** to confirm the change.

10 In the port window, to change the clocking mode, select a new value from the **clocking-mode** drop-down list.

11 For an E1 port, select a new CRC4 interworking mode from the **crc4-interworking** drop-down list.

12 For a T1 port, the following fields can be modified:

- select a new value in the **line-length-equalization** drop-down list
- select a new value in the **framing-format** drop-down list. T1 framing format is either ESF (Extended Super Frame) or SF (Super Frame).
- select a new value in the **line-code** drop-down list. T1 line format are either B8ZS or AMI.

13 Click **Modify**. A confirmation dialog box appears.

14 Click **Yes** to confirm the change.

15 In the node window, click **Load**. A confirmation dialog box appears.

16 Click **Yes** to confirm the change.

17 Click **Unlock**. A confirmation dialog box appears.

18 Click **Yes** to confirm the change.

—End—

MTP2 high-speed link ports

Perform the following steps to change the E1 MTP Level High-speed Link.

Configuring MTP2 high-speed link ports

Step	Action
	At the OAMP workstation
1	Click **Configuration>platform>port**.
2	Click the **Search** panel tab, click the **Retrieve** button (located in the command bar to the immediate left of the **Help** button), and locate the MTP Level 2 High-speed Link port you want to modify. Double-click the port to open it in the Administration panel.
3	Click **Configuration>platform>node**. (You can leave the port window open in the background.)
4	Click **Graphical View**.
5	Double-click the icon for the link system node you are changing.
6	Click **Lock**. A confirmation dialog box appears.
7	Click **Yes** to confirm the change.
8	Click **Offline**. A confirmation dialog box appears.
9	Click **Yes** to confirm the change.
10	In the port window, select a new clocking mode value from the **clocking-mode** drop-down list.
11	Select a new CRC4 interworking mode from the **crc4-interworking** drop-down list.
12	Click **Modify**. A confirmation dialog box appears.
13	Click **Yes** to confirm the change.
14	In the node window, click **Load**. A confirmation dialog box appears.
15	Click **Yes** to confirm the change.

16 Click **Unlock**. A confirmation dialog box appears.

17 Click **Yes** to confirm the change.

—End—

Port maintenance activities

You can perform a bit error rate test (BERT) or a remote loopback on a port. For steps to run a BERT, see "Perform BERT" in the Security and Administration guide. Setting up a remote loopback can be found in the same section of the manual under "Remote loopback".

Configuring a combined SG and STP on the USP

Application

Use this procedure to configure a Signaling Gateway (SG) and Signaling Transfer Point (STP) on the same USP.

Following are some considerations when configuring a SG and STP on the same USP:

- The USP total system limits are shared between the SG and STP applications. That is, the total number of links, linksets, and routesets are shared between the SG and STP applications.
- Resources provisioned against either of the applications or system identities are owned by that application or system identity.
- Virtual linksets are intended to interconnect SGs and STPs on the same USP.
- Virtual linksets cannot be provisioned in a combined linkset with a physical linkset. That is, if you want the SG to route over a combined linkset to a mated pair of STPs, one of which is the local USP STP, you have to use a physical looped-around linkset as opposed to using a virtual linkset to the local STP.
- The SG and STP applications must be assigned unique point codes (PC).

Prerequisites

None.

Action

Perform the following steps to complete this procedure.

Step	Action
	At the OAMP workstation
1	Provision a USP system identity for the SG. If required, refer to procedure "Configuring a System Identity" (page 117).
2	Provision a USP system identity for the STP. If required, refer to procedure "Configuring a System Identity" (page 117).
3	Provision a virtual linkset to interconnect the SG and STP. If required, refer to procedure "Configuring Linksets" (page 124).

—End—

Configuring Channels

Channelized SS7 link termination requires that the proper channel used on the T1 or E1 link be configured. When a Channelized link node is provisioned (either a chanlslink [supporting 4 E1 channels] or a multi-chanlslink [supporting 8 E1 or T1 channels]), default channels are provisioned in the Channel table. These defaults can be modified using the following procedures.

Modifying channel speed

Modifying channel speed

Step	Action
	At the OAMP workstation
1	Click **Configuration>platform>channel**.
2	Click the **Search** panel tab, click the **Retrieve** button (located in the command bar to the immediate left of the **Help** button), and locate the channel you want to modify. Double-click the channel to open it in the Administration panel.
3	Click **Configuration>platform>node**. You can leave the channel window open in the background.
4	Click **Graphical View**.
5	Double-click the icon for the link system node you are changing.
6	Click **Lock**. A confirmation dialog box appears.
7	Click **Yes** to confirm the change.
8	Click **Offline**. A confirmation dialog box appears.
9	Click **Yes** to confirm the change.
10	In the channel window, select the new channel speed in the **channel-speed** drop-down box.
11	Click **Modify**. A confirmation dialog box appears.
12	Click **Yes** to confirm the change.
13	In the node window, click **Load**. A confirmation dialog box appears.

14 Click **Yes** to confirm the change.

15 Click **Unlock**. A confirmation dialog box appears.

16 Click **Yes** to confirm the change.

—End—

Modifying channel number

To modify the channel number, the current record must be deleted and replaced. Perform the following steps to change the channel number.

Modifying channel number

Step	Action
	At the OAMP workstation
1	Click **Configuration>platform>channel**.
2	Click the **Search** panel tab, click the **Retrieve** button (located in the command bar to the immediate left of the **Help** button), and locate the channel you want to modify. Double-click the channel to open it in the Administration panel.
3	Click **Configuration>platform>node**. You can leave the channel window open in the background.
4	Click **Graphical View**.
5	Double-click the icon for the link system node you are changing.
6	Click **Lock**. A confirmation dialog box appears.
7	Click **Yes** to confirm the change.
8	Click **Offline**. A confirmation dialog box appears.
9	Click **Yes** to confirm the change.
10	In the channel window, click **Delete** to delete this channel.
11	Click **New** to create a new channel.
12	Enter the shelf number in the **shelf** box or click on the box to select the proper node from the list of configured node.
13	Enter the slot number in the **slot** box.

14 Enter the physical port in the **port** box. Only one single physical port is current supported on the Channelized node, therefore, this entry is always 0.

15 Enter the E1 or T1 channel number for this SS7 channelized link in the **channel-num** box.

16 Select the link speed associated with this channel in the **channel-speed** drop-down box.

17 Click **Add**. A confirmation dialog box appears.

18 Click **Yes** to confirm the change.

—End—

Configuring Timers and Parameters

The USP uses timers and parameters for many link and linkset functions. The following timer and parameter tables are available on the USP:

- level-2-timer - Level 2 timers apply to MTP Level 2 based links. This includes Low-speed Links (i.e. V.35, DS-0A and channelized links) and E1 High-speed Links based on MTP Level 2.
- level-3-timer - Level 3 timers apply to linksets.
- slt-timer - Signaling Link Test timers are related to all SS7 links.
- saal-timer - Signaling ATM Adaptation Layer (SAAL) timers apply to ATM High-speed Links.
- saal-parm - Signaling ATM Adaptation Layer (SAAL) parameters apply to ATM High-speed Links.
- sctp-parm - SCTP parameters apply to IP High-speed Links and IPS7 Application Server Process paths.

The USP's timers and parameters (except saal-timer and saal-parm) have default settings, as recommended in standards for ANSI and ITU SS7 networks. You can provision new timer values and apply them to provisioned links or linksets. The index for default values is 0. Timers are grouped by level and given an index. You can provision up to 31 timer or parameter indices per level.

Nortel Networks recommends that you provision timers before provisioning links and linksets. You must provision at least one SAAL timer index and one SAAL parameter index before provisioning ATM High-speed Links.

ATTENTION

Default SAAL timer and SAAL parameter indices do not exist for ATM High-speed links.

Further description of ANSI and ITU network timers can be found in the Telcordia GR-246-CORE (Issue 4, Dec. 1999) and ITU-T Q.70x Series (July 1996) documents.

MTP and MTP SLT timer indexes

A set of timers is grouped by an index number. You can create a new set of timers with a unique index or delete existing indexes.

Adding a MTP Level 2 timer index

Step	Action
	At the OAMP workstation
1	Click **Configuration>timer-parm>level-2-timer.**
2	Select a standard from the **protocol-standard** drop-down list.
3	For itu14 or itu24, select a link type from the **link-type** drop-down list. Valid link-types are lslink (low-speed link) or hslink (high-speed link).
4	Enter an index number in the **l2-timer-index** box for a new set of timer values. An index must be a unique number between 1 and 31.
5	Enter the timer values in the **timer** boxes. The default value of the timer can be found using the context-sensitive help. You can start the provisioning of a new timer set from an existing timer set, by first locating it in the search tab, then double-clicking it to switch to the Administration tab. Clicking New enables the creation of a new timer index based on the data from the existing timer index.
6	Click **Add**. A confirmation dialog box appears.
7	Click **Yes** to confirm the change.
	—End—

Adding a MTP Level 3 timer index

Step	Action
	At the OAMP workstation
1	Click **Configuration>timer-parm>level-3-timer.**
2	Select a standard from the **protocol-standard** drop-down list.
3	Enter an index number in the **l3-timer-index** box for a new set of timer values. An index must be a unique number between 1 and 31.
4	Enter the timer values in the timer boxes. The default value of the time can be found using the context-sensitive help. You can start the provisioning of a new timer set from an existing timer set, by first locating it in the **search** tab, then double-clicking it to switch to the **Administration** tab. Clicking **New** enables the creation of a new timer index based on the data from the existing timer index.

ATTENTION
T18,T20,T22,T23,T24,T26,T27 are specified for each system-id.
T19,T21,T25,T28,T29,T30 are specified for each linkset.
All linksets within the same system-id must use the same values of T18,T20,T22,T23,T24,T26,T27.

5 Click **Add**. A confirmation dialog box appears.

6 Click **Yes** to confirm the change.

—End—

Adding a MTP Signaling Link Test (SLT) timer index

Step	Action

At the OAMP workstation

1 Click **Configuration>timer-parm>slt-timer.**

2 Select a standard from the **protocol-standard** drop-down list.

3 Enter an index number in the **slt-timer-index** box for a new set of timer values. An index must be a unique number between 1 and 31.

4 Enter the timer values in the timer boxes. The default value of the timer can be found using the context-sensitive help.

It is also possible to start the provisioning of a new timer set from an existing timer set, by first locating it in the search tab, then double clicking it to switch to the Administration tab. Clicking New enables the creation of a new timer index based on the data from the existing timer index.

5 Click **Add**. A confirmation dialog box appears.

6 Click **Yes** to confirm the change.

—End—

Modifying MTP timer indexes

You cannot modify the timers associated with an MTP timer index. To change timer values, add a new index with the new values. Modify desired links to use the new index. If the old index is no longer used, delete the index.

Deleting a MTP Level2 timer index

Step	Action

At the OAMP workstation

> ***ATTENTION***
> *You cannot delete a timer index that is in use. To delete an index, ensure that it is not used by any links or linksets.*

1

2 Click **Configuration>timer-parm>level-2-timer.**

3 Click the **Search** panel tab, click the **Retrieve** button (located in the command bar to the immediate left of the **Help** button), and locate the record you want to delete. Double-click the index in the search results to transfer to the Administration panel.

4 Click **Delete**.

—End—

Deleting a MTP Level 3 timer index

Step	Action

At the OAMP workstation

1 Click **Configuration>timer-parm>level-3-timer.**

2 Click the **Search** panel tab, click the **Retrieve** button (located in the command bar to the immediate left of the **Help** button), and locate the record you want to delete. Double-click the index in the search results to transfer to the Administration panel.

3 Click **Delete**.

—End—

Deleting a SLT timer index

Step	Action

At the OAMP workstation

1 Click **Configuration>timer-parm>slt-timer.**

2 Click the **Search** panel tab, click the **Retrieve** button (located in the command bar to the immediate left of the Help button), and locate

the record you want to delete. Double-click the index in the search results to transfer to the Administration panel.

3 Click **Delete**.

—End—

SAAL timer and parameter index

SAAL replaces MTP Layer 2 in the protocol stack for ATM High-speed Links. SAAL is comprised of the Service Specific Convergence Sublayer (SSCS) and the ATM Adaption Layer 5 Common Part (AAL5 CP).

ATTENTION
ATM High-speed Links can be only provisioned in ANSI networks.

Although default SAAL timer and SAAL parameter indices do not exist for ATM High-speed links, some recommended default values do exist. These are as follows:

Recommended default values

Parameter name	Default value	Unit	Notes
timer-cc	200	millisecond	
timer-keep-alive	100	millisecond	
timer-no-response	1.5	second	
timer-poll	100	millisecond	
timer-idle	100	millisecond	
timer-t1	5	second	
timer-t2	120	second	
timer-t3	10000	microsecond	
timer-repeat-srec	1.9	hour	
timer-no-credit	1.5	second	
t-sup	120	second	
t-loss	1.3	second	
tau	100	millisecond	
timer-force-proving	10	second	Nortel proprietary. If a link goes down in timer-force-proving seconds after it went up, the SAAL will force "normal" proving the next time the link tries to come up.

Parameter name	Default value	Unit	Notes
sscf-nni-n1	6000		The number of PDUs to send during normal proving. In the Nortel implementation, two PDUs are sent on each T3 expiry during the proving phase until all "sscf-nni-n1" PDUs are sent. With the sscf-nni-n1 default value set to 6000, the USP will take 30 seconds (6000/2/timer-t3 = 30 seconds) to complete proving. This in turn, requires the T2 of the local and far-end SAAL to be configured to greater than 30 seconds, which will adversely affect the SAAL links coming up if the local or far end T2 is set too low (<=30 seconds). To overcome this issue, ensure the local and far end T2 are set to greater than 30 seconds, or set sscf-nni-n1 to a lower value. For example, by setting sscf-nni-n1 to a value of 2000, the proving time is lowered to an interval of 10 seconds.
sscop-maxcc	4		
sscop-maxpd	500		
sscop-max-stat	67		
efc-allocation-rate	3622	cell/second	
efc-allocation-freq	3		
lm-max-nrp	1		
lm-alpha	0.1		
lm-threshold	0.244		
lm-mon-int-spanning	9		
lm-mon-int-per-block	3		

See ITU-T recommendation Q.2110, Q.2140 and Q.2144 for more information.

A set of timers or parameters is grouped by an index number. To create a new set of timers or parameters and give them an index, follow these steps:

Adding a SAAL timer index

Step	Action

At the OAMP workstation

1 Click **Configuration>timer-parm>saal-timer.**

2 Enter an index number in the **saal-timer-index** box for a new set of timer values. An index must be a unique number between 0 and 31.

The default value of the timer can be found using the context-sensitive help.

You can start the provisioning of a new timer set from an existing timer set, by first locating it in the search tab, then double clicking it to switch to the Administration tab. Clicking New enables the creation of a new timer index based on the data from the existing timer index.

ATTENTION
There is no default SAAL Timer Index

3 Enter new timer values in the timer boxes for the timers you want to change.

4 Click **Add**. A confirmation dialog box appears.

5 Click **Yes** to confirm the change.

—End—

Adding a SAAL parameter index

Step	Action

At the OAMP workstation

1 Click **Configuration>timer-parm>saal-parm.**

2 Enter an index number in the **saal-parm-index** box for a new set of timer values. An index must be a unique number between 0 and 31.

The default value of the parm can be found using the context-sensitive help.

3 Enter parameter values in the parameter boxes for the parameters you want to change.

4 Click **Add**. A confirmation dialog box appears.

5 Click **Yes** to confirm the change.

—End—

Modifying a SAAL timer or parameter index

You cannot modify the timers or parameters with a SAAL timer or parameter index. To change timer values, add a new index with the new values. Modify desired links to use the new index. If the old index is no longer used, delete the index.

Deleting a SAAL timer index

Step	Action

ATTENTION

You cannot delete a timer or parameter index that is in use. To delete an index, ensure that it is not used by any links or linksets.

At the OAMP workstation

1 Click **Configuration>timer-parm>saal-timer.**

2 Click the **Search** panel tab, click the **Retrieve** button (located in the command bar to the immediate left of the **Help** button), and locate the record you want to delete. Double-click the index in the search results to transfer to the Administration panel.

3 Click **Delete**. A confirmation dialog box appears.

4 Click **Yes** to confirm the change.

—End—

Deleting a SAAL parameter index

Step	Action

At the OAMP workstation

1 Click **Configuration>timer-parm>saal-parm.**

2 Click the **Search** panel tab, click the **Retrieve** button (located in the command bar to the immediate left of the **Help** button), and locate the record you want to delete. Double-click the index in the search results to transfer to the Administration panel.

3 Click **Delete**. A confirmation dialog box appears.

4 Click **Yes** to confirm the change.

—End—

SCTP/M2PA parameters

Perform the following procedures to add and delete SCTP/M2PA parameters.

Adding SCTP/M2PA parameters

Step	Action

At the OAMP workstation

1 Click **Configuration>timer-parm>sctp-parm.**

2 Enter an index number in the **sctp-parm-index** box for a new set of timer values. An index must be a unique number between 0 and 31.

The default value of the timer can be found using the context-sensitive help.

You can start the provisioning of a new parm set from an existing timer set, by first locating it in the search tab, then double clicking it to switch to the Administration tab. Clicking New enables the creation of a new parm index based on the data from the existing timer index.

3 Enter the parameter values for each parameter. A warning appears if you enter an invalid parameter.

4 Click **Add** to apply the changes. A confirmation dialog box appears.

5 Click **Yes** to confirm the change.

—End—

Modifying SCTP/M3UA parameters

You cannot modify the parameters associated with a SCTP/M3UA parameter index. To change parm values, add a new index with the new values. Modify desired links to use the new index. If the old index is no longer used, delete the index.

Deleting SCTP/M3UA parameters

Step Action

ATTENTION
You cannot delete a timer or parameter index that is in use. To delete an index, ensure that it is not used by any links or linksets.

At the OAMP workstation

1 Click **Configuration>timer-parm>sctp-parm.**

2 Click the **Search** panel tab, click the **Retrieve** button (located in the command bar to the immediate left of the *Help* button), and locate the record you want to delete. Double-click the index in the search results to transfer to the Administration panel.

3 Click **Delete**. A confirmation dialog box appears.

4 Click **Yes** to confirm the change.

—End—

ANSI network timer indexes

For ANSI network timers, USP complies with Telcordia GR-246-CORE (Issue 7, December 2002). The following tables list the MTP Level 2 timers and the MTP Level 3 timers.

MTP Level 2 Timers

Timer	Entry	Description
t1	Numeric (129 ~160)	Timer "Aligned/ready." Specify the aligned ready timeout interval in 100 ms units. The default value is 130 (13 s).
t2	Numeric (50 ~300)	Timer "not aligned." Specify the non-aligned timeout interval in 100 ms units. The default value is 115 (11.5 s).
t3	Numeric (50 ~140)	Timer "aligned." Specify the aligned timeout interval in 100 ms units. The default value is 115 (11.5 s).
t4N	Numeric (15 ~30)	Normal proving period timer. Specify the emergency proving period timeout interval in 100 ms units. The default value is 23 (2.3 s).

Timer	Entry	Description
t4E	Numeric (4 ~10)	Emergency proving period timer. Specify the emergency proving period timeout interval in 100 ms units. The default value is 6 (0.6 s).
t5	Numeric (1)	Timer "sending SIB." Specify the sending status indication busy (SIB) timeout interval in 100 ms units. The default value is 1 (100 ms). This timer can be set to the default value only.
t6	Numeric (10 ~ 60)	Timer "remote congestion." Specify the remote congestion timeout interval in 100 ms units. The default value is 30 (3 s).
t7	Numeric (5 ~ 20)	Timer "excessive delay of acknowledgement." Specify the excessive delay of acknowledgement timeout interval in 100 ms units. The default value is 5 (0.5 s).
t8	N/A	Interval timer for errored interval monitor. This timer is used for 1.536Mbits/links. USP does not need this timer.

MTP Level 3 Timers

Timer	Entry	Description
t1	Numeric (5 ~ 12)	Delay to avoid message mis-sequence on changeover. Specify the mis-sequence changeover timeout interval in 100 ms units. The default value is 5 (0.5s).
t2	Numeric (7 ~ 20)	Waiting for changeover acknowledgement. Specify the changeover acknowledgement timeout interval in 100 ms units. The default value is 7 (0.7 ms).
t3	Numeric (5 ~ 12)	Time controlled diversion - delay to avoid mis-sequencing on changeback. Specify mis-sequence changeback timeout interval in 100 ms units. The default value is 5 (0.5s).

Timer	Entry	Description
t4	Numeric (5 ~ 12)	Waiting for changeback acknowledgement (first attempt). Specify the first attempt changeback acknowledgement timeout interval in 100 ms units. The default value is 5 (0.5 s).
t5	Numeric (5 ~ 12)	Waiting for changeback acknowledgement (second attempt). Specify the second attempt changeback acknowledgement timeout interval in 100 ms units. The default value is 5 (0.5 s).
t6	Numeric (5 ~ 12)	Delay to avoid message mis-sequencing on controlled rerouting. Specify the controlled rerouting timeout interval in 100 ms units. The default value is 5 (0.5 ms).
t7	N/A	Waiting for signaling data link connection acknowledgement. Specify the signaling data link (SDL) connection acknowledgement timeout interval. It is not supported by USP.
t8	Numeric (10)	Transfer-prohibited inhibited timer (transient solution). Specify the transfer prohibited timeout interval in 100 ms units. The default value is 10 (1 s). This timer can be set to the default value only.
t9	N/A	It is not used by GR-246-CORE.
t10	Numeric (30)	Waiting to repeat signaling-route-set -test message. Specify the signaling routeset test message timeout interval in 1 s units. The default value is 30 (30 s). This timer can be set to the default value only.
t11	N/A	Transfer-restricted timer. Specify the signaling routeset test message timeout interval. It is not supported by USP.
t12	Numeric (8 ~ 15)	Waiting for uninhibit acknowledgement. Specify the uninhibit acknowledgement timeout interval in 100 ms units. The default value is 10 (1 s).

Timer	Entry	Description
t13	Numeric (8 ~ 15)	Waiting for force uninhibit. Specify the forced uninhibit timeout interval in 100 ms units. The default value is 10 (1 s).
t14	Numeric (2 ~ 3)	Waiting for inhibition acknowledgement. Specify the inhibit acknowledgement message timeout interval in 1 s units. The default value is 3 (3 s).
t15	Numeric (3)	Waiting to repeat signaling route set congestion test. Specify the repeat routeset congestion test timeout interval in 1 s units. The default value is 3 (3 s). This timer can be set to the default value only.
t16	Numeric (14)	Waiting for routeset congestion status update. Specify the routeset congestion status update timeout interval in 100 ms units. The default value is 14 (1.4 s). This timer can be set to the default value only.
t17	Numeric (8 ~ 15)	Delay to avoid oscillation of initial alignment failure and link restart. Specify the initial alignment failure and link restart interval in 100 ms units. The default value is 10 (1 s).
t18	Numeric (10)	Repeat TFR once by response method. Specify the transfer cluster restricted timeout interval in 1 s units.
t19	Numeric (8 ~ 10)	Failed link craft referral timer. Specify the failed link craft referral timeout interval in 1 min. units. The default value is 8 (8 min.).
t20	Numeric (90 ~ 120)	Waiting to repeat local inhibit test. Specify the local inhibit test timeout interval in 1 s units. The default value is 120 (120 s).
t21	Numeric (90 ~ 120)	Waiting to repeat remote inhibit test. Specify the remote inhibit test timeout interval in 1 s units. The default value is 120 (120 s).

Timer	Entry	Description
t22	Numeric (0 ~ 500)	Timer at restarting SP waiting for signaling links to become available all traffic restart allowed messages. Specify the waiting period for signaling links that are available at restarting node timeout value in 1 s units. The default value is 30 (30 s).
t23	Numeric (0 ~ 500)	Timer at restarting SP with transfer function, started after T22, waiting to broadcast all traffic restart allowed messages. Specify the receiving TRA (traffic restart allowed) message timeout value in 1 s units. The default value is 30 (30 s).
t24	Numeric (0 ~ 500)	Timer at restarting SP with transfer function, started after T23, waiting to broadcast all traffic restart allowed messages. Specify the broadcasting status timeout interval in 1 s units. The default value is 30 (30 s).
t25	Numeric (30 ~ 35)	Timer at restarting SP and SP adjacent to restarting SP, waiting for traffic restart allowed message. Specify the adjacent node to restart node waiting for TRA (traffic restart allowed) message timeout interval in 1 s units. The default value is 30 (30s).
t26	Numeric (12 ~ 15)	Timer at restarting SP waiting to repeat traffic restart waiting message. Specify the waiting to repeat TRW (traffic restart waiting) message timeout interval in 1 s units. The default value is 12 (12 s).
t27	Numeric (0 ~ 5)	Minimum duration of unavailability for full restart. Specify the minimum duration of unavailability for full restart timeout interval in 1 s units. The default value is 0 (0 s).
t28	Numeric (3 ~ 35)	Timer at SP adjacent to restarting SP waiting for traffic restart waiting message. Specify the waiting for TRW (traffic restart waiting) message at node adjacent to restart node timeout interval in 1 s units. The default value is 20 (20 s).

Timer	Entry	Description
t29	Numeric (60 ~ 65)	Timer started when TRA sent in response to unexpected TRA or TRW. Specify the TRA (traffic restart allowed) message sent in response to unexpected TRA or TRW message timeout interval in 1 s units. The default value is 60 (60 s).
t30	Numeric (30 ~ 35)	Timer to limit sending of TFPs and TFRs in response to unexpected TRA or TRW. Specify the limit sending of TFP (transfer prohibited) and TFR (transfer restricted) messages in response to unexpected TRA or TRW message timeout intervals in 1 s units. The default value is 30 (30 s).
t31	Numeric (10 ~ 120)	False link congestion detection timer. Specify the false link congestion detection timeout interval in 1 s units. The default value is 30 (30 s).
t32	N/A	Link oscillation timer - Procedure A. Specify the link oscillation timeout interval. It is not supported by USP.
t33	Numeric (60 ~ 600)	Probation timer for link oscillation - Procedure B. Specify the link oscillation probation timeout interval in 1 s units. The default value is 60 (60 s). In USP, this timer is also used in the ITU network although it is not defined in the ITU specification.
t34	Numeric (5 ~ 120)	Suspension timer for link oscillation - Procedure B. Specify the link oscillation suspension timeout interval in 1 s units. The default value is 60 (60 s). In USP, this timer is also used in the ITU network although it is not defined in the ITU specification.

Configuring a System Identity

Your system is identified by up to 32 system identities. A system identity is made up of a system name, a point code (PC), network indicator, and information related to the protocol standard (ANSI, ITU 14-bit, or ITU-24 bit).

You can provision the USP system identities to suit one of the following applications:

- Signaling Gateway (SG)

  To enable SG characteristics for the system identity, select the **sg-enabled-option** checkbox on the System Identity window.

- Signaling Transfer Point (STP), Number Portability (NP), Service Location Register (SLR)

  To enable STP, NP, or SLR characteristics for the system identity, leave the **sg-enabled-option** checkbox unchecked.

Adding a New System Identity

Your USP is typically assigned a system identity during commissioning. To set up a new system identity, perform the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>mtp>system-id**.
2	Enter a name in the **system-name** dialog box, up to 16 alphanumeric characters in length.
3	Enter an integer from 0 to 31 in the **system-id** dialog box.
4	Enter an integer from 0 to 255 in the **network-id** dialog box. **network-id** is used to communicate with Application Servers.
5	Select a protocol standard, "ansi", "itu14", or "itu24" from the **protocol-standard** list.

ATTENTION
Some of the boxes in this window are disabled as a result of your protocol selection.

6	Determine the appropriate country variant from the **pointcode-variant** list. The following values are valid country variants:

ATTENTION
Ensure the variant you select is compatible with the Core.

If you selected	Then
the ANSI protocol	the only valid country variant is "ansi"
the ITU 24-bit protocol	the only valid country variant is "ntc7-888"
the ITU 14-bit protocol	Select the appropriate country variant. The following list contains the valid country variants.

- itu14-basic
- itu14-383
- itu14-4343
- itu14-545
- itu14-473
- itu14-644
- itu14-464
- itu14-446
- itu14-77
- itu14-293
- itu14-437
- itu14-347

7 Enter a point code in the **pointcode** dialog box.

8 Select a network indicator from the **network-indicator** drop down list. The following values are valid network indicators:

- International
- International Sp
- National
- National Sp

9 Complete one of the following tasks, based on the application you are setting up on your system.

If you want to	Then
set up the system identity for the SG application	check the **sg-enabled-option** checkbox
set up the system identity for the NP, SLR, or STP application	leave the **sg-enabled-option** checkbox unchecked.

ATTENTION
As an STP, NP, or SLR, the USP broadcasts TFx messages. As an SG, the USP does not broadcast TFx messages.

10 Select Shared or Divided from the **cls-type** drop-down menu. A shared combined linkset shares the signaling traffic from a failed link to other available links in the combined linkset. A divided combined linkset shares the signaling traffic from a failed link to available links of the same linkset in the combined linkset. If there are no available links on that linkset, the system sends the traffic to links on the other linkset in the combined linkset.

11 If you selected ITU 14-bit or ITU 24-bit as the protocol standard, and the network indicator is National, click the **tfr-option** check box if you want the Transfer Restricted (TFR) mode enabled for your system identity.

12 If you selected SG as the network element and ANSI or ITU 14-bit as the protocol standard, check the **trid-distribution-option** checkbox if you want the system to route messages to the application servers using the TRID value of the message.

ATTENTION
This checkbox is currently disabled from the GUI.

13 Check the **mtp-restart-option** checkbox if you want the MTP restart option to be enabled for this system identity.

14 For ANSI system identities, enter the integer value **1** or **2** in the **false-link-congestion-level** dialog box.

15 Check the **asm-associate-option** to associate the ASM with the system identity. The **asm-associate-option** can only be checked if **sg-enabled-option** is checked and an ASM is already provisioned.

16 Select an **asm-name** from the drop-down menu to associate the system identity with an ASM. The **asm-name** drop-down menu will be enabled if the **asm-associate-option** is checked.

17 Click **Add** to save your system identification information. The information you have entered is added to the system identity records list. A confirmation dialog box appears.

18 Click **Yes** to confirm the change.

—End—

Modifying a System Identity

To modify an existing system identity, perform the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>mtp>system-id**.
2	Click the **Search** panel tab, click the Retrieve button (located in the command bar to the immediate left of the Help button), and locate the record you want to modify.
3	Double click the index in the search results to transfer to the administration panel. The information for this system identity is displayed in the various boxes.
4	To change the system name, highlight the displayed system name in the **system-name** box and enter a different one.
5	To change the network id, highlight the displayed network id in the **network-id** box and enter a different one.
6	To change the network indicator, select a different one from the **network-indicator** list.
7	To change the false link congestion level, enter a different one in the **false-link-congestion-level** box.
8	To change the Transfer Restricted (TFR) mode state, select or deselect the **tfr-option** checkbox as appropriate.
9	Check the **mtp-restart-option** checkbox if you want the MTP restart option to be enabled. The MTP restart option is available for each network appearance defined on the window. If you do not want the MTP restart option to be available, uncheck the MTP Restart box.
10	Click **Modify** to save your identification information changes. The information for your system identity is updated in the system identity records list. A confirmation dialog box appears

11 Click **Yes** to confirm the change.

—End—

Deleting a System Identity

Before you can delete a system identity, all SS7 and IPS7 provisioning data associated with it must be deleted.

After deleting all SS7 and IPS7 provisioning information associated with the system identity that you want to delete, perform the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>mtp>system id**.
2	Click the **Search** panel tab, click the Retrieve button (located in the command bar to the immediate left of the Help button), and locate the record you want to delete.
3	Click **Delete**. A confirmation dialog box appears
4	Click **Yes** to confirm the change.

—End—

Configuring Capability Codes

A system identity can also use alternate point codes, called capability codes. The alternate point codes are usually shared with mated systems to facilitate loadsharing. You can add and remove capability codes for your system identity.

Adding Capability Codes

Capability codes can be added to your system identity.

To add new capability codes, perform the following steps:

Step	Action
At the OAMP workstation	
1	Click **Configuration>mtp>capability-code.**
2	Select the **system-id** from the drop down box.
3	Enter a new capability code in the **pointcode** box.
4	Click **Add** to save this new capability code. The code is displayed in the Provisioned Cap Codes list. A confirmation dialog box appears.
5	Click **Yes** to confirm the change.

—End—

Deleting Capability Codes

To delete existing capability codes, perform the following steps:

Step	Action
At the OAMP workstation	
1	Click **Configuration>mtp>capability-code.**
2	Click the **Search** panel tab, click the Retrieve button (located in the command bar to the immediate left of the Help button), and locate the record you want to delete. Double click the result in the search results to transfer to the administration panel.
3	Click **Delete**. A confirmation dialog box appears.
4	Click **Yes** to confirm the change.

—End—

Configuring Linksets

A linkset is a set of links that carries signaling information between two nodes in a signaling network. A linkset associated with an ANSI-based system identity or with an IT-based system identity can have up to 16 links. You can add new linksets and change or delete existing ones.

A virtual linkset is an internal linkset the enables two system identities on the same USP to communicate without the requirement of additional hardware.

Adding Linksets

To add new linksets, perform the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>mtp>linkset**.
2	Enter a name for the new linkset in the **linkset-name** dialog box. The name can be up to 16 alphanumeric characters in length.
3	Click the **system-id** list and select the system identity to be associated with this linkset.
4	Choose a link type from the **linkset-type** list. Below is a brief explanation of each linkset type. • A-Links connect STPs to SCP databases and SSP switch end-offices. • B-Links join an STP pair to another STP pair. • C-Links connect two STP nodes to create an STP pair. • D-Links connect local and regional STP pairs. • E-Links connect remote STP pairs to SCP databases and SSP switch end-offices. • F-Links connect SPs, SCPs, and SSPs to one another using signaling links. F-links do not connect to an STP.
5	Select a level three timer from the **l3-timer-index** list.
6	If Network Indicator Interworking is required, select the appropriate network indicator from the **ni- interworking** list. The valid values include: • International

- International SP
- National
- National SP
- disabled

7 Check the **protocol-type**. The valid selections are **mtp, virtual**, or **m3ua**. If you select **virtual**, select an **associated-system-id**. The far-end pointcode must be the pointcode of the selected associated system id.

8 Enter the far-end point code in the **far-end-pointcode** dialog box. The format of this box is dependent upon the protocol settings selected for your system identity.

9 If you have special study operational measurements (SSOMs) provisioned on your system and want to link one to the linkset, you must wait until after the linkset is added, then modify it to activate SSOMs.

10 If you set the **protocol-type** to M3UA, choose an **ipsp-type** from the drop down menu. The options are:

- ipsp-se-Client (Single Exchange Client). The USP starts the M3UA connection by sending ASP-UP.
- ipsp-se-Server (Single Exchange Server). The USP waits for the far end to start the M3UA connection.

11 Leave the **tfp-broadcast-option** disabled if your system is an SG, otherwise set as appropriate.

12 Check the **far-end-mtp-restart-option** box to inform the system that MTP restart is enabled at the far end of the linkset.

13 Click **Add** to save the new linkset. The information for this linkset is displayed in the Linkset Records list. A confirmation dialog box appears.

14 Click **Yes** to confirm the change.

—End—

Modifying Linksets

To modify existing linksets, perform the following steps:

Step	Action

At the OAMP workstation

1 Click **Configuration>mtp>linkset**.

2 Click the **Search** panel tab, click the Retrieve button (located in the command bar to the immediate left of the Help button) and locate the record you want to modify. Double click the linkset in the search results to transfer to the administration panel.

3 The following fields can be modified:

- linkset-name
- linkset-type
- l3-timer-index
- ni-interworking
- protocol-type (all links in the linkset must be deleted before you change this option)
- far-end-pointcode
- ssom-control
- associated-system-id
- ipsp-type
- tfp-broadcast-option
- far-end-mtp-restart-option

ATTENTION
You cannot modify the content of the system-id. To change the system-id, delete the linkset and add a new one with the appropriate system-id.

Enter the new value for the field to be changed.

ATTENTION
You cannot modify the content of the **Far End PC** boxes. To change the far-end point code, delete the linkset and add a new one with the appropriate far-end point code.

You cannot modify the link-type from or to C link type.

4 Click **Modify**. A confirmation dialog box appears.

5 Click **Yes** to confirm the change.

—End—

Deleting Linksets

You cannot delete linksets that have any provisioned SLCs, or are used as part of a linkset group or combined linkset. To delete existing linksets, perform the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>mtp>linkset**.
2	Click the **Search** panel tab, click the Retrieve button (located in the command bar to the immediate left of the Help button) and locate the record you want to delete. Double click the linkset in the search results to transfer to the administration panel.
3	Click **Delete**. A confirmation dialog box appears.
4	Click **Yes** to confirm the change.

—End—

Activating and Deactivating Linksets

To activate or deactivate linksets, perform the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>mtp>linkset**.
2	Click the **Search** panel tab, click the Retrieve button (located in the command bar to the immediate left of the Help button) and locate the linkset you want to activate or deactivate. Double click the linkset in the search results to transfer to the administration panel.
3	Click **Activate** to activate the displayed linkset, or click **Deactivate** to deactivate the displayed linkset. All links in a linkset are activated or deactivated by this command. A confirmation dialog box appears.

ATTENTION
If you deactivate the last in-service link on a linkset, you receive a warning message that indicates your actions could impact network traffic.

4	Click **Yes** to confirm the change.

—End—

Configuring Links

Links provide the physical connection between two adjacent signaling points in a network. You can add new links and change or delete existing ones.

Adding Links

To add new links, perform the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>mtp>link**.
2	Select the **link-type** for this link from the drop down box. Supported link types include: • ss7iplink: IP High-speed Link using M2PA, M2UA-SAAL, M2UA-MTP2, or M3UA • atmhslink: ATM High-speed Link over T1 or E1 interfaces • chanlslink: Channelized links supporting up to 8 channel over E1 or T1. • lslink: Low-speed link, V.35 or DS0A. • Virtuallink: used to connect 2 System Identities on the same USP. • mtp2hslink: MTP L2 High-speed Link.
3	Click the **system-id** list and select the system identity to be associated with this link.
4	Select a linkset from the **linkset-name** list.

CAUTION
When USP connects to third party M3UA peer and the link-type is selected as ss7iplink, you must provision only one link into one linkset of which the protocol-type is M3UA. Provisioning multiple links in the same linkset will result in incorrect M3UA handling.

5	Assign an unused SLC for this link by entering one in the **SLC** box. This code is a logical representation (0 to 15) of a physical link and is agreed upon with the far end node. An SLC can only be used once per linkset.

6 Select a shelf, slot, and port for the link. Click the... button to display a list of available nodes.

7 Indicate whether the system should periodically perform signal link testing (SLT). Click the **periodic-slt-option** check box to change the test status (defaults to unchecked, no test).

Click the check box to toggle between checked and unchecked.

8 Use the table below to determine the next step, based on the type of link that you are adding.

If you are provisioning:	Go to
an SS7iplink	step 9.
an atmhslink	step 10.
a chanlslink	step 11.
an lslink	step 12.
an mtp2hslink	step 13.

9 For SS7iplink, complete the following steps:

a. Click the **protocol** list and select a protocol for this link.

b. Enter the far end destination IP address in the **dest-ipaddress** box.

The provisioned IP address becomes the primary IP address if the peer is multi-homed. In addition to the primary address, each association on the USP accepts up to four multi-homed IP addresses from the far end.

c. If the protocol for this link is M2UA-SAAL or M2UA-MTP2, enter an interface identifier in the **IID** box.

ATTENTION
The interface identifier needs to match the peer interface identifier for the link.

d. In the **local-port** box, enter the number of the local port. For M3UA links, the port is 2905.

e. In the **remote-port** box, enter the number of the remote port.

f. Click the **sctp-operation-mode** list and select an operation for the link. If you select server, the connection starts. If you select client, the client establishes the connection.

ATTENTION

If client mode is selected, then **sctp-checksum** must be set (the choices are adler and crc32).

If the transport protocol is m2ua or m3ua, then you must set the checksum to crc32.

g. Click the **sctp-parms-index** list and select an SCTP parameter index number to associate with this link.

h. Proceed to step 14.

10 For ATM High-speed Links, complete the following steps:

a. Enter a **port** value of 0 for atmhslinks.

b. To enable MTP3b, select the **MTPb-option** checkbox.

ATTENTION

MTP3b support was introduced in USP 10.0 to enable the full ATM HSL functionality. Users must select a high- speed link that is capable of transporting MTP3b messages because not all ATM HSL or terminating nodes support MTP3b.

c. Enter a VCC value in the **vcc** box. The value must be between 0 and 15 for atmhslinks.

d. Enter a VPI in the **vpi** box. The default is 0.

e. Enter a VCI in the **vci** box. The default is 5.

f. Select a SAAL parameter index from the **saal-parm-index** list.

There is no default SAAL parameter index.

g. Select a SAAL timer index from the **saal-timer-index** list.

There is no default SAAL timer index.

h. Proceed to step 14.

11 For channelized links, complete the following steps:

a. Enter a **port** value of 0 for chanlslinks.

b. Enter a channel in the channel box.

c. Select a provisioned MTP link timer index from the **l2-timer-index** list.

The default index is the first available index.

ATTENTION

A system-id must be selected prior to selecting the l2-timer-index or a multiple timer list with the same index is displayed.

d. Select a provisioned MTP link SLT timer index from the **slt-timer-index** list.

The default index is the first available index.

e. Indicate whether the system should perform preventive cyclic retransmission (PCR) on the link using the **pcr-option** check box. PCR is recommended for all satellite links, and intercontinental links where the one-way propagation delay is greater than 15 ms. Both the transmitting and receiving terminal units of the link must use the same error correction method.

ATTENTION

The default value is unchecked. If PCR is not enabled, the link uses basic error correction at MTP level 2.

i. Select a value between 5 and 20 (representing tenths of a second) in the **l2-t7-timer** box. This value represents the excessive delay of acknowledgement timer. PCR continually retransmits unacknowledged MSUs until an acknowledgement is received or the T7 timer expires, at which point the link is taken down.

ATTENTION

The default value for the T7 timer is 600 ms.

Changing the T7 timer value on this screen will not change the T7 timer value for the provisioned timer index. If PCR is selected, the value in the T7 timer box is used for the excessive delay of acknowledgement. If PCR is not selected, the value for T7 in the timer index is used for the excessive delay of acknowledgement.

ii. Select a value between 1 and 50 (representing tenths of a second) in the **pcr-delay** box. This value represents the round trip propagation delay for the link in milliseconds.

The default value is 10, or 1000 ms.

f. Proceed to step 14.

12 For low-speed link, complete the following steps:

a. Enter a **port** value of 0-3 for lslinks.

b. Select a provisioned MTP link timer index from the **l2-timer-index** list.

The default index is the first available index.

ATTENTION
A system-id must be selected prior to selecting the l2-timer-index or a multiple timer list with the same index will be displayed.

c. Select a provisioned MTP link SLT timer index from the **slt-timer-index** list.

The default index is the first available index.

d. Indicate whether the system should perform preventive cyclic retransmission (PCR) on the link using the **pcr-option** check box. PCR is recommended for all satellite links, and intercontinental links where the one-way propagation delay is greater than 15 ms. Both the transmitting and receiving terminal units of the link must use the same error correction method.

ATTENTION
The default value is unchecked. If PCR is not enabled, the link will use basic error correction at MTP level 2.

i. Select a value between 5 and 20 (representing tenths of a second) in the **l2-t7-timer** box. This value represents the excessive delay of acknowledgement timer. PCR continually retransmits unacknowledged MSUs until an acknowledgement is received or the T7 timer expires, at which point the link is taken down.

ii. Select a value between 1 and 50 (representing tenths of a second) in the **pcr-delay** box. This value represents the round trip propagation delay for the link in milliseconds.

The default value is 10, or 1000 ms.

e. Proceed to step 14.

13 For MTP2 High-speed links, complete the following steps:

a. Enter a **port** value of 1 for mtp2hslinks.

b. Select a provisioned MTP link timer index from the **l2-timer-index** list.

The default index is the first available index.

ATTENTION
A system-id must be selected prior to selecting the l2-timer-index or a multiple timer list with the same index is displayed.

c. Select a provisioned MTP link SLT timer index from the **slt-timer-index** list.

The default index is the first available index.

d. Proceed to step 14.

14 Click **Add**. A confirmation dialog box appears.

15 Click **Yes** to confirm the change.

—End—

Modifying Links

To edit links, perform the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>mtp>link**.
2	Click the **Search** panel tab, click the Retrieve button (located in the command bar to the immediate left of the Help button) and locate the record you want to modify. Double click the link to open it in the administration panel and edit active fields as required.
3	Click **Modify** to save these link changes. A confirmation dialog box appears.
4	Click **Yes** to confirm the change.

—End—

Deleting Links

To delete existing links, perform the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>mtp>link**.
2	Click the **Search** panel tab, click the Retrieve button (located in the command bar to the immediate left of the Help button) and locate the record you want to delete. Double click the link to open it in the administration panel.
3	Click **Delete**. A confirmation dialog box appears.
4	Click **Yes** to confirm the change.

—End—

Inhibiting and Uninhibited Links

Inhibit differs from deactivate because an inhibit command does not disrupt traffic. The system finds another link within the linkset before taking the inhibited link down.

To inhibit or uninhibited links, perform the following steps.

Step	Action
	At the OAMP workstation
1	Click **Configuration>mtp>link**.
2	Click the **Search** panel tab, click the Retrieve button (located in the command bar to the immediate left of the Help button) and locate the record you want to Inhibit. Double click the link to open it in the administration panel.
3	Click **Uninhibit** to uninhibit the displayed link, or click **Inhibit** to inhibit the displayed link. A confirmation dialog box appears. When you uninhibited or inhibit a link, several boxes are updated in the Link Status. When you successfully uninhibit a link, the **local-inhibit-state** box changes to Uninhibited. When you successfully inhibit a link, the **local-inhibit-state** box changes to Local Inhibit.
4	Click **Yes** to confirm the change.

—End—

Activating and Deactivating Links

You can stop traffic on a link by changing its status to inactive. You can allow traffic on a link by changing its status to active.

To activate or deactivate links, perform the following steps

Step	Action
	At the OAMP workstation
1	Click **Configuration>mtp>link**.

2 Click the **Search** panel tab, click the Retrieve button (located in the command bar to the immediate left of the Help button) and locate the record you want to activate or deactivate. Double click the link to open it in the administration panel.

3 Click **Activate** to activate the displayed link, or click **Deactivate** to deactivate the displayed link. A confirmation dialog box appears

When you activate or deactivate a link, several boxes are updated in the Operational Date section of this window.

4 Click **Yes** to confirm the change.

—End—

Understanding Link States

The information displayed in the l3-link-status, activation-state, remote-block-status, local-inhibit-state, remote-inhibit-state, congestion-level, discard-level and level-2-status report information on your links. The system updates all SS7 states once per second.

l3-link-status

The l3-link-status box shows the availability of the link: available or unavailable

activation-state

The activation-state box shows you if the link is active. Possible states are inactive, act-restoring, active, failed, suspended-t17, suspended-card-out-of-service, and initializing.

remote-inhibit-status

The remote-inhibit-status refers to links that are inhibited by the far-end node of this link. The remote-inhibit-status box displays the remote inhibit status: remote-inhibit or uninhibited.

remote-block-state

The local-block-state refers to links that are inhibited locally. The local-block-state box displays the local inhibit state: remote-blocked or unblocked.

local-inhibit-state

The local-inhibit-state refers to links that are inhibited by the near-end node of this link. The local-inhibit-state box displays the local inhibit state: local-inhibit or uninhibited.

discard-level

The discard-level ranges from 0 (lowest) through 3 (highest). All messages are assigned a discard priority level. Any messages with a priority level less than the currently displayed discard level are discarded.

congestion-level

Measurement of link congestion differs, depending on the protocol used by your system. If your system identity is ANSI-based, link congestion is measured in four levels: 0 (lowest) through 3 (highest). If your system identity is ITU 14-bit based, link congestion is measured in two levels: 0 (lowest) and 1 (highest).

The congestion levels provide a way for the USP to manage messages during times of elevated congestion. Each SS7 message is assigned a congestion priority level. Messages with high priority levels are more likely to be sent, even when congestion is high.

Any messages with a priority level lower than the currently displayed congestion level result in the following actions:

- The system generates a signaling network management (SNM) transfer control message (TFC) to notify the senders of the messages in the network of the congestion status.
- The system checks the discard level.

If the congestion level continues to remain above 0 for an extended period of time, you may need to add a link.

level-2-status

The level 2 status for a link appears in the level-2-status box. Possible states are idle, in-service, out-of-service, initial-alignment, aligned-not-ready, aligned-ready, processor-outage, not-aligned, proving, aligned, monitoring, local-processor-outage, remote-processor-outage, both-processor-outage, l2-congestion and unknown.

Configuring Combined Linksets

A combined linkset is a set of two linksets used equally to loadshare SS7 messages. B- and D-links are typically used in combined linksets. You can add new combined linksets and change or delete existing ones.

Adding combined linksets

Adding combined linksets

Step	Action
	At the OAMP workstation
1	Click **Configuration>mtp>combined-linkset**.
2	Enter a name for the new combined linkset in the **combined-linkset-name** box. The name can be up to 16 alphanumeric characters in length.
3	Click the **system-id** list and select the system identity to be associated with this combined linkset.
4	Select a linkset from the **first-linkset-name** list.

ATTENTION
This linkset must be deactivated. Use the SS7 MTP Linkset Administration window for this.

5	Select a linkset from the **second-linkset-name** list.

ATTENTION
This linkset must be deactivated. Use the SS7 MTP Linkset Administration window for this.

6	Click **Add**. A confirmation dialog box appears.
7	Click **Yes** to confirm the change.

—End—

Modifying combined linksets

Modifying combined linksets

Step	Action
	At the OAMP workstation
1	Click **Configuration>mtp>combined linkset**.
2	Click the **Search** panel tab, click the Retrieve button (located in the command bar to the immediate left of the Help button), and locate the record you want to modify. Double-click the combined linkset to open it in the Administration panel.
3	Change the entries in the **first-linkset-name** and **second-linkset-name** boxes as needed.

ATTENTION
This linkset must be deactivated. Use the SS7 MTP Linkset Administration window for this.

4	Click **Modify**. A confirmation dialog box appears.
5	Click **Yes** to confirm the change.

—End—

Deleting combined linksets

Deleting combined linksets

Step	Action
	At the OAMP workstation
1	Click **Configuration>mtp>combined-linkset**.
2	Click the **Search** panel tab, click the **Retrieve** button (located in the command bar to the immediate left of the Help button) and locate the record you want to delete. Double-click the combined linkset to open it in the Administration panel.
3	Click **Delete**. A confirmation dialog box appears. You cannot delete a combined linkset if it is being used by a linkset group. You can view and change this information from the SS7 MTP Linkset Group Administration window.
4	Click **Yes** to confirm the change.

—End—

Configuring Linkset Groups

A linkset group contains up to three linksets/combined linksets. The linksets and combined linksets that comprise a linkset group determine normal (primary) and alternate loadshare priorities for signaling routes.

Adding linkset groups

Adding linkset groups

Step	Action
	At the OAMP workstation
1	Click **Configuration>mtp>linkset-group**.
2	Enter a unique name for the new linkset group in the **linkset-group-name** box. The name can be up to 16 alphanumeric characters in length.
3	Click the **system-id** list and select the system identity to be associated with this linkset group.
4	From the drop-down menu beside the route boxes, indicate the types of routes you plan to assign. Click either **ls** (linkset) or **cls** (combined linkset) for each route you plan to use.
5	Select a linkset or combined linkset from the **pri-linkset** list. Each linkset group must be assigned a normal route. Alternate routes are optional.
6	Select a linkset or combined linkset from the **alt1-linkset** list. Alternate routes are used only when the normal route is not available.
7	Select a linkset or combined linkset from the **alt2-linkset** list. Alternate routes are used only when the normal route is not available.
8	Click **Add** to save this new linkset group. The information for this linkset group is displayed in the Linkset Group Records list. A confirmation dialog box appears.
9	Click **Yes** to confirm the change.

—End—

Modifying linkset groups

Modifying linkset groups

Step	Action
	At the OAMP workstation
1	Click **Configuration>mtp>linkset-group**.
2	Click the **Search** panel tab, click the **Retrieve** button (located in the command bar to the immediate left of the Help button), and locate the record you want to modify. Double-click the linkset group to open it in the Administration panel.
3	Change the entries in the **pri-linkset, alt1-linkset, alt2-linkset** boxes as needed.
4	Click **Modify** to save these linkset group changes. A confirmation dialog box appears.
5	Click **Yes** to confirm the change.
	—End—

Deleting linkset groups

ATTENTION
You cannot delete a linkset group if there are any associated routesets.

Deleting linkset groups

Step	Action
	At the OAMP workstation
1	Click **Configuration>mtp>linkset-group**.
2	Click the **Search** panel tab, click the **Retrieve** button (located in the command bar to the immediate left of the Help button), and locate the record you want to delete. Double-click the linkset group to open it in the Administration panel.
3	Click **Delete**. A confirmation dialog box appears.
4	Click **Yes** to confirm the change.
	—End—

Configuring Routesets

You can provision a routeset by assigning a point code and CLLI code to a configured linkset group. The following information explains how to provision routesets and how to evaluate the routeset status.

Adding routesets

ATTENTION
All routesets are added in a deactivated state on the USP. They appear as offline on the Core, and when the USP is configured as an SG, no alarm is raised on the Core.

Adding routesets

Step	Action
	At the OAMP workstation
1	Click **Configuration>mtp>routeset**.
2	Enter the routeset name in the **routeset-name** box. This entry can be up to 16 alphanumeric characters in length.
3	Click the **system-id** list and select the system identity to be associated with this routeset.
4	Select a linkset group from the **linkset-group-name** list.
5	Assign a point code in the **dest-pointcode** box. The format of this box is dependent on the protocol setting selected for your system identity. If you want to datafill a cluster routeset, you can leave the member field empty.
6	Leave the **routeset-index** box empty so it can be automatically assigned by the system, or enter a routeset-index that is not yet used in the system.

ATTENTION
The routeset-index is referenced by routeset, AS, and ASD tables. If the routeset-index is already used, an error message will be displayed.

When provisioning the Application Server Master for mated USPs and the **multi-asm-enable** option is not checked, the second USP routeset-index must be the same as the first USP routeset-index.

7 Click the **xlist-enabled-option** if you are provisioning a network or cluster routeset and if you want the system to track the state of the individual members in that network and cluster routeset.

ATTENTION
The **xlist-enabled-option** only applies for ANSI system identity.

8 Click the **xlist-tfp-broadcast-option** if TFPs are to be broadcasted for prohibited Xlist members of this Cluster Routeset when a TCR (Transfer Cluster Restricted) message is received. The **xlist-enabled-option** must be enabled in order to set the **tfp-broadcast-option**.

9 Click **Add**. A confirmation dialog box appears.

ATTENTION
You must activate the routeset order to allow traffic on it.

10 Click **Yes** to confirm the change.

—End—

Modifying routesets

ATTENTION
The routeset must be deactivated before you can modify it.

Modifying routesets

Step	Action
	At the OAMP workstation
1	Click **Configuration>mtp>routeset**.
2	Click the **Search** panel tab, click the Retrieve button (located in the command bar to the immediate left of the Help button) and locate the record you want to modify. Double-click the routeset to open it in the Administration panel.
3	Change the entries in the **routeset-name** and **linkset-group-name** boxes as needed. Highlight the displayed CLLI or linkset group and enter new ones.
4	Change the **xlist-enabled-option** or **tfp-broadcast-option** as required (ANSI only).

5 Click **Modify**. A confirmation dialog box appears.

6 Click **Yes** to confirm the change.

—End—

Deleting routesets

ATTENTION
If the USP is configured as an SG, then routesets must be deactivated on the USP, offline on the Core, and have no remote code dependencies before you can delete them.

Deleting routesets

Step	Action

At the OAMP workstation

1 Click **Configuration>mtp>routeset**.

2 Click the **Search** panel tab, click the **Retrieve** button (located in the command bar to the immediate left of the Help button) and locate the record you want to delete. Double-click the routeset to open it in the Administration panel.

3 Click **Delete**. A confirmation dialog box appears.

4 Click **Yes** to confirm the change.

—End—

Activating routesets

Activating routesets

Step	Action

At the OAMP workstation

1 Click **Configuration>mtp>routeset**.

2 Click the **Search** panel tab, click the Retrieve button (located in the command bar to the immediate left of the Help button) and locate the record you want to activate. Double click the routeset to open it in the Administration panel.

3 Click **Activate**. A confirmation dialog box appears.

4 Click **Yes** to confirm the change.

—End—

Deactivating routesets

Deactivating routesets

Step	Action
	At the OAMP workstation
1	Click **Configuration>mtp>routeset**.
2	Click the **Search** panel tab, click the **Retrieve** button (located in the command bar to the immediate left of the Help button) and locate the record you want to deactivate. Double-click the routeset to open it in the Administration panel.
3	Click **Deactivate**. A confirmation dialog box appears.
4	Click **Yes** to confirm the change.

—End—

Routeset states

The information displayed in the Operational Data section of this window gives you additional information about the condition of your network and how signals are being handled.

Routeset status

Box Name	Description
Accessibility	This box indicates whether the selected routeset is accessible. The status can be accessible, inaccessible, restricted, or deactivated. All routesets are added in the deactivated state and must be manually activated before they can carry traffic. The accessibility status of a routeset is dependent on the individual route status (TFP, TFA, or TFR), and the state of the associated linksets. Linkset failures associated with the routes of a routeset can cause the routeset to have a status of "Inaccessible" even if the Route 1 and Route 2 status for the normal route, alternative route 1, and alternative route 2 are not in the transfer prohibited (TFP) state. The Route 1 and Route 2 Status boxes display the state for the last TFM received. A routeset can also have an "Inaccessible" status during a combination of linkset failures and TFP status for its associated routes. The accessibility status of a route can have one of the following values: • Accessible: This state indicates that at least one of the routes in the normal route is transfer allowed (TFA), and that the linkset (or one of the linksets in a combined linkset) has more than 50 percent of its links in service to carry traffic. • Restricted: This state indicates either the normal route is not available, or that it is available but the linksets that carry traffic have fewer than 50 per cent of their links in service. The normal route may not be available because the route 1 and route 2 both have a status of TFP, or because the associated linksets are not available. • Inaccessible: This state indicates that this routeset has no available associated routes. Either the associated linksets are not available and/or the routes have a status of TFP.

Box Name	Description
Alarm Status	The alarm-status box displays the alarm level of the displayed routeset. The system displays the status for this box as none, minor, major or critical. A routeset is in a critical alarm state when all routes to the destination are unavailable. A routeset is in a major alarm state when one of the routes to the destination is unavailable. A routeset is in a minor alarm state when a link to the destination (as long as it is not the last link in a linkset) is unavailable.
Current Route	This box indicates the route currently used by the selected routeset. The status can be normal-route, alt1-route, alt2-route or not-available.
Congestion	The Congestion Status box displays the overall routeset congestion level. To determine the overall routeset congestion level, the system measures and compares internal link congestion and external network congestion level, and then displays the higher of these two congestion types. Measurement of routeset congestion differs, depending on the protocol used by your system. If your system identity is ANSI-based, link congestion is measured in four levels: 0 (lowest) through 3 (highest). If your system identity is ITU based, link congestion is measured in two levels: 0 (lowest) and 1 (highest). Each network message is assigned a congestion priority level. Messages with high priority levels are more likely to be sent, even when congestion is high. Any routesets with a priority level lower than the currently displayed congestion level result in an SNM (system network management) TFC (transfer control message) to notify the senders of the messages accumulating in the network.
Network-congestion	The network-congestion box displays the external network congestion level. If your system identity is ANSI-based, link congestion is measured in four levels: 0 (lowest) through 3 (highest). If your system identity is ITU 14-bit based, link congestion is measured in two levels: 0 (lowest) and 1 (highest). The congestion levels provide a way for the USP to manage messages during time of elevated congestion.
Normal Route	This box displays the status of the linkset or combined linkset associated with the Normal route.

Box Name	Description
Alternate Route 1	This box displays the status of the linkset or combined linkset associated with the Alternate route 1.
Alternate Route 2	This box displays the status of the linkset or combined linkset associated with the Alternate route 2. The status of a route is either: tfa, tfr, tfp, deactivated or unavailable. If a route includes only one linkset, the route 2 status boxes are empty. If a route includes a combined linkset, the route1 and route 2 status boxes contain information.

Xlist

A Network Routeset is provisioned in the Routeset table with only the Network part of the Point Code, while a Cluster Routeset is provisioned with only the Network and Cluster part of the Point Code.

The XLIST table is a dynamic table that contains information on members of Network or Cluster routesets that have a more restricted state than the parent Network or Cluster routesets. This table is read-only.

Viewing Xlist members

To view Xlist members, perform the following steps:

Viewing Xlist Members

Step	Action
	At the OAMP workstation
1	Click **Configuration>mtp>x-list**.
2	Click the **Search** panel tab, click the Retrieve button (located in the command bar to the immediate left of the Help button) and locate the record you want to view. Double click the routeset to open it in the administration panel. Only members that have more restricted states than their parent Network or Cluster Routeset state are listed in the table.
	—End—

Understanding X-List Routeset States

The information displayed in the Administration tab for a member routeset is described below.

- routeset-name: This is the name of the Network or Cluster Routeset.
- dest-pointcode: This is the actual Point Code of the member.
- accessibility: This box indicates if the selected member is accessible. The status can be accessible, inaccessible, or restricted.
- alarm-status: This box displays the alarm level of the member routeset. The alarm status can be none, major, or critical. A member routeset is in a critical alarm state when all routes to the destination are unavailable. A member routeset is in a major alarm state when the member routeset is in a restricted state.

- Normal Route: This box displays the status of the linkset or combined linkset associated with the Normal route.
- Alternate Route 1: This box displays the status of the linkset or combined linkset associated with the Alternate route 1.
- Alternate Route 2: This box displays the status of the linkset or combined linkset associated with the Alternate Route 2.

ATTENTION

The status of a route is one of the following: tfa, tfr, tfp, deactivated, or unavailable

If a route includes only one linkset, the route 2 status box is empty. If a route includes a combined linkset, the route1 and route 2 status boxes contain information.

Configuring SCCP, Remote Point Codes (RPC)

An RPC is an SS7 node to which the Universal Signaling Point (USP) can route SS7 messages, based on GTT (global title translation).

A Remote PointCode is selected from the list of provisioned routesets and Application Server Destinations (ASD).

Adding RPCs

To add new RPCs, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>sccp>remote-pointcode.**
2	Select a system id from the **system-id** drop-down menu.
3	Enter the remote pointcode value in the **remote-pointcode** box or use the … selection box to select a routeset or Application Server Destination. You can provision up to 2000 RPCs on your USP.
4	Check the **xudt-support-option** box if the RPC supports extended unit data transfer (XUDT). If you do not select XUDT, the system attempts to translate XUDT messages that do not include optional data back to unit data transfer (UDT) messages.
5	Click **Add**.

—End—

Modifying RPCs

To modify RPCs, perform the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>sccp>remote-pointcode.**
2	Click the **Search** panel tab and locate the RPC you want to modify. Double click the RPC to open it in the administration panel.
3	Modify the required fields.

The only field that can be modified is the **xudt-support-option** checkbox.

4 Click **Modify**.

—End—

Deleting RPCs

To delete existing RPCs, complete the following steps:

Step	Action

At the OAMP workstation

1 Click **Configuration>sccp>remote-pointcode**.

2 Click the **Search** panel tab and locate the RPC you want to delete. Double click the RPC to open it in the administration panel.

3 Click **Delete**.

ATTENTION
If any RSSs, CPCs, or GTT results refer to the RPC you are trying to delete, you must first delete the associated RSSs, CPCs, or results.

—End—

Configuring Remote Subsystems

ATTENTION
A Remote PointCode must be provisioned for an SS7 node prior to provisioning the Remote Subsystem.

A remote subsystem (RSS) is an application located on an SS7 node to which the USP can route SS7 messages based on GTTs.

Adding Remote Subsystems

Step	Action

At the OAMP Workstation

1 Click **Configuration>sccp>remote-subsystem**.

2 Select the system identity to which you want to add an RSS from the **system-id** drop-down list.

3 Enter the remote pointcode value in the **remote-pointcode** box or use the ... selection box to select remote point code.

4 Enter the Subsystem Number in the **ssn** box. The value can range from 0 to 255.

Subsystem Numbers

Subsystem Number	SCCP User Function
0	SSN not known/not used
1	SCCP management
2	reserved
3	ISDN user part
4	operation and maintenance application part (OMAP)
5	mobile application part (MAP)
6	home location register (HLR)
7	visited location register (VLR)
8	mobile switching center (MSC)
9	equipment identification register (EIR)
10	authentication center (AC for ANSI, AUC for ITU)
11-254	spare
255	reserved for expansion

5 Enter the RSS name in the **ssn-name** box. This box accepts up to eight characters.

Each RSS name for the RSSs within an RPC must be unique.

6 Click **Add** to add this RSS to the database. The status of the new RSS and RSS test information automatically appears in the Operational Data part of the form.

—End—

Modifying Remote Subsystems

Step	Action
	At the OAMP Workstation
1	Click **Configuration>sccp>remote-subsystem**.
2	Click the **Search** panel tab. Locate the RSS you want to edit. Double click the RSS in the search results to transfer to the administration panel.
3	Modify the contents of the **ssn-name** field. This field accepts up to eight alphanumeric characters. Each RSS name for the RSSs within an RPC must be unique.
4	Click **Modify**.

—End—

Deleting Remote Subsystems

Step	Action
	At the OAMP Workstation
1	Click **Configuration>sccp>remote subsystem**.
2	Click the **Search** panel tab. Locate the RSS you want to edit. Double click the RSS in the search results to transfer to the administration panel.
3	Click **Delete**.

ATTENTION

If any CPCs, or GTT results refer to the RSS you are trying to delete, you must first delete the associated CPCs, or results.

—End—

Configuring SCCP, Concerned Point Codes (Remote Subsystems)

A concerned point code (CPC) is a point code to which the USP sends subsystem status changes. When the USP receives subsystem status changes from a remote subsystem, it relays this information to the concerned point code. You can have up to eight CPCs provisioned for each RSS. A CPC is selected from the list of provisioned Remote PointCodes.

ATTENTION
Remote Subsystem Concerned PointCodes cannot be modified.

Adding CPCs

To add new CPCs, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>sccp>remote-subsystem-concerned- point-code**.
2	Select the system identity to which you want to add an CPC from the **system-id** drop-down list.
3	Enter the remote pointcode value in the **remote-pointcode** box or use the ... selection box to select remote point code
4	Enter the subsystem number in the **ssn** box. The ssn box is provisioned automatically when the RPC is selected from the ... box.
5	Enter the concerned pointcode value in the concerned-pointcode box or use the ... selection box to select the concerned point code.
6	Click **Add**.

—End—

Deleting CPCs

To delete existing CPCs, complete the following steps:

Step	Action
	At the OAMP workstation

1 Click **Configuration>SCCP>remote-subsystem-concerned-point-code**.

2 Click the **Search** panel tab. Locate the RSS from which you want to delete a CPC. Double click the RSS in the search results to transfer to the administration panel.

3 Click **Delete**.

—End—

Configuring SCCP, Local Subsystems

A local subsystem (LSS) is a subsystem that is managed locally by the USP. The actual application associated with the subsystem can reside on the USP (as in the case of Number Portability or Service Location Register or Low Layer Control Point) or in the IP Space when these applications are located on Application Servers.

The local subsystem class (lss-class) defines the type of the subsystem. The following classes are supported.

Number Portability LSS (NP_ANSI and NP_ITU14)

An NP LSS enables Location Routing Number (LRN) or Message Relay (MR) queries to be terminated at the USP. Based on the portability information provided by the LSMS or NSM, the NP LSS queries the local NP database to check if the number has been ported.

You can provision only one NP LSS class: NP_ANSI or NP_ITU14. However, multiple subsystems can be defined using the same class. The USP supports up to six NP LSS instances in total, and these instances are shared by all NP Subsystems.

Signaling Gateway LSS (IP_LSS)

The applications for IP Local Subsystem are located on Application Servers connected to the USP by means of an IP Network. The LSS consists of one or more application servers. In order to provision an LSS, you must first provision AS processes (ASP), ASs, and AS paths. Up to 16 Local Subsystem Instances (i.e. Application Servers) can be provisioned per IP local Subsystem.

ATTENTION

IP_LSS can be provisioned only for System IDs that are configured as Signaling Gateway (sg-enabled-option checked).

Route Master LSS (RM_LSS)

The RouteMaster is responsible for presenting a consolidated view of the Host and Donor Local Subsystems to the rest of the network. In order to perform this function, the RouteMaster is provisioned with each of the Local and Remote Subsystems on the Host and Donor switches.

The state of the local subsystem is based on the state of the Remote Subsystem provisioned, and the required instances provisioned. If the required instances field is set to 1, then only one of the associated remote subsystems on the Host or Donor must be available for the Local

RouteMaster Subsystem to be available. If the Required Instances field is set to 2, then both of the associated Remote Subsystems must be in service for the RouteMaster Local Subsystem to be available.

The RouteMaster responds to all SCCP Management messages (based on a consolidated view of Host and Donor Subsystems).

Service Location Register LSS (SLR)

The SLR LSS provides the ability to perform IMSI to RN or MSISDN to RN lookups for the purpose of routing wireless queries to the correct Home Location Register (HLR). The USP supports up to six SLR LSS instances in total, and these instances are shared by all SLR Subsystems.

The SLR LSS is common for both ANSI and ITU networks, which means that the SLR is represented by a single class: SLR. The type of network is determined by the system identity associated with the LSS. You can provision multiple subsystems using the same SLR class.

Low Layer Control Point LSS (LLCP)

An LLCP LLS enables Low Layer Intelligent Network queries to be terminated at the USP. Based on the Low Layer Intelligent Network information provided by the Low Layer Management Point (LLMP), the LLCP LSS queries the local LLCP database to determine how to handle the call.

Adding LSSs

To add a new local subsystem, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configure>sccp>local-subsystem**.
2	From the **system-id** list, select the system identity to which you want to add an LSS.
3	Select an LSS_Class from the **lss_Class** list.

ATTENTION

For an NP application, you can provision only one LSS class: NP_ANSI or NP_ITU14.

4	For IP LSS and RM LSS enter the name of the application in the **lss-application** box.

5 Enter an LSS number into the **ssn** box. The valid values range from 0 to 255.

Subsystem Numbers

Subsystem Number	SCCP User Function
0	SSN not known/not used
1	SCCP management
2	reserved
3	ISDN user part
4	operation and maintenance application part (OMAP)
5	mobile application part (MAP)
6	home location register (HLR)
7	visited location register (VLR)
8	mobile switching center (MSC)
9	equipment identification register (EIR)
10	authentication center (AC for ANSI, AUC for ITU)
11-254	spare
255	reserved for expansion

6 In the **required-instances** box, enter the minimum number of operational instances required for the LSS to be in the Allowed state. You can enter a number from 1 to 6 (for an NP_ANSI, NP_ITU14, SLR, and LLCP) or 1 to 16 (for an IP_LSS subsystem).

ATTENTION

The value entered into the **Required Instances** box applies to all subsystems defined against the same LSS class. This means that you must provision the same value for all local subsystems of the same LSS class.

ATTENTION

The recommendation is that the minimum number of instances for an NP, SLR, or LLCP is at least one less than the number of instances provisioned.

7 From the **app-code** list, select the application capability code (ACC) for the LSS that you want to add. A capability code must already be provisioned. One of the provisioned capability codes can act as an ACC.

The USP supports ACCs to enable the USP to report the following MTP level messages:

- transfer prohibited (TFP) -- sent when the LSS becomes unavailable
- transfer allowed (TFA) -- sent when the LSS becomes available

This capability enables external nodes to route MTP messages around LSS failures.

If other nodes send the USP a subsystem status test (SST) message with the ACC in the destination point code, the USP returns a subsystem available (SSA) or subsystem prohibited (SSP) message with the ACC in the originating point code.

8 Enter the Replicated Pointcode in the **replicated-pointcode** box or select the replicate point using the ... box.

9 If you are provisioning an IP_LSS, perform the following additional steps:

a. Click the **opc-tcap-distribution-option** checkbox to enable the distribution of the TCAP query messages based on the OPC of the message. The distribution makes use of the OPC distribution specified in the Application Server Assignment table.

> **ATTENTION**
> This functionality is not currently used by any solutions and should not be checked.

b. if the **opc-tcap-distribution-option** is selected, you can select a default Application Server in the default-AS list. This default AS receives all TCAP query messages that cannot be routed by information in the Application Server Assignment table.

c. Select the desired Class/Distribution method from **class-1-distribution** drop-down menu. Distribution to the Subsystem Instances is made using either the SLS value of the message or round robin.

10 If you are provisioning an LLCP local subsystem, perform the following additional steps:

a. In the **scmg-disabled-option** box, indicate if scmg management messages should be sent for this system when the subsystem state changes.

b. In the **crp-option** box, indicate if circular routing prevention should be performed on outgoing messages.

c. In the **sar-option** box, indicate if segmentation and reassembly should be used on outgoing messages.

11 Click **Add**.

—End—

Modifying LSSs

To modify the LSS information, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configure>sccp>local-subsystem**.
2	Click the **Search** panel tab. Locate the LSS you want to edit. Double click the LSS in the search results to transfer to the administration panel.
3	The following fields can be modified for a local subsystem: a. Required Instances: Enter the new minimum number of operational instances required for the LSS to be in the Allowed state. b. Application Capability Codes: From the **app-cap-code** list, select the new ACC for the LSS that you want to modify. c. Enter the Replicated Pointcode in the **replicated-pointcode** box or select the replicate point using the ... box. d. For IP_LSS, the **opc-tcap-distribution-option**, **default-as** and the **class-1-distribution** field can also be modified.
4	Click **Modify**.

—End—

Deleting LSSs

If any CPCs, LSS instances of the same type, or SSN Only results exist for the LSS you are trying to delete, you must first deactivate the LSS, then delete the associated CPCs, LSS instances, or SSN Only results, respectively.

If you have NP, SLR, or LLCP provisioned against an LSS, you must delete all associated NP, SLR, or LLCP information before you delete the LSS.

To delete existing LSSs, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configure>sccp>local subsystem**.
2	Click the **Search** panel tab. Locate the LSS you want to delete. Double click the LSS in the search results to transfer to the administration panel.
3	Click **Delete**.

—End—

Activating and Deactivating LSSs

To activate or deactivate existing LSSs, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configure>sccp>local subsystem**.
2	Click the **Search** panel tab. Locate the LSS you want to activate or deactivate. Double click the LSS in the search results to transfer to the administration panel.
3	Click **Activate** or **Deactivate**. For LSS class NP_ITU14, the Country Code must be provisioned in the **Configuration>np>np-itu>np-lss-misc** form prior to activation. For LSS class SLR, the Country Code must be provisioned in the **Configuration>slr>slr-misc** form prior to activation.

—End—

Configuring SCCP, LSS Instances

A subsystem is made up of a number of local subsystem instances. Each LSS instance provides a portion of its local subsystem type's overall functionality.

For a Number Portability (NP_ANSI and NP_ITU14) or Service Location Register (SLR) Application, an LSS instance corresponds to a physical NPC or NPS processor card. The provisioning limit is up to six instances for these LSSs. NP and SLR LSS instances are shared across all system identities. They are provisioned using the shared-local-subsystem-instance form.

For an IP Local Subsystem, an LSS instance is an Application Server. The provisioning limit is up to 16 instances for an IP_LSS class. IP_LSS instances are dedicated to a System Identity and they are provisioned using the dedicated-local-subsystem-instance form.

Adding shared LSS Instances

To add new shared LSS instances (for NP_ANSI, NP_ITU14 and SLR LSS), complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configure>sccp>shared-local-subsystem-instance**.
2	Select an lss class from the **lss-class** drop-down menu (NP_ANSI, NP_ITU14 or SLR).
3	Enter the Instance number in the **instance** box.
4	Enter the shelf and slot for the NPC or NPS card of this instance or use the ... box to select the proper card.
5	Click **Add**.

—End—

Deleting shared LSS Instances

To delete instances, complete the following steps:

Step	Action
	At the OAMP workstation

1 Click **Configure>sccp>shared-local-subsystem-instance**.

2 Click the **Search** panel tab. Locate the LSS instance you want to delete. Double click the LSS instance in the search results to transfer to the administration panel.

3 Click **Deactivate**.

4 Verify that the NPC or NPS system node associated with this LSS instance is locked and offline.

5 Click **Delete**.

—End—

Activating and Deactivating shared LSS Instances

To activate and deactivate instances, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configure>sccp>shared-local-subsystem-instance**.
2	Click the **Search** panel tab. Locate the LSS instance. Double click the LSS instance in the search results to transfer to the administration panel.
3	If activating, ensure that the corresponding system node is unlocked.
4	Click **Activate** or **Deactivate**.

—End—

Adding dedicated LSS instances

To add new LSS instances (for IP_LSS), complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configure>sccp>dedicated-local-subsystem-instance**.
2	Select the system identity associated with the LSS using the **system-id** drop-down list.
3	Select the IP_LSS class from the **lss-class** drop-down menu.

4 Enter the SSN number of the Local Subsystem in the **ssn** box to which the instances will be added or select it using the ... box.

5 Enter the Instance number in the **instance** box.

6 Select the Application Server from the **as-name** drop-down list.

> **ATTENTION**
> An Application Server can only be used for one instance in a subsystem but it can be used for multiple instances in different subsystems.

7 Click **Add**.

—End—

Deleting dedicated LSS instances

To delete instances (for IP_LSS), complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configure>sccp>dedicated-local-subsystem-instance**.
2	Click the **Search** panel tab. Locate the LSS instance you want to delete. Double click the LSS instance in the search results to transfer to the administration panel.
3	Click **Deactivate**.
4	Click **Delete**.

—End—

Activating and Deactivating dedicated LSS Instances

To activate and deactivate instances (for IP_LSS), complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configure>sccp>dedicated-local-subsystem-instance**.
2	Click the **Search** panel tab. Locate the LSS instance. Double click the LSS instance in the search results to transfer to the administration panel.

3 Click **Activate** or **Deactivate**.

—End—

Configuring SCCP, Concerned Point Codes (Local Subsystems)

CPC is a point code to which the USP sends subsystem status changes. The USP sends subsystem status changes to all CPCs associated with the local subsystem. You can provision up to 64 CPCs per local subsystem (LSS).

Adding CPCs

To add new CPCs, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configure>sccp>local-subsystem-concerned-pointcode**.
2	Select the system identity associated with the LSS using the **system-id** drop-down list.
3	Enter the SSN number of the Local Subsystem in the **ssn** box to which the CPC will be added or select it using the ... box.
4	Enter the Pointcode in the **concerned-pointcode** box or selected the remote pointcode using the ... box.
5	Click **Add**.

—End—

Deleting CPCs

To delete exiting CPCs, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configure>sccp>local-subsystem-concerned-pointcode**.
2	Click the **Search** panel tab. Locate the CPC you want to delete. Double click the CPC in the search results to transfer to the administration panel.
3	Click **Delete**.

—End—

Configuring NPE Chains

Once you have provisioned Number Portability Extension (NPE) cards, you can provision-related NPE chains.

An NPE chain consists of the following elements:

- a master NP Controller (NPC) or NP Server (NPS) system node
- an optional alternate NPS system node
- a maximum of four NPE system nodes

The NPE system nodes in a chain form a level with other NPE system nodes at the same position in other chains. The NPE system nodes specified for NPE1 form level one, NPE2 form level two, and so on. You can provision a maximum of six NPE chains.

You can update an NPE level only if all the chains are balanced for that level. For example, in a configuration of two chains where chain one has two NPEs and chain two has three NPEs, there are only two levels of NPEs. The system can update the NPEs only at levels one and two.

The local subsystem instance (LSSI) cannot be active when you are provisioning or modifying NPE chains.

For Number Portability, each NPE level increases the database capacity by 10 million records, to a system maximum of 40 million records. If your database supports fewer than 10 million records, you do not need to provision NPE chains.

For the Service Location Register, each NPE level increases the database capacity by 14 million records, to a system maximum of 70 million records. If your database supports fewer than 14 million records, you do not need to provision NPE chains.

If the NPE chain contains a combination of Release 9.0 PP5 cards (such as NTST11FA and NTST11FB) and cards from previous releases, you must provision the Release 9.0 PP5 hardware as the master system node for the chain.

Adding an NPE Chain

Before you add an NPE chain, ensure that:

- all NPC, NPS, and NPE system nodes are already provisioned on the system
- the master and alternate NPC and NPS system nodes are locked

To add an NPE chain, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>sccp>npe-chain**.
2	Click... next to **master-shelf** to select the NPC or NPS system node to serve as the master system node for the chain. The list contains all provisioned NPC and NPS system nodes, including nodes already provisioned in a chain.
	Once an NPC or NPS system node is associated with one NPE chain, it cannot be associated with another NPE chain.
3	Click... next to **alt-shelf** to select the NPS system node to serve as the alternate system node. for the chain The list contains all provisioned NPS system nodes, including nodes already provisioned in a chain.
	ATTENTION This step is optional.
4	Click... next to **npe1-shelf** list, select the NPE system node to serve as the first NPE level in the chain. The list contains all provisioned NPE system nodes, including nodes already provisioned in a chain.
5	Click... next to **npe2-shelf** list, select the NPE system node to serve as the second NPE level in the chain. The list contains all provisioned NPE system nodes, including nodes already provisioned in a chain. Do not select an NPE node already selected as the first NPE level in the chain, or already a member of another NPE chain.
6	Click... next to **npe3-shelf** list, select the NPE system node to serve as the third NPE level in the chain. The list contains all provisioned NPE system nodes, including nodes already provisioned in a chain. Do not select an NPE node already selected as the first or second NPE level in the chain, or already a member of another NPE chain.
7	Click... next to **npe4-shelf** list, select the NPE system node to serve as the fourth NPE level in the chain. The list contains all provisioned NPE system nodes, including nodes already provisioned in a chain. Do not select an NPE node already selected as the first or second or third NPE level in the chain, or already a member of another NPE chain.

8 Click **Add** to save the NPE chain and add it to the system provisioning.

If you have already provisioned the master NPC or NPS for an LSSI on the LSS Type and Instances Provisioning window, this procedure is complete.

If you have not already provisioned the NPC or NPS master with an LSSI, you must provision an LSSI for this chain.

—End—

Modifying an NPE Chain

The master and alternate NPC and NPS system nodes must be locked before you can modify an NPE chain.

You cannot modify the following nodes:

- the NPC/NPS master
- an NPS alternate that has already been provisioned
- the first NPE system node in the chain

If you want to modify any of these nodes, you must delete the chain.

Add a System Node to an NPE Chain

To add a system node to an NPE chain, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>sccp>npe-chain**.
2	Click the **Search** panel tab. Locate the NPE chain you want to modify. Double click the result in the search results to transfer to the administration panel.
3	To add an alternate NPS system node to the chain, click... next to the **alt-shelf** list. A list of all provisioned NPS system nodes appears, including nodes already provisioned in a chain. Select the NPS system node that you want to add.
4	To add a second NPE system node to the chain, click ... next to **npe2-shelf** to select the NPE system node to serve as the second NPE level in the chain. The list contains all provisioned NPE system nodes, including nodes already provisioned in a chain.

Do not select an NPE node already selected as the first NPE level in the chain, or already a member of another NPE chain.

You cannot modify an NPE system node that has already been provisioned. To modify an NPE system node in a chain, you must delete the last node in the chain up to the second node in a chain.

5 To add a third NPE system node to the chain, click ... next to **npe3-shelf** to select the NPE system node to serve as the third NPE level in the chain. The list contains all provisioned NPE system nodes, including nodes already provisioned in a chain.

Do not select an NPE node already selected as the first or second NPE level in the chain, or already a member of another NPE chain.

6 To add a fourth NPE system node to the chain, click ... next to **npe4-shelf** to select the NPE system node to serve as the fourth NPE level in the chain. The list contains all provisioned NPE system nodes, including nodes already provisioned in a chain.

Do not select an NPE node already selected as the first or second NPE level in the chain, or already a member of another NPE chain.

7 Click **Modify** to save the NPE chain.

—End—

Deleting an NPE System Node from an NPE Chain

If you want to delete an NPE system node, you must first remove the NPE system node from the NPE chain.

To delete an NPE system node, or chain level, from an NPE chain, you must delete all lower NPE levels of the chain, one level at a time. When you have deleted the lower levels of the chain, you can delete the selected NPE system node.

ATTENTION

Before you can delete an NPE system node from a chain, you must first deactivate the local subsystem instance (LSSI) and lock the master and alternate NPC and NPS.

To delete an NPE system node from an NPE chain, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>sccp>npe-chain**.

2 Enter a blank in the **npe4-shelf** and **npe4-slot** fields or in the corresponding field of the last NPE in the chain if you don't have a full chain.

3 Click **Modify** to save your changes and to remove the selected NPE node from the chain.

4 If you want to remove another NPE node from the chain, repeat steps 2 and 3 for the next NPE in the chain.

5 Perform a full bulk load of data to redistribute the NP database records among the remaining NPE levels.

—End—

Deleting an NPE Chain

All NPC and NPS system nodes must be locked before you can delete the NPE chain.

To delete an NPE chain, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>sccp>npe-chain**.
2	Click the **Search** panel tab. Locate the NPE chain you want to delete. Double click the result in the search results to transfer to the administration panel.
3	Click **Delete**.
4	Perform a full bulk load to redistribute NP data among the remaining NP system nodes.

—End—

Configuring GTT Result

Under the gtt-result form, GTT results of *PC-only*, *PC-SSN* and *SSN-Only* can be configured.

PC-Only: A result name can have up to 16 result destinations (point codes) and the destination selection is made based on the provisioned cost associated with the destination. Lower cost destinations are selected first. The PC-Only result also contains a PC and routing indicator. When translation occurs, the PC and routing indicator in the message signaling unit (MSU) is replaced with the provisioned one (Point Code is replaced in the MTP L3 Destination Point Code [DPC] and in the SCCP Called Party Address [CGPA]). The MSU is then routed, using MTP (message transfer part), toward its destination.

PC-SSN: A result name can have up to 16 result destinations (point codes) and the destination selection is made based on the provisioned cost associated with the destination. Lower cost destinations are selected first. When translation occurs, the PC and SSN in the message signaling unit (MSU) are replaced with the provisioned one. Point Code is replaced in the MTP L3 Destination Point Code (DPC) and in the SCCP Called Party Address (CGPA). The MSU is then routed, using MTP (message transfer part), toward its destination.

SSN-Only: The result points to a Local Subsystem on the USP and the message is distributed to one of its active instances.

Adding PC Only Results

To add new PC Only results, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>gtt>gtt-result**.
2	Click the **system-id** list and select the system identity for this result.
3	Enter the result name in the **result-name** box. This box can accept up to 17 characters. The result name must be unique across all result types.
4	Click the **equal-priority-threshold** box in order to share the traffic load in the destinations of the smallest cost group, or among all cost groups if the smallest cost group has only one available destination. This step is optional.

5 Select **pc-only** from the result-type list in the Result Destination Data portion of the window. For each result name, you can create a maximum of 16 destinations.

6 Enter a cost and load factor in the **cost** and **load** box. The cost value sets priority of routing selection for messages The lower the cost is, the higher the priority. The variation in load factors for different destinations in the same group determines how evenly the load is distributed. The smaller the variation is, the more even is the distribution.

ATTENTION
When you enter 0 in the Load Factor box, the system takes the destination out of routing selection.

7 Select the appropriate remote system identity from the **remote-system-id** drop-down list.

8 Enter the remote point code in the **remote-pointcode** box or select it using the ... box.

9 Click the **routing-indicator** list and select the routing type for this result record. Select *Route on GT* when you want global titles that use this result record to have their outgoing message indicators set to route on global title. Select *Route on PC* when you want global titles that use this result record to have their outgoing message indicators set to route on point code.

10 Click **Add**.

—End—

Modifying PC Only Results

To modify existing PC Only results, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>gtt>gtt-result**.
2	Click the **Search** panel tab. Locate the result. Double click the result in the search results to transfer to the administration panel.
3	The following fields can be modified: • Result-name: • Equal-priority-threshold:

- Cost:
- Load:
- Remote-system-id:
- Remote-pointcode:
- Routing-indicator:

4 Click **Modify**.

—End—

Deleting PC Only Results

To delete existing PC Only results, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>gtt>gtt-result**.
2	Click the **Search** panel tab. Locate the result you want to delete. Double click the result in the search results to transfer to the administration panel.
3	Click **Delete**.

ATTENTION
If any PC/GT results or GTT translations refer to the PC Only result you are trying to delete, you must first delete the associated PC/GT results or GTT translations.

—End—

Configuring GTT, PC/SSN Results

Adding PC/SSN Results

To provision a PC/SSN result, perform the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>gtt>gtt-result**.
2	Click the **system-id** list and select the system identity for this result.

3 Enter the result name in the **result-name** box. This box can accept up to 17 characters.

The result name must be unique across all result types.

4 Click the **equal-priority-threshold** box in order to share the traffic load in the destinations of the smallest cost group, or among all cost groups if the smallest cost group has only one available destination.

5 Select **pc-ssn** from the result-type list in the Result Destination Data portion of the window. For each result name, you can create a maximum of 16 destinations.

6 Enter a cost and load factor in the **cost** and **load** box. The cost value sets the priority of routing selection for messages. The lower the cost is, the higher the priority. The variation in load factors for different destinations in the same group determines how evenly the load is distributed. The smaller the variation is, the more even is the distribution.

ATTENTION
When you enter 0 in the Load Factor box, the system takes the destination out of routing selection.

7 Select the appropriate remote system identity from the **remote-system-id** drop-down list.

8 Enter the remote point code in the **remote-pointcode** box or select it using the ... box.

9 Enter the SSN in the **ssn** box.

Subsystem Numbers

Subsystem Number	SCCP User Function
0	SSN not known/not used
1	SCCP management
2	reserved
3	ISDN user part
4	operation and maintenance application part (OMAP)
5	mobile application part (MAP)
6	home location register (HLR)
7	visited location register (VLR)
8	mobile switching center (MSC)
9	equipment identification register (EIR)

Subsystem Number	SCCP User Function
10	authentication center (AC for ANSI, AUC for ITU)
11-254	spare
255	reserved for expansion

10 Click **Add**.

—End—

Modifying PC/SSN Results

Step	Action

At the OAMP workstation

1 Click **Configuration>gtt>gtt-result**.

2 Click the **Search** panel tab. Locate the result. Double click the result in the search results to transfer to the administration panel.

3 The following fields can be modified:

- Result-name:
- Equal-priority-threshold:
- Cost:
- Load:
- Remote-system-id:
- Remote-pointcode:
- SSN

4 Click **Modify**.

—End—

Deleting PC/SSN Results

Step	Action

At the OAMP workstation

1 Click **Configuration>gtt>gtt-result**.

2 Click the **Search** panel tab. Locate the result you want to delete. Double click the result in the search results to transfer to the administration panel.

3 Click **Delete**.

ATTENTION
If any GTT translation refers to the PC/SSN result you want to delete, you must first delete the associated GTT translation.

—End—

Configuring GTT, SSN Only Results

To provision a SSN-Only result, perform the following steps:

ATTENTION
There can be only one SSN-Only result per result name.

Adding SSN Only Results

Step	Action

At the OAMP workstation

1 Click **Configuration>gtt>gtt-result**.

2 Click the **system-id** list and select the system identity for this result.

3 Enter the result name in the **result-name** box. This box can accept up to 17 alphanumeric characters.

The result name must be unique across all result types.

4 Click the **equal-priority-threshold** box in order to share the traffic load in the destinations of the smallest cost group, or among all cost groups if the smallest cost group has only one available destination.

5 Select **ssn-only** from the result-type list in the Result Destination Data portion of the window.

6 Enter a cost and load factor in the **cost** and **load** box.

7 Enter the local SSN in the **ssn** box or use the ... box to select the proper Local SSN.

8 Click **Add**.

—End—

Modifying SSN Only Results

Step	Action

At the OAMP workstation

1 Click **Configuration>gtt>gtt-result**.

2 Click the **Search** panel tab. Locate the result you want to modify. Double click the result in the search results to transfer to the administration panel.

3 The following fields can be modified:

- Result-name:
- Equal-priority-threshold:
- Cost:
- Load:
- SSN:

4 Click **Modify**.

—End—

Deleting SSN Only Results

Step	Action

At the OAMP workstation

1 Click **Configuration>gtt>gtt-result**.

2 Click the **Search** panel tab. Locate the result you want to delete. Double click the result in the search results to transfer to the administration panel.

3 Click **Delete**.

ATTENTION
If any GTT translation refers to the SSN Only result you want to delete, you must first delete the associated GTT translation.

—End—

Configuring GTA Results

The PC-GTA result builds on the PC Only result to enable all aspects of the GT in the SCCP called party address to be modified before the message switching unit (MSU) is routed, through the message transfer part (MTP), toward its destination. The PC-GTA routing data set consists of a

- global title indicator (GTI)
- a translation type (TT)
- nature of address (NoA)
- numbering plan (NP)
- global title address (GTA)
- a PC Only result name

For ANSI results, only the GTI, TT, GTA, and PC Only results are used. You can select only one PC Only result for each PC-GTA result.

Adding PC/GTA Results

Use the following procedure to add a PC/GTA result:

Step	Action
	At the OAMP workstation
1	Click **Configuration>gtt>gta-result**.
2	Click the **system-id** list and select the system identity for this result.
3	Enter the result name in the **result-name** box. This box can accept up to 17 characters. The result name must be unique across all result types.
4	Select the GT Indicator from the **gt-indicator** drop-down list. For ANSI, the supported GTI is gta+tt. For ITU14 and ITU24, the supported GTI are: • gta+noa • gta+tt • gta+tt+np • gta+tt+np+noa
5	If the GT Indicator requires a Translation Type, enter it in the **translation-type** box. The range is 0 to 255.

6 If the GT Indicator requires a Nature of Address, enter it in the **nature-of-address** box. The following types of nature of address are available:

- Spare (0)
- Subscriber Number (1)
- Reserved for National Use (2)
- National Significant Number (3)
- International Number (4)
- Spare (5 to 127)

7 If the GT indicator requires a Numbering Plan, select it from the **numbering-plan** drop-down list. Numbering plans supported for ITU are:

- e163-e164
- e212
- e214

8 Enter the PC-Only result name in the **pconly-result-name** box or select it using the ... box.

9 Enter the GTA in the **gt-address** box. The box accepts a value of 3 to 32 hexadecimal digits.

10 Deselect the **replace-gta-option** box if you want to disable the automatic GTA replacement function. By default, the Replace GTA box is checked so that the system automatically replaces GTA digits and the rest of the Global Title in the incoming messages.

11 Click **Add**.

—End—

Modifying PC/GTA Results

Use the following steps to modify a PC/GTA result:

Step	Action
	At the OAMP workstation
1	Click **Configuration>gtt>gta-result**.

2 Click the **Search** panel tab. Locate the result. Double click the result in the search results to transfer the following result information to the administration panel.

- Result-name
- Gt-indicator
- Translation-type
- Nature-of-address
- Numbering-plan
- Pconly-result-name
- Gt-address
- Replace-gta-option

3 Click **Modify**.

—End—

Deleting PC/GTA Results

Use the following steps to delete a PC/GTA result record:

Step	Action
	At the OAMP workstation
1	Click **Configuration>gtt>gtt-result**.
2	Click the **Search** panel tab. Locate the result you want to delete. Double click the result in the search results to transfer to the administration panel.
3	Click **Delete**.

—End—

ATTENTION

If any GTT translation refers to the PC/GTA result you want to delete, you must first delete the associated GTT translation.

Configuring MRGT Result

The Number Portability Message Relay/Global Title (NP MR/GT) result is applicable only to ITU type system identities and is typically used for message relay queries. The NP MR/GT result enables you to change the numbering plan, nature of address (NoA), GT addressing method, global title address (GTA), and final GT result, based on whether a number is ported or non-ported.

Adding MR/GT Results

To add an MR/GT result, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>gtt>mrgt-result**.
2	Click the **system-id** list and select the system identity for this result. Only ITU system Ids are listed (ITU14 or ITU24).
3	Enter the result name in the **result-name** box. This box can accept up to 17 characters. The result name must be unique across all result types.
4	Select the GT Indicator from the **gt-indicator** drop-down list. For ITU14 and ITU24, the supported GTI are:

Global title indicator	Applicability
NOA + GTA	for routing based on the nature of address (NoA) and global title address (GTA) settings
TT + GTA	for routing based on translation type and GTA settings
TT + NumPlan + GTA	for routing based on translation type, numbering plan, and GTA settings
TT + NumPlan + NoA + GTA	for routing based on translation type, numbering plan, nature of address, and GTA settings

5	If the Global Title Indicator selected above requires a Translation Type, enter it in the **translation-type** box. Valid entries are decimal values from 0 to 255.

6 If the GT indicator requires a Numbering Plan, select it from the **numbering-plan** drop-down list. Numbering plans supported for ITU are:

- E.163/E.164
- E.212
- E.214

7 Select the parameters that will be used to modify the Global Title Address of the outgoing message.

a. Select an entry in the **ported-nature-of-address** list. Valid choices are *do-not-change-noa* and *change-noa*. If you select change-noa, then you must enter a valid noa value from 0 to 127 in the **to** box.

b. Select a global title addressing method from the **ported-address-method** list, based on the information provided in the following table:

GTA Addressing Method	Applicability
DN Only	for routing based on the directory number (DN) only
Concatenated (RN+DN)	for routing based on the concatenated: routing number (RN) and DN
CC+DN	for routing based on country code (CC) and DN
Manually Replace GTA...	for routing based on a manually entered GTA
Concatenated (CC+RN+DN)	for routing based on CC, routing number (RN,) and DN
Concatenated (RN+CC+DN)	for routing based on RN, CC, and DN

c. If you selected *gta* in step b, enter a global title address into the **ported-gta** box. Valid entries are up to 32 hexadecimal digits (0 to 9, a to f, A to F).

d. Select a result name for the **ported-result-name** by clicking on the ... box and choosing a valid result from the list. The result name can be any provisioned PC Only or PC/SSN result name. The selected result name is used to relay the message.

8 Select parameters that will be used to modify the global title address of the outgoing message relay message when no matching service is found in the NP database.

a. Select an entry in the **non-ported-nature-of-address** list Valid choices are *do-not-change-noa* and *change-noa*. If you select change-noa, then you must enter a valid noa value from 0 to 127 in the **to** box.

b. Select a global title address method from the **non-ported-address-method** list, based on the information provided in the following table:

GT Addressing Method	Applicability
DN Only	for routing based on the directory number only
CC + DN	for routing based on the dialed number and country code
Manually Replace GTA...	for routing based on a manually entered GTA

c. If you selected gta in step b, enter a global title address into the **non-ported-gta** box. Valid entries are up to 32 hexadecimal digits (0 to 9, a to f, A to F).

d. Select a result name for the **non-ported-result-name** by clicking on the ... box and choosing a valid result the list. The result name can be any provisioned PC Only or PC/SSN result name. The selected result name is used to relay the message.

9 Select a result name for the error-result-name by clicking on the ... box and choosing a valid result from the list. The result name can be any provisioned PC Only or PC/SSN result name. This result is used to route the message when an error occurs during an NP database (NPDB) lookup or the system cannot determine if a number is a CC validation failure or Service Determination Failure.

The TT and numbering-plan are not changed in outgoing messages.

10 Click **Add**.

—End—

Modifying MR/GT Results

To modify an MR/GT result, complete the following steps:

Step	Action

At the OAMP workstation

1 Click **Configuration>gtt>mrgt-result**.

2 Click the **Search** panel tab. Locate the result you want to modify. Double click the result in the search results to transfer to the administration panel.

3 Enter the result name in the **result-name** box. This box can accept up to 17 characters.

The result name must be unique across all result types.

4 Select the GT Indicator from the **gt-indicator** drop-down list. For ITU14 and ITU24, the supported GTI are:

Global title indicator	Applicability
NOA+GTA	for routing based on the nature of address (NoA) and global title address (GTA) settings
TT+GTA	for routing based on translation type and GTA settings
TT+NumPlan+GTA	for routing based on translation type, numbering plan, and GTA settings
TT+NumbPlan+NOA +GTA	for routing based on translation type, numbering plan, nature of address, and GTA settings

5 If the Global Title Indicator selected above requires a Translation Type, enter it in the **translation-type** box. Valid entries are decimal values from 0 to 255.

6 If the GT indicator requires a Numbering Plan, select it from the **numbering-plan** drop-down list. Numbering plans supported for ITU are:

- E.163/E.164
- E.212
- E.214

7 Select parameters that are used to modify the Global Title Address of the outgoing message relay message when a matching service is found in the NP database.

a. Select an entry in the **ported-nature-of-address** list. Valid choices are *do-not-change-noa* and *change-noa*. If you select

change-noa, then you must enter a valid noa value from 0 to 127 in the **to** box.

b. Select a global title addressing method from the **ported-address-method** list, based on the information provided in the following table:

GTA Addressing Method	Applicability
DN Only	for routing based on the directory number only
Concatenated (RN+DN)	for routing based on the concatenated: RN and DN
CC+DN	for routing based on CC and DN
Manually Replace GTA...	for routing based on a manually entered GTA
Concatenated (CC+RN+DN)	for routing based on CC, RN, and DN
Concatenated (RN+CC+DN)	for routing based on RN, CC, and DN

c. If you selected gta in step b, enter a global title address into the **ported-gta** box. Valid entries are up to 32 hexadecimal digits (0 to 9, a to f, A to F).

d. Select a result name for the **ported-result-name** by clicking on the ... box and choosing a valid result the list. The result name can be any provisioned PC Only or PC/SSN result name. The selected result name is used to relay the message.

8 Select parameters that will be used to modify the global title address of the outgoing message relay message when a no matching service is found in the NP database.

a. Select an entry in the **non-ported-nature-of-address** list Valid choices are *do-not-change-noa* and *change-noa*. If you select change-noa, then you must enter a valid noa value from 0 to 127 in the **to** box.

b. Select a global title addressing method from the **non-ported-address-method** list, based on the information provided in the following table:

GT Addressing Method	Applicability
DN Only	for routing based on the dialed number only
CC + DN	for routing based on the dialed number and country code
Manually Replace GTA...	for routing based on a manually entered GTA

c. If you selected gta in step b, enter a global title address into the **ported-gta** box. Valid entries are up to 32 hexadecimal characters (0 to 9, a to f, A to F).

d. Select a result name for the **non-ported-result-name** by clicking on the ... box and choosing a valid result the list. The result name can be any provisioned PC Only or PC/SSN result name. The selected result name is used to relay the message.

9 Select a result name for the error-result-name by clicking on the ... box and choosing a valid result from the list. The result name can be any provisioned PC Only or PC/SSN result name. This result is used to route the message when an error occurs during an NP database (NPDB) lookup or the system cannot determine if a number is an incorrect CC or Service Determination Failed.

The TT and numbering-plan are not changed in outgoing messages.

10 Click **Modify**.

—End—

Deleting MR/GT Results

To delete an NP MR/GT result, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>gtt>mrgt-result**.
2	Click the **Search** panel tab. Locate the result you want to delete. Double click the result in the search results to transfer to the administration panel.

3 Click **Delete**.

—End—

Configuring GTT Translations

The Global Title Translations (GTT) convert application addresses, such as dialed digits, into addresses recognized by SS7.

GTT translations provide the values that are compared against the global title in incoming messages to determine the next step in routing. A translation can be set up as a Singlet by specifying a single value for the low global title and high global title. For example, low global title = 800222, high global title = 800222.

A translation can also be set up as a range by specifying different values for the low global title and high global title. For example, low global title = 800333, high global title = 800444.

The low and high global titles do not need to use the same number of digits. Global titles are treated as character strings, not as numeric values.

Add GTT Translations

To add GTT translations, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>gtt>gtt-translation**.
2	Click the **system-id** list and select the appropriate system identity.
3	Click the **gt-indicator** drop-down list and select a global title indicator. For ANSI, the supported GTI are gta+tt. For ITU14 and ITU24, the supported GTI are: • gta+noa • gta+tt • gta+tt+np • gta+tt+np+noa
4	If the GT Indicator requires a Translation Type, enter it in the **translation-type** box.
5	If the GT Indicator requires a Nature of Address, enter it in the **nature-of-address** box. The following types of nature of address are available:

- Spare (0)
- Subscriber Number (1)
- Reserved for National Use (2)
- National Significant Number (3)
- International Number (4)
- Spare (5-127)

6 If the GT indicator requires a Numbering Plan, select it from the **numbering-plan** drop-down list. Numbering plans supported for ITU are:

- E.163 / E.164
- E.212
- E.214

7 Enter a new low GTA in the **low-gta** box. This box accepts values from 3 to 32 digits.

8 Enter a new high GTA in the **high-gta** box. This box accepts values from 3 to 32 hexadecimal numerals.

9 Enter an existing result name in the **result-name** box on click on the ... box to select a result name.

10 Click **np-gtt-required-option** checkbox if you want this feature activated.

This box can be checked only when the system identity associated with this GTT is also associated with a number portability (NP) local subsystem (LSS).

11 Click **Add** to add this GTT translation to the database.

—End—

Modifying GTT Translations

To modify GTT Translations, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>gtt>gtt-translation**.

2 Click the **Search** panel tab. Locate the translation you want to modify. Double click the result in the search results to transfer to the administration panel.

3 The following fields can be modified:

- low-gta
- high-gta
- result-name
- np-gtt-required-option

4 Click **Modify**.

—End—

Deleting GTT Translations

To delete GTT Translations, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>gtt>gtt-translation**.
2	Click the **Search** panel tab. Locate the translation you want to **Delete**. Double click the result in the search results to transfer to the administration panel.
3	Click **Delete**.

—End—

Configuring Gateway Screening and Message Tracing

Message tracing is a monitoring system that stores a copy of the contents of MSUs (message signaling units) containing specific data matches based on message trace rules that you identify. MSU tracing provides message trapping capabilities that can be used to assist you in detecting and resolving SS7 network problems.

You can perform the following message tracing tasks:

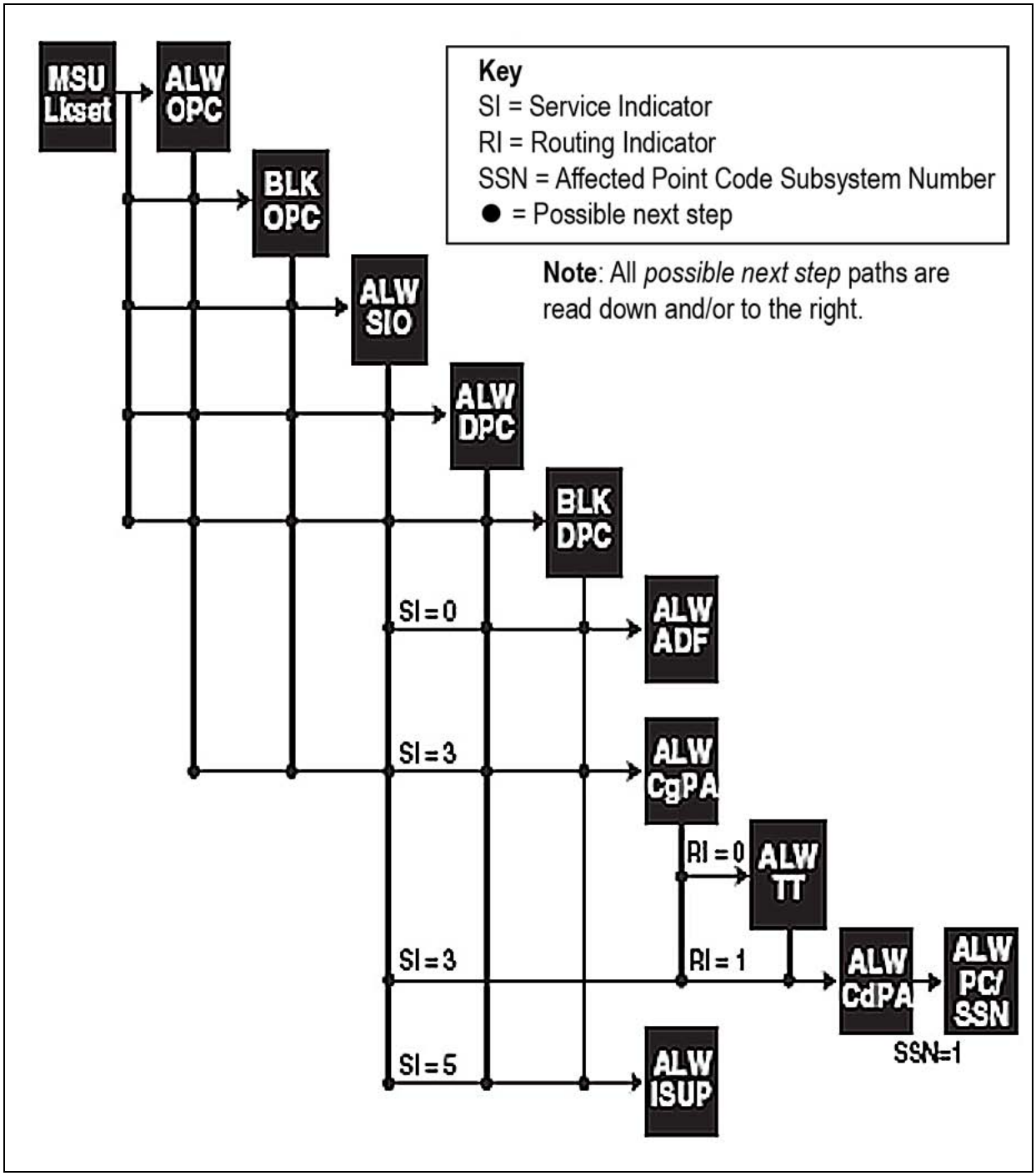
- Control MSU tracing per system identity by provisioning rules in the form of criteria, sets, and rows
- Assign GWS/MSU trace criteria to linksets associated with a selected system identity
- Enable and disable MSU trace per linkset
- View MSU trace records

GWS/MSU Trace Criteria

GWS/MSU trace criteria definitions determine the rules for screening and tracing. GWS and MSU trace share a common rule set definition (for example, one criterion assigned per linkset associated with a system identity).

The following figure details the hierarchy of trace criteria.

Gateway Screening trace criteria



Adding GWS/MSU Trace Criteria

To add a criterion to the database for a system identity, perform the following steps:

Step	Action

At the OAMP workstation

1 Click **Configuration>gws>criteria-name.**

2 Click the **Administration** tab.

3 Click **New**.

4 In the Provisioning Data panel, click the system-id drop-down list and select the system identity you want to associate with the new criteria.

5 Enter a new criteria in the **criteria-name** field.

6 Click **Add**.

—End—

Modifying GWS/MSU Trace Criteria

It is not possible to modify a GWS/MSU Trace Criteria.

Deleting GWS/MSU Trace Criteria

To delete a criterion from the database for a system identity, perform the following steps:

Step	Action

At the OAMP workstation

1 Click **Configuration>gws>criteria-name.**

2 Click the **Search** tab and double click the criteria name you want to delete to transfer to the Administration panel.

3 Click *Delete*.

—End—

Configuring GWS/MSU Trace Criteria for Linksets

Once criteria information is defined, you can assign the criteria (rules) associated with a system identity to a linkset associated with the same system identity. The rules from the assigned criteria will then be used by the GWS/MSU trace processing to determine which MSUs to accept, reject, ignore, and/or trace.

If updates are made to a defined criteria after it has been assigned to one or more linksets, those changes are broadcast to all applicable processors' databases.

Assigning Controls for Linksets

To assign a new criterion name to a linkset associated with a specific system identity, perform the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>gws>control.**
2	Click the **Search** tab and double click the linkset name you want to modify the gateway screening/msu trace parameter in order to transfer to the Administration panel.
3	Select the criteria name from the **criteria-name** drop-down
4	Click the gws-mode drop-down list and make a selection. The following list describes each GWS mode: • "Off" means that gateway screening is not active for the displayed linkset name. • "On" means that gateway screening is active for the displayed linkset name. • "Test" means that gateway screening is in test mode. In this case, the system screens the data, generates MSU reject logs (when appropriate), and updates OMs, but does not discard messages.
5	Click the **inbound-trace-mode** drop-down list and make a selection. This setting contains the overall inbound trace processing using the criteria sets and the rows within the sets. To further modify and control on the row level, use the appropriate SS7 GWS/MSU trace row windows.

The following list describes each MSU trace mode:

- "Disabled” means that inbound MSU trace is not active for the displayed linkset name.
- "Enabled” means that inbound MSU trace is active for the displayed linkset name.

6 If you enabled the inbound trace mode, enter an **inbound-setname**.

7 Click the **outbound-trace-mode** drop-down list and make a selection.

This setting contains the overall outbound trace processing using the criteria sets and the rows within the sets. To further modify and control on the row level, use the appropriate SS7 GWS/MSU trace row windows.

The following list describes each MSU trace mode:

- "Disabled” means that outbound MSU trace is not active for the displayed linkset name.
- "Enabled” means that outbound MSU trace is active for the displayed linkset name.

8 If you enabled the outbound trace mode, enter an **outbound-setname.**

9 Click **Modify**.

—End—

Configuring GWS/MSU Trace Sets

Each GWS/MSU trace criterion associated with a system identity is comprised of sets. Each set contains several different types of rules. MSU data field matching for GWS/MSU trace is controlled by these rules.

GWS and MSU trace use sets from the same criterion. The same sets are used for both GWS and inbound MSU trace; however, for outbound MSU trace, different sets from the criterion can be specified.

Each GWS/MSU trace set can be further defined into rows. These rows determine the MSU data field type-specific rules for GWS/MSU trace. GWS and MSU trace use rows from the same criterion. The same rows are used for both GWS and inbound MSU trace. However, for outbound MSU trace, different rows from the criterion can be specified.

ATTENTION

The same criterion definitions can be used to define two independent groups of sets and rows, contained in the same file. These groups of sets and rows can then be used independently for inbound and outbound processing.

Adding GWS/MSU trace sets

Step	Action

At the OAMP workstation

1 Click **Configuration>gws>criteria-set**.

2 Click the **Administration** tab.

3 Click the **criteria-name** drop-down list and make a selection.

4 Enter a new **set-name**.

5 Click the **set-type** drop-down list and make a selection. Set types are grouped into two categories:

- Use the allowed type (alw) to specify parameters for MSU data matching that are allowed.
- Use the blocked type (blk) to specify parameters for MSU data matching that are not allowed.

6 If you selected the blkopc or blkdpc set type, click the **gws-action** drop-down list and make a selection.

7 If you selected the blkopc or blkdpc set type, click the **trace-action** drop-down list and make a selection.

8 If you selected “continue” either for the **gws-action** or for the **trace-action**, enter a valid **next-set-name**. The next-set-name refers to the set of rules to be applied for screening/tracing after this set. Valid next set types that may be entered are shown in the table "" (page 203).

9 Click **Add**.

—End—

Modifying GWS/MSU trace sets

Step	Action

At the OAMP workstation

1 Click **Configuration>gws>criteria-set**.

You can modify only the gws-action and trace-action for the blkOPC or blkDPC set types through this procedure. If you want to change the set-name or set-type, use the “Deleting GWS/MSU trace sets” procedure and “Adding GWS/MSU trace sets” procedure.

2 Click the Search tab, double-click the criteria-name to be modified.

3 To change the **gws-action**, click the gws-action drop-down list and make a selection.

4 To change the trace-action, click the **trace-action** drop-down list and make a selection.

5 If you selected “continue” either for the **gws-action** or for the **trace-action**, enter a valid **next-set-name**. The next-set-name refers to the set of rules to be applied for screening/tracing after this set. Valid next set types that may be entered are shown in the following table.

Next set definitions

Current Set Type	Possible Next Set Types
BlkDPC	AlwADF AlwCgPA AlwISUP
BlkOPC	AlwSIO AlwDPC BlkDPC AlwCgPA

6 Click **Modify**.

—End—

Deleting GWS/MSU trace sets

Step	Action

At the OAMP workstation

1 Click **Configuration>gws>criteria-set.**

2 Click the **Search** tab, double-click the criteria set to be deleted to transfer to the Administration panel.

3 Click **Delete**.

ATTENTION

You cannot delete a set if it has associated rows.

You cannot delete a set if it is referenced by another set, either at the row level or blocked set level.

—End—

Configuring GWS/MSU AlwOPC (Allowed Originating Point Code) Rows

The AlwOPC rows enable you to specify the necessary OPC values for MSU field matching, in either a range or singlet (single value) form. Each row also indicates the screening/tracing mode for the next set.

Perform the following procedures to add, modify, and delete AlwOPC rows.

Adding AlwOPC rows

Step	Action
	At the OAMP workstation
1	Click **Configuration>gws>criteria-row-alwopc.**
2	Click the Administration tab and click **New**.
3	Select the **criteria-name** for the criteria-name drop-down list.
4	Enter the set name in the **set-name** box or select a set using the … box.
5	To change the gws-action, click the gws-action drop-down list and make a selection. If you want to continue gateway screening from this set to another set, select “continue”. If you do not want to continue gateway screening from this set, select “stop”. Select “ignore” to specify that MSUs received with matching OPC values should be discarded.

ATTENTION
If you choose “ignore”, the reject log normally associated with an MSU is not generated. However, OMs are updated.

6	To change the trace-action, click the trace-action drop-down list and make a selection. If you want to trace received MSUs that have values within the range specified by this row, select “stop-trap”. If you want to continue MSU tracing from this set to another, select “continue”. If you do not want to continue MSU tracing from this set and do not want to trace received MSUs, click “stop-no-trap”.
7	If you selected “continue” either for the gws-action or for the trace-action, enter a valid next-set-name. The next-set-name refers to the set of rules to be applied for screening/tracing after this set.

8 Specify a range (or singlet) of OPCs for comparison with the OPC values of received MSUs during processing for gateway screening and/or MSU tracing. To do this,

a. Enter the first OPC of the range in the **pointcode-low** box

b. Enter the last OPC of the range in the **pointcode-high** box.

These boxes accept up to nine numeric digits and two hyphens. If you want to produce a singlet (single value) rather than a range, enter the same value in both fields.

9 Click **Add**.

10 If necessary, you can click **view-next-set-name** to open the associated window for your next set.

—End—

Modifying AlwOPC rows

Step	Action

At the OAMP workstation

1 Click **Configuration>gws>criteria-row-alwopc.**

2 Click the **Search** panel tab. Locate the AlwOPC row you want to modify. Double-click the AlwOPC row in the search results to transfer to the Administration panel.

3 To change the **gws-action**, click the gws-action drop-down list and make a selection. If you want to continue gateway screening from this set to another set, select “continue”. If you do not want to continue gateway screening from this set, select “stop”. Select “ignore” to specify that MSUs received with matching OPC values should be discarded.

ATTENTION
If you choose “ignore”, the reject log normally associated with an MSU is not generated. However, OMs are updated.

4 To change the trace-action, click the **trace-action** drop-down list and make a selection. If you want to trace received MSUs that have values within the range specified by this row, select “stop-trap”. If you want to continue MSU tracing from this set to another, select “continue”. If you do not want to continue MSU tracing from this set and do not want to trace received MSUs, click “stop-no-trap”.

5 If you selected “continue” either for the **gws-action** or for the **trace-action**, enter a valid **next-set-name**. The next-set-name refers to the set of rules to be applied for screening/tracing after this set. Valid next set types that may be entered are shown in the following table.

Next set definitions

Current Set Type	Possible Next Set Types
AlwOPC	BlkOPC AlwSIO AlwDPC BlkDPC AlwCgPA

6 If you wish, specify a new range (or singlet) of OPCs for comparison with the OPC values of received MSUs during processing for gateway screening and/or MSU tracing. To do this, enter the last OPC of the range in the **pointcode-high** field. These boxes accept up to nine numeric digits and two hyphens.

If you want to produce a singlet (single value) rather than a range, enter the same value in both fields.

You cannot change the value in the pointcode-low field.

7 Click **Modify**.

8 If necessary, you can click **view-next-set-name** to open the associated window for your next set.

—End—

Deleting AlwOPC rows

Step	Action

At the OAMP workstation

1 Click **Configuration>gws>criteria-row-alwopc.**

2 Click the **Search** panel tab. Locate the AlwOPC row you want to delete. Double-click the AlwOPC row in the search results to transfer to the Administration panel.

3 Click **Delete**.

—End—

Configuring GWS/MSU, BlkOPC (Blocked Originating Point Code) Rows

The BlkOPC rows enable you to specify the OPC values to be blocked, in either a range or singlet (single value) form.

Adding BlkOPC Rows

Step	Action
	At the OAMP Workstation
1	Click **Configuration>gws>criteria-row-blkopc**.
2	Click the Administration tab and click **New**.
3	Select the criteria-name from the **criteria-name** drop-down list.
4	Enter the set name in the **set-name** box or select a set using the … box.
5	Specify a range (or singlet) of OPCs for comparison with the OPC values of received MSUs during processing for gateway screening and/or MSU tracing. To do this, enter the last OPC of the range in the **pointcode-high** field. These boxes accept up to nine numeric digits and two hyphens. If you want to produce a singlet (single value) rather than a range, enter the same value in both fields.
6	Click **Add**.

—End—

Modifying BlkOPC Rows

Step	Action
	At the OAMP Workstation
1	Click **Configuration>gws>criteria-row-blkopc.**
2	Click the **Search** panel tab. Locate the BlkOPC row you want to modify. Double click the BlkOPC row in the search results to transfer to the administration panel.

3 Specify a range (or singlet) of OPCs for comparison with the OPC values of received MSUs during processing for gateway screening and/or MSU tracing. To do this, enter the first OPC of the range in the **pointcode-low** field and enter the last OPC of the range in the **pointcode-high** field. These boxes accept up to nine numeric digits and two hyphens

If you want to produce a singlet (single value) rather than a range, enter the same value in both fields.

You cannot change the value in the pointcode-low field.

4 Click **Modify**.

—End—

Deleting BlkOPC Rows

Step	Action

At the OAMP Workstation

1 Click **Configuration>gws>criteria-row-blkopc.**

2 Click the **Search** panel tab. Locate the BlkOPC row you want to delete. Double click the BlkOPC row in the search results to transfer to the administration panel.

3 Click **Delete**.

—End—

Configuring GWS/MSU, AlwSIO (Allowed Service Indicator Octets) Rows

The AlwSIO rows enable you to specify the necessary service information octets (SIO) values for MSU field matching, in either range or singlet (single value) form. You can also add in the H0/H1 headings (when SIO = 0, 1, or 2). Each row also indicates the screening/tracing mode for the next set.

Adding AlwSIO Rows

Step	Action
	At the OAMP workstation
1	Click **Configuration>gws>criteria-row-alwsio.**
2	Click the Administration tab and click **New**
3	Select the criteria-name from the **criteria-name** drop-down list.
4	Enter the set name in the **set-name** box or select a set using the … box.
5	To change the **gws-action**, click the gws-action drop-down list and make a selection. If you want to continue gateway screening from this set to another set, select “continue”. If you do not want to continue gateway screening from this set, select “stop”. Select “ignore” to specify that MSUs received with matching OPC values should be discarded.

ATTENTION
If you choose “ignore”, the reject log normally associated with an MSU is not generated. However, OMs are updated.

6	To change the trace-action, click the trace-action drop-down list and make a selection. If you want to trace received MSUs that have values within the range specified by this row, select “stop-trap”. If you want to continue MSU tracing from this set to another, select “continue”. If you do not want to continue MSU tracing from this set and do not want to trace received MSUs, click “stop-no-trap”.
7	If you selected “continue” either for the gws-action or for the trace-action, enter a valid next-set-name. The next-set-name refers to the set of rules to be applied for screening/tracing after this set.
8	Select a new service indicator range (or singlet). To specify a range, click the is-high drop-down list and make a service indicator code

selection. If you want to produce a singlet (single value) rather than a range, select the same value in both fields.

ATTENTION

You cannot change the service indicator value in the **si-low** field.

You cannot use the snm (0), sccp (3), tup (4), or isup (5) service indicator codes in a range. These four service indicator codes can be entered only as singlets.

Signaling handling functions use service indicators to distribute messages. The following table shows how service indicator codes are allocated in U.S. networks.

Service indicator allocation

SI Code	SI Message Name
SNM (0)	Signaling network management messages
SNT (1)	Signaling network management messages (regular messages)
SNTS (2)	Signaling network management messages (special messages)
SCCP (3)	Signaling Connection Control Part messages
TUP (4)	Telephone User Part messages
ISUP (5)	ISDN User Part messages
DUPC (6)	Data User Part (call- and circuit-related messages)
DUPF (7)	DUP (7) Data User Part (facility registration and cancellation messages)
MTP-TEST (8)	MTP Testing User Part messages
B-ISUP (9)	Broadband ISDN User Part messages
S-ISUP (10)	Satellite ISDN User Part messages
spare (11)	Spare
spare (12)	Spare
BICC (13)	
spare (14)	Spare
reserved (15)	Reserved for individual network use

9 If you chose snm (0), snt (1), or snts (2) in the service indicator list (si-low or si-high), you need to specify an H0 heading code range (or singlet). To do this, enter an H0 heading code in the h0-high field.

If you want to produce a singlet (single value) rather than a range, enter the same value in fields.

ATTENTION

For H0/H1 ranges, always use multiple range entries for complete control of transmitted and received messages.

You cannot change the h0-low field.

H0 heading codes identify message groups. The following tables list each H0 message and associated name for the SNM (0), SNT (1), and SNTS (2) service indicators.

SNM (0) heading code messages

Heading Code	Heading Code Message Name
1	CHM Changeover and changeback messages
2	ECM Emergency changeover messages
3	FCM Signaling traffic flow control messages
4	TFM Transfer-prohibited, transfer-allowed, and transfer-restricted messages
5	RSM Signaling routeset test messages
6	MIM Management inhibiting messages
7	TRM Traffic restart messages
8	DLM Signaling data link connection order messages
9	Not applicable
10	UFC MTP user flow control messages
11-15	Not applicable

SNT (1) and SNTS (2) heading code messages

Heading Code	Heading Code Message Name
1	Test Msg Test Message
2-15	Not applicable

10 If you chose snm (0), snt (1), or snts (2) in the service indicator list (si-low or si-high), you also need to specify an H1 heading code range. To do this, enter an H1 heading code in the h1-high field. If you want to produce a singlet (single value) rather than a range, enter the same value in fields.

ATTENTION

For H0/H1 ranges, always use multiple range entries for complete control of transmitted and received messages.

You cannot change the value in the h1-low field.

H1 heading code ranges identify message groups. The following tables list each H0 message and associated H1 messages.

H0 heading codes and SNM H1 messages

H0 Heading Codes	Associated H1 Heading Codes and Messages
1 - CNM Changeover and changeback messages	1 - COO Changeover order signal 2 - COA Changeover acknowledgment signal 5 - CBD Changeback declaration signal 6 - CBA Changeback acknowledgment signal 3, 4, 7–15 - Not applicable
2 - ECM Emergency changeover messages	1 - ECO Emergency changeover order signal 2 - ECA Emergency changeover acknowledgment signal 3–15 - Not applicable
3 - FCM Signaling traffic flow control messages	1 - RCT Signaling routeset congestion test signal 2 - TFC Transfer controlled signal 3–15 - Not applicable
4 - TFM Transfer-prohibited, transfer-allowed, and transfer-restricted messages	1 - TFP Transfer prohibited signal 2 - TCP Transfer cluster prohibited signal 3 - TFR Transfer restricted signal 4 - TCR Transfer cluster restricted signal 5 - TFA Transfer allowed signal 6 - TCA Transfer cluster allowed signal 7–15 - Not applicable
5 - RSM Signaling routeset test messages	1 - RSP Signaling routeset test prohibited signal 2 - RSR Signaling routeset test restricted signal 3 - RCP Signaling routeset test cluster prohibited signal 4 - RCR Signaling routeset test cluster restricted signal 5–15 - Not applicable

H0 Heading Codes	Associated H1 Heading Codes and Messages
6 - MIM Management inhibiting messages	1 - LIN Link inhibit message 2 - LUN Link uninhibit message 3 - LIA Link inhibit acknowledgment message 4 - LUA Link uninhibit acknowledgment message 5 - LID Link inhibit denied message 6 - LFU Link forced uninhibit message 7 - LLI Link local inhibit test signal 8 - LRI Link remote inhibit test signal 9–15 - Not applicable
7 - TRM Traffic restart messages	1 - TRA Traffic restart allowed signal 2 - TRW Traffic restart waiting signal 3–15 - Not applicable
8 - DLM Signaling data link connection order messages	1 - DLC Signaling data link connection order signal 2 - CSS Connection successful signal 3 - CNS Connection not successful signal 4 - CNP Connection not possible signal 5–15 - Not applicable
9 - Not applicable	1–15 - Not applicable
10 - UFC MTP user flow control messages	1 - UPU User part unavailable 2–15 - Not applicable
11–15 - Not applicable	1–15 - Not applicable

H0 heading codes and SNT and SNTS H1 messages

H0 Heading Code	Associated H1 Heading Codes
1 - Test Msg	1 - SLT Signaling link test
Signaling test message	2 - SLTA Signaling link test acknowledgment 3–15 - Not applicable
2–15 - Not applicable	1–15 - Not applicable

11 Choose a congestion priority range (or singlet). To specify a range, click the **priority-low** drop-down list and make a congestion priority code selection. Then click the **priority-high** drop-down list and make a congestion priority code selection.

If the AlwSIO row is associated with a system identity that uses the ITU 14-bit protocol, you can enter only zero in the priority-low and priority-high lists.

If you want to produce a singlet (single value) rather than a range, select the same value in both fields.

Congestion in ANSI networks is measured in four levels: 0 (lowest) through 3 (highest). These congestion levels provide a way to manage messages during times of elevated congestion.

Each network message is assigned a congestion priority code (level). Messages with high priority levels are more likely to be sent, even when congestion is high.

The following table shows congestion priority codes and associated explanations.

ANSI congestion priority code explanations

Priority	Explanation
priority (0)	Application-specific (for example, Circuit Validation Test)
priority (1)	Application-specific (for example, Initial Address)
priority (2)	Application-specific (for example, Release Complete)
priority (3)	Assigned to MTP and SCCP messages that are critical to the performance of the signaling network

12 Choose a network indicator code range (or singlet). To specify a range, click the ni-low drop-down list and make a network indicator code selection and then click the ni-high drop-down list and make a network indicator code selection. If you want to produce a singlet (single value) rather than a range, select the same value in both fields.

The network indicator allows you to discriminate between international and national messages. The following table shows network indicator codes and associated message names.

Network indicator codes and associated messages

Network Indicator Code	Network Indicator Message Name
international (0)	International message
international spare (1)	Spare (for international use only)
national (2)	National network
national spare (3)	Reserved for national use

13 Click **Add**.

14 If necessary, you can click **view-next-set-name** to open the associated window for your next set.

—End—

Modifying AlwSIO Rows

To modify and AlwSIO row, perform the following steps:

Step	Action

At the OAMP workstation

1 Click **Configuration>gws>criteria-row-alwsio.**

2 Click the **Search** panel tab. Locate the AlwSIO row you want to modify. Double click the AlwSIO row in the search results to transfer to the administration panel.

3 To change the **gws-action**, click the gws-action drop-down list and make a selection. If you want to continue gateway screening from this set to another set, select “continue”. If you do not want to continue gateway screening from this set, select “stop”. Select “ignore” to specify that MSUs received with matching OPC values should be discarded.

ATTENTION
If you choose “ignore”, the reject log normally associated with an MSU is not generated. However, OMs are updated.

4 To change the **trace-action**, click the trace-action drop-down list and make a selection. If you want to trace received MSUs that have values within the range specified by this row, select “stop-trap”. If you want to continue MSU tracing from this set to another, select “continue”. If you do not want to continue MSU tracing from this set and do not want to trace received MSUs, click “stop-no-trap”.

5 If you selected “continue” either for the **gws-action** or for the **trace-action**, enter a valid **next-set-name**. The next-set-name refers to the set of rules to be applied for screening/tracing after

this set. Valid next set types that can be entered are shown in the following table.

Next set definitions

Current Set Type	Possible Next Set Types
alwSIO	alwDPC alwADF alwCgPA alwCdPA alwISUP

6 If necessary, select a new service indicator range (or singlet). To specify a range, click the **si-high** drop-down list and make a service indicator code selection. If you want to produce a singlet (single value) rather than a range, select the same value in both fields.

ATTENTION
You cannot change the service indicator value in the si-low field.

You cannot use the snm (0), sccp (3), tup (4), or isup (5) service indicator codes in a range. These four service indicator codes can be entered only as singlets.

Signaling handling functions use service indicators to distribute messages. The following table shows how service indicator codes are allocated in American (U.S.) networks.

Service indicator allocation

SI Code	SI Message Name
SNM (0)	Signaling network management messages
SNT (1)	Signaling network management messages (regular messages)
SNTS (2)	Signaling network management messages (special messages)
SCCP (3)	Signaling Connection Control Part messages
TUP (4)	Telephone User Part messages
ISUP (5)	ISDN User Part messages
DUPC (6)	Data User Part (call- and circuit-related messages)
DUPF (7)	DUP (7)Data User Part (facility registration and cancellation messages)
MTP-TEST (8)	MTP Testing User Part messages

SI Code	SI Message Name
B-ISUP (9)	Broadband ISDN User Part messages
S-ISUP (10)	Satellite ISDN User Part messages
spare (11)	Spare
spare (12)	Spare
BICC (13)	
spare (14)	Spare
reserved (15)	Reserved for individual network use

7 If you chose snm (0), snt (1), or snts (2) in the service indicator list (si-low or si-high), you need to specify an H0 heading code range (or singlet). To do this, enter the H0 heading code in the h0-low field. Next, enter the **H0** heading code in the h0-high field. If you want to produce a singlet (single value) rather than a range, enter the same value in fields.

ATTENTION
For H0/H1 ranges, always use multiple range entries for complete control of transmitted and received messages.

H0 heading codes identify message groups. The following tables list each H0 message and associated name for the snm (0), snt (1), and snts (2) service indicators.

SNM (0) heading code messages

Heading Code	Heading Code Message Name
1	CHM Changeover and changeback messages
2	ECM Emergency changeover messages
3	FCM Signaling traffic flow control messages
4	TFM Transfer-prohibited, transfer-allowed, and transfer-restricted messages
5	RSM Signaling routeset test messages
6	MIM Management inhibiting messages
7	TRM Traffic restart messages
8	DLM Signaling data link connection order messages
9	Not applicable

Heading Code	Heading Code Message Name
10	UFC MTP user flow control messages
11-15	Not applicable

SNT (1) and SNTS (2) heading code messages

Heading Code	Heading Code Message Name
1	Test Msg Test Message
2-15	Not applicable

8 If you chose snm (0), snt (1), or snts (2) in the service indicator list (si-low or si-high), you also need to specify an H1 heading code range. To do this, click the **h1-low** drop-down list and make a selection. Next, click the **h1-high** drop-down list and make a selection. If you want to produce a singlet (single value) rather than a range, choose the same value in fields.

ATTENTION
For H0/H1 ranges, always use multiple range entries for complete control of transmitted and received messages.

H1 heading code ranges identify message groups. The following tables list each H0 message and associated H1 messages.

H0 heading codes and SNM H1 messages

H0 Heading Codes	Associated H1 Heading Codes and Messages
1 - CNM Changeover and changeback messages	1 - COO Changeover order signal 2 - COA Changeover acknowledgment signal 5 - CBD Changeback declaration signal 6 - CBA Changeback acknowledgment signal 3, 4, 7–15 - Not applicable
2 - ECM Emergency changeover messages	1 - ECO Emergency changeover order signal 2 - ECA Emergency changeover acknowledgment signal 3–15 - Not applicable
3 - FCM Signaling traffic flow control messages	1 - RCT Signaling routeset congestion test signal 2 - TFC Transfer controlled signal 3–15 - Not applicable

H0 Heading Codes	Associated H1 Heading Codes and Messages
4 - TFM Transfer-prohibited, transfer-allowed, and transfer-restricted messages	1 - TFP Transfer prohibited signal 2 - TCP Transfer cluster prohibited signal 3 - TFR Transfer restricted signal 4 - TCR Transfer cluster restricted signal 5 - TFA Transfer allowed signal 6 - TCA Transfer cluster allowed signal 7–15 - Not applicable
5 - RSM Signaling routeset test messages	1 - RSP Signaling routeset test prohibited signal 2 - RSR Signaling routeset test restricted signal 3 - RCP Signaling routeset test cluster prohibited signal 4 - RCR Signaling routeset test cluster restricted signal 5–15 - Not applicable
6 - MIM Management inhibiting messages	1 - LIN Link inhibit message 2 - LUN Link uninhibit message 3 - LIA Link inhibit acknowledgment message 4 - LUA Link uninhibit acknowledgment message 5 - LID Link inhibit denied message 6 - LFU Link forced uninhibit message 7 - LLI Link local inhibit test signal 8 - LRI Link remote inhibit test signal 9–15 - Not applicable
7 - TRM Traffic restart messages	1 - TRA Traffic restart allowed signal 2 - TRW Traffic restart waiting signal 3–15 - Not applicable
8 - DLM Signaling data link connection order messages	1 - DLC Signaling data link connection order signal 2 - CSS Connection successful signal 3 - CNS Connection not successful signal 4 - CNP Connection not possible signal 5–15 - Not applicable
9 - Not applicable	1-15 - Not applicable
10 - UFC MTP user flow control messages	1 - UPU User part unavailable 2–15 - Not applicable
11–15 - Not applicable	1–15 - Not applicable

H0 heading codes and SNT and SNTS H1 messages

H0 Heading Code	Associated H1 Heading Codes
1 - Test Msg	1 - SLT Signaling link test

H0 Heading Code	Associated H1 Heading Codes
Signaling test message	2 - SLTA Signaling link test acknowledgment 3–15 - Not applicable
2–15 - Not applicable	1–15 - Not applicable

9 If necessary, change the congestion priority range (or singlet). To do this, click the **priority-high** drop-down list and make a congestion priority code selection.

ATTENTION

You cannot change the congestion priority value in the priority-low field.

If the AlwSIO row is associated with a system identity that uses the ITU 14-bit protocol, you can only enter zero in the priority-low and priority-high lists.

If you want to produce a singlet (single value) rather than a range, select the same value in both fields.

Congestion in ANSI networks is measured in four levels: 0 (lowest) through 3 (highest). These congestion levels provide a way to manage messages during times of elevated congestion.

Each network message is assigned a congestion priority code (level). Messages with high priority levels are more likely to be sent, even when congestion is high.

The following table shows congestion priority codes and associated explanations.

ANSI congestion priority code explanations

Priority	Explanation
priority (0)	Application-specific (for example, Circuit Validation Test)
priority (1)	Application-specific (for example, Initial Address)
priority (2)	Application-specific (for example, Release Complete)
priority (3)	Assigned to MTP and SCCP messages that are critical to the performance of the signaling network

10 If necessary, change the network indicator code range (or singlet). To do this, click the **ni-high** drop-down list and make a network indicator code selection. If you want to produce a singlet (single value) rather than a range, select the same value in both fields.

ATTENTION
You cannot change the network indicator code in the ni-low field.

The network indicator allows you to discriminate between international and national messages. The following table shows network indicator codes and associated message names.

Network indicator codes and associated messages

Network Indicator Code	Network Indicator Message Name
international (0)	International message
international spare (1)	Spare (for international use only)
national (2)	National network
national spare (3)	Reserved for national use

11 Click **Modify**.

12 If necessary, you can click **view-next-set-name** to open the associated window for your next set.

—End—

Deleting AlwSIO Rows

To delete an AlwSIO row, perform the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>gws>criteria-row-alwsio.**
2	Click the **Search** panel tab. Locate the AlwSIO row you want to delete. Double click the AlwSIO row in the search results to transfer to the administration panel.
3	Click **Delete**.

—End—

Configuring GWS/MSU AlwDPC (Allowed Destination Point Code) Rows

The AlwDPC rows enable you to specify the necessary destination point code (DPC) values for MSU field matching, in either a range or singlet (single value) form. Each row also indicates the screening/tracing mode for the next set.

Adding AlwDPC Rows

To add an AlwDPC row, perform the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>gws>criteria-row-alwdpc.**
2	Click the Administration tab and click **New**.
3	Select the **criteria-name** for the criteria-name drop-down list.
4	Enter the set name in the **set-name** box or select a set using the … box.
5	To change the **gws-action**, click the gws-action drop-down list and make a selection. If you want to continue gateway screening from this set to another set, select “continue”. If you do not want to continue gateway screening from this set, select “stop”. Select “ignore” to specify that MSUs received with matching DPC values should be discarded.

ATTENTION
If you choose “ignore”, the reject log normally associated with an MSU is not generated. However, OMs are updated.

6	To change the **trace-action**, click the trace-action drop-down list and make a selection. If you want to trace received MSUs that have values within the range specified by this row, select “stop-trap”. If you want to continue MSU tracing from this set to another, select “continue”. If you do not want to continue MSU tracing from this set and do not want to trace received MSUs, click “stop-no-trap”.
7	If you selected “continue” either for the **gws-action** or for the **trace-action**, enter a valid **next-set-name**. The next-set-name refers to the set of rules to be applied for screening/tracing after

this set. Valid next set types that can be entered are shown in the following table.

Next set definitions

Current Set Type	Possible Next Set Types
alwDPC	blkDPC alwADF alwCgPA alwISUP

8 Specify a range (or singlet) of DPCs for comparison with the DPC values of received MSUs during processing for gateway screening and/or MSU tracing. To do this, enter the first DPC of the range in the pointcode-low field and enter the last DPC of the range in the pointcode-high field. These boxes accept up to nine numeric digits and two hyphens.

If you want to produce a singlet (single value) rather than a range, enter the same value in both fields.

9 Click **Add**.

10 If necessary, you can click **view-next-set-name** to open the associated window for your next set.

—End—

Modifying AlwDPC Rows

To modify an existing AlwDPC row, perform the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>gws>criteria-row-alwdpc.**
2	Click the **Search** panel tab. Locate the AlwDPC row you want to modify. Double click the AlwDPC row in the search results to transfer to the administration panel.
3	To change the **gws-action**, click the gws-action drop-down list and make a selection. If you want to continue gateway screening from this set to another set, select “continue”. If you do not want to continue gateway screening from this set, select “stop”. Select “ignore” to specify that MSUs received with matching DPC values should be discarded.

ATTENTION
If you choose “ignore”, the reject log normally associated with an MSU is not generated. However, OMs are updated.

4 To change the trace-action, click the trace-action drop-down list and make a selection. If you want to trace received MSUs that have values within the range specified by this row, select “stop-trap”. If you want to continue MSU tracing from this set to another, select “continue”. If you do not want to continue MSU tracing from this set and do not want to trace received MSUs, click “stop-no-trap”.

5 If you selected “continue” either for the **gws-action** or for the **trace-action**, enter a valid next-set-name. The next-set-name refers to the set of rules to be applied for screening/tracing after this set. Valid next set types that can be entered are shown in the following table.

Next set definitions

Current Set Type	Possible Next Set Types
alwDPC	blkDPC alwADF alwCgPA alwISUP

6 If you wish, specify a new range (or singlet) of DPCs for comparison with the DPC values of received MSUs during processing for gateway screening and/or MSU tracing. To do this, enter the last DPC of the range in the pointcode-high field. These boxes accept up to nine numeric digits and two hyphens.

If you want to produce a singlet (single value) rather than a range, enter the same value in both fields.

You cannot change the value in the pointcode-low field.

7 Click **Modify**.

8 If necessary, you can click **view-next-set-name** to open the associated window for your next set.

—End—

Deleting AlwDPC Rows

To delete an existing AlwDPC row, perform the following steps:

Step	Action

At the OAMP workstation

1 Click **Configuration>gws>criteria-row-alwdpc.**

2 Click the **Search** tab. Locate the AlwDPC row you want to delete. Double click the AlwDPC row in the search results to transfer to the administration panel.

3 Click **Delete**.

—End—

Configuring GWS/MSU, BlkDPC (Blocked Destination Point Code) Rows

The BlkDPC rows enable you to specify the DPC values to be blocked, in either a range or singlet (single value) form.

Adding BlkDPC Rows

Step	Action
At the OAMP Workstation	
1	Click **Configuration>gws>criteria-row-blkdpc.**
2	Click the Administration tab and click **New**.
3	Select the **criteria-name** for the criteria-name drop-down list.
4	Enter the set name in the **set-name** box or select a set using the … box.
5	Specify a range (or singlet) of DPCs for comparison with the DPC values of received MSUs during processing for gateway screening and/or MSU tracing. To do this, enter the first DPC of the range in the **pointcode-low** field and enter the last DPC of the range in the **pointcode-high** field. These boxes accept up to nine numeric digits and two hyphens. If you want to produce a singlet (single value) rather than a range, enter the same value in both fields.
6	Click **Add**.

—End—

Modifying BlkDPC Rows

Step	Action
At the OAMP Workstation	
1	Click **Configuration>gws>criteria-row-blkdpc.**
2	Click the **Search** panel tab. Locate the BlkDPC row you want to modify. Double click the BlkDPC row in the search results to transfer to the administration panel.

3 If you wish, specify a new range (or singlet) of DPCs for comparison with the DPC values of received MSUs during processing for gateway screening and/or MSU tracing. To do this, enter the last DPC of the range in the **pointcode-high** field. These boxes accept up to nine numeric digits and two hyphens.

   If you want to produce a singlet (single value) rather than a range, enter the same value in both fields.

   You cannot change the value in the pointcode-low field.

4 Click **Modify**.

—End—

Deleting BlkDPC Rows

Step	Action

At the OAMP Workstation

1 Click **Configuration>gws>criteria-row-blkdpc.**

2 Click the **Search** panel tab. Locate the BlkDPC row you want to modify. Double click the BlkDPC row in the search results to transfer to the administration panel.

3 Click **Delete**.

—End—

Configuring GWS/MSU, AlwADF (Allowed Affected Destination Field) Rows

The AlwADF rows enable you to specify the necessary point code values for MSU field matching, in either a range or singlet (single value) form. AlwADF screening checks that the affected point code in TFx/TCx, TFC, and signaling-route-set-test messages are allowed.

Adding AlwADF Rows

Step	Action

At the OAMP Workstation

1 Click **Configuration>gws>criteria-row-alwadf.**

2 Click the Administration tab and click **New**.

3 Select the **criteria-name** for the criteria-name drop-down list.

4 Enter the set name in the **set-name** box or select a set using the … box.

5 To change the **gws-action**, click the gws-action drop-down list and make a selection. If you do not want to continue gateway screening from this set, select “stop”. Select “ignore” to specify that MSUs received with matching OPC values should be discarded.

> **ATTENTION**
> If you choose “ignore”, the reject log normally associated with an MSU will not be generated. However, OMs are updated.

6 To change the trace-action, click the **trace-action** drop-down list and make a selection. If you want to trace received MSUs that have values within the range specified by this row, select “stop-trap”. If you do not want to trace received MSUs, click “stop-no-trap”.

7 Specify a range (or singlet) of affected PCs for comparison with the affected PC values of received MSUs during processing for gateway screening and/or MSU tracing. To do this,

a. Enter the first affected PC of the range in the pointcode-low box.

b. Enter the last affected PC of the range in the **pointcode-high** box.

These boxes accept up to nine numeric digits and two hyphens. If you want to produce a singlet (single value) rather than a range, enter the same value in both fields.

8 Click **Add**.

9 If necessary, you can click **view-next-set-name** to open the associated window for your next set.

—End—

Modifying AlwADF Rows

Step	Action

At the OAMP Workstation

1 Click **Configuration>gws>criteria-row-alwadf.**

2 Click the **Search** panel tab. Locate the AlwADF row you want to modify. Double click the AlwADF row in the search results to transfer to the administration panel.

3 To change the gws-action, click the **gws-action** drop-down list and make a selection. Select “ignore” to specify that MSUs received with matching OPC values should be discarded. Select “stop” if you don’t select “ignore”.

ATTENTION
If you choose “ignore”, the reject log normally associated with an MSU is not generated. However, OMs are updated.

4 To change the trace-action, click the **trace-action** drop-down list and make a selection. If you want to trace received MSUs that have values within the range specified by this row, select “stop-trap”. If you do not want to trace receive MSUs, select “stop-no-trap”.

5 If you wish, specify a new range (or singlet) of point codes for comparison with the point code values of received MSUs during processing for gateway screening and/or MSU tracing. To do this, enter the last point code of the range in the pointcode-high field. This field accepts up to nine numeric digits and two hyphens.

If you want to produce a singlet (single value) rather than a range, enter the same value in both fields.

You cannot change the value in the pointcode-low field.

6 Click **Modify**.

—End—

Deleting AlwADF Rows

Step	Action

At the OAMP Workstation

1 Click **Configuration>gws>criteria-row-alwadf.**

2 Click the **Search** panel tab. Locate the AlwADF row you want to delete. Double click the AlwADF row in the search results to transfer to the administration panel.

3 Click **Delete**.

—End—

Configuring GWS/MSU AlwCgPA (Allowed Calling Party) Rows

The AlwCgPA rows enable you to specify the point code and subsystem number (SSN) values for MSU field matching, in either a range or singlet (single value) form. As part of the AlwCgPA row, you can also specify a SCCP message type and CdPA routing indicator. Each row also indicates the screening/tracing mode for the next set.

Adding AlwCgPA Rows

To add an AlwCgPA row, perform the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>gws>criteria-row-alwcgpa.**
2	Click the Administration tab and click **New**.
3	Select the criteria-name for the **criteria-name** drop-down list.
4	Enter the set name in the **set-name** box or select a set using the … box.
5	To change the **gws-action**, click the **gws-action** drop-down list and make a selection. If you want to continue gateway screening from this set to another set, select “continue”. If you do not want to continue gateway screening from this set, select “stop”. Select “ignore” to specify that MSUs received with matching OPC values should be discarded.

ATTENTION

If you choose ignore, the reject log normally associated with an MSU is not generated. However, OMs are updated.

6	To change the trace-action, click the trace-action drop-down list and make a selection. If you want to trace received MSUs that have values within the range specified by this row, select “stop-trap”. If you want to continue MSU tracing from this set to another, select “continue”. If you do not want to continue MSU tracing from this set and do not want to trace received MSUs, click “stop-no-trap”.
7	If you selected “continue” either for the **gws-action** or for the **trace-action**, enter a valid **next-set-name**. The next-set-name

refers to the set of rules to be applied for screening/tracing after this set. (Refer to "Next set definitions" (page 236).)

8 Specify a range (or singlet) of point codes for comparison with the point code values of received MSUs during processing for gateway screening and/or MSU tracing. To do this, enter the first point code of the range in the pointcode-low field and enter the last point code of the range in the pointcode-high field. These fields accept up to nine numeric digits and two hyphens.

If you want to produce a singlet (single value) rather than a range, enter the same value in both fields.

9 Specify a range (or singlet) of SSNs for comparison with the SSNs of received MSUs during processing for gateway screening and/or MSU tracing. To do this, enter the first SSN of the range in the ssn-low field and enter the last SSN of the range in the ssn-high field.

If you want to produce a singlet (single value) rather than a range, enter the same value in both fields.

The following table shows subsystem numbers (SSN) and associated SCCP user functions.

Subsystem numbers and associated SCCP functions

Subsystem Number	SCCP User Function
0	SSN not known/not used
1	SCCP management
2	reserved
3	ISDN user part
4	OMAP
5	Mobile application part (MAP)
6	Home location register (HLR)
7	Visited location register (VLR)
8	Mobile switching center (MSC)
9	Equipment identification register (EIR)
10	Authentication center (AC for ANSI, AUC for ITU)
11-254	Spare
255	Reserved for expansion

10 Click the **sccp-msg-type** drop-down list and select an SCCP message type. Refer to the following table for additional information about each available choice in this list.

SCCP message information

SCCP Measurement Types	SCCP Measurement Names
UDT (9)	Unit data type
XUDT (17)	Extended unit data type
UDTS (10)	Unit data type service
XUDTS (18)	Extended unit data type service

11 Click the **cdpa-routing-indicator** drop-down list and select a called party routing indicator. You can route on GTT, DPC, or both (match on either GTT or DPC).

12 Click **Add**.

13 If necessary, you can click **view-next-set-name** to open the associated window for your next set.

—End—

Modifying AlwCgPA Rows

To modify an existing AlwCgPA record, perform the following steps:

Step	Action

At the OAMP workstation

1 Click **Configuration>gws>criteria-row-alwcgpa.**

2 Click the **Search** panel tab. Locate the AlwCGPA row you want to modify. Double click the AlwCGPA row in the search results to transfer to the administration panel

3 To change the gws-action, click the **gws-action** drop-down list and make a selection. If you want to continue gateway screening from this set to another set, select “continue”. If you do not want to continue gateway screening from this set, select “stop”. Select “ignore” to specify that MSUs received with matching OPC values should be discarded.

ATTENTION
If you choose ignore, the reject log normally associated with an MSU is not generated. However, OMs are updated.

4 To change the trace-action, click the **trace-action** drop-down list and make a selection. If you want to trace received MSUs that have values within the range specified by this row, select stop-trap". If you want to continue MSU tracing from this set to another, select "continue". If you do not want to continue MSU tracing from this set and do not want to trace received MSUs, click "stop-no-trap".

5 If you selected "continue" either for the **gws-action** or for the **trace-action**, enter a valid next-set-name. The **next-set-name** refers to the set of rules to be applied for screening/tracing after this set. Valid next set types that can be entered are shown in the following table.

Next set definitions

Current set type	Possible next set types
alwCgPA	• alwTT • alwCdPA (if the RTS indicator equals Rte on DPC, or both)

6 If you wish, specify a new range (or singlet) of point codes for comparison with the point code values of received MSUs during processing for gateway screening and/or MSU tracing. To do this, enter the last point code of the range in the pointcode-high field. This field accepts up to nine numeric digits and two hyphens.

If you want to produce a singlet (single value) rather than a range, enter the same value in both fields.

You cannot change the value in the pointcode-low field.

7 If you wish, specify a new range (or singlet) of SSNs for comparison with the SSNs of received MSUs during processing for gateway screening and/or MSU tracing. To do this, enter the last SSN of the range in the ssn-high field.

If you want to produce a singlet (single value) rather than a range, enter the same value in both fields.

You cannot change the value in the ssn-low field.

The following table shows subsystem numbers (SSN) and associated SCCP user functions.

Subsystem numbers and associated SCCP functions

Subsystem Number	SCCP User Function
0	SSN not known/not used
1	SCCP management
2	reserved
3	ISDN user part
4	OMAP
5	Mobile application part (MAP)
6	Home location register (HLR)
7	Visited location register (VLR)
8	Mobile switching center (MSC)
9	Equipment identification register (EIR)
10	Authentication center (AC for ANSI, AUC for ITU)
11-254	Spare
255	Reserved for expansion

8 Click **Modify**.

9 If necessary, you can click **view-next-set-name** to open the associated window for your next set.

—End—

Deleting AlwCgPA Rows

To delete an existing AlwCgPA row, perform the following steps:

Step	Action

At the OAMP workstation

1 Click **Configuration>gws>criteria-row-alwcgpa.**

2 Click the **Search** panel tab. Locate the AlwCGPA row you want to delete. Double click the AlwCGPA row in the search results to transfer to the administration panel

3 Click **Delete**.

—End—

Configuring GWS MSU AlwTT (Allowed Translation Type) Rows

The AlwTT rows enable you to specify the translation type values for MSU field matching, in either a range or singlet (single value) form. Each row also indicates the screening/tracing mode for the next set.

In ANSI-based networks, all SCCP messages contain translation type information. In ITU-based networks, it is possible for an SCCP message not to contain translation type information. If you are screening by Allowed Translation Type on an ITU 14-bit based system identity and an SCCP message without translation type information is detected, GWS stops and the message is allowed into the network.

Adding AlwTT Rows

Step	Action
	At the OAMP Workstation
1	Click **Configuration>gws>criteria-row-alwtt.**
2	Click the Administration tab and click **New**.
3	Select the criteria-name for the **criteria-name** drop-down list.
4	Enter the set name in the **set-name** box or select a set using the … box.
5	To change the gws-action, click the **gws-action** drop-down list and make a selection. If you want to continue gateway screening from this set to another set, select “continue”. If you do not want to continue gateway screening from this set, select “stop”. Select “ignore” to specify that MSUs received with matching OPC values should be discarded.

ATTENTION
If you choose ignore, the reject log normally associated with an MSU is not generated. However, OMs are updated.

6	To change the trace-action, click the trace-action drop-down list and make a selection. If you want to trace received MSUs that have values within the range specified by this row, select “stop-trap”. If you want to continue MSU tracing from this set to another, select “continue”. If you do not want to continue MSU tracing from this set and do not want to trace received MSUs, click “stop-no-trap”.

7 If you selected “continue” either for the **gws-action** or for the **trace-action**, enter a valid **next-set-name**. The next-set-name refers to the set of rules to be applied for screening/tracing after this set. Valid next set types that can be entered are shown in the following table.

Next set definitions

Current Set Type	Possible Next Set Types
alwTT	alwCdPA

8 Specify a range (or singlet) of translation types for comparison with the values of received MSUs during processing for gateway screening and/or MSU tracing. To do this, enter the first translation type of the range in the **trans-type-low** field and enter the last translation type of the range in the **trans-type-high** field. These fields accept up to three numeric digits.

If you want to produce a singlet (single value) rather than a range, enter the same value in both fields.

The following table shows the translation type codes and associated application/translation groups.

Translation type and associated groups

Translation Type Code	Application/Translation Group
0	Reserved
1	Identification code
2	Reserved
3	Cellular nationwide roaming service
4	Global title = global code
5	Calling name delivery
6	Reserved
7	Message waiting
8	SCP-assisted call processing applications
9-31	Internetwork applications
32-191	Spare
192-250	Network-specific applications
251	Reserved
252	Network-specific applications
253	Reserved

Translation Type Code	Application/Translation Group
254	Used for internetwork applications, in some cases.
255	Reserved

9 Click **Add.**

10 If necessary, you can click **view-next-set-name** to open the associated window for your next set.

—End—

Modifying AlwTT Rows

Step Action

At the OAMP Workstation

1 Click **Configuration>gws>criteria-row-alwtt.**

2 Click the **Search** panel tab. Locate the AlwTT row you want to modify. Double click the AlwTT row in the search results to transfer to the administration panel.

3 To change the gws-action, click the **gws-action** drop-down list and make a selection. If you want to continue gateway screening from this set to another set, select “continue”. If you do not want to continue gateway screening from this set, select “stop”. Select “ignore” to specify that MSUs received with matching OPC values should be discarded.

ATTENTION
If you choose ignore, the reject log normally associated with an MSU is not generated. However, OMs are updated.

4 To change the trace-action, click the **trace-action** drop-down list and make a selection. If you want to trace received MSUs that have values within the range specified by this row, select “stop-trap”. If you want to continue MSU tracing from this set to another, select “continue”. If you do not want to continue MSU tracing from this set and do not want to trace received MSUs, select “stop-no-trap”.

5 If you selected “continue” either for the **gws-action** or for the **trace-action**, enter a valid **next-set-name**. The next-set-name refers to the set of rules to be applied for screening/tracing after

this set. Valid next set types that can be entered are shown in the following table.

Next set definitions

Current Set Type	Possible Next Set Types
alwTT	alwCdPA

6 If you wish, specify a new range (or singlet) of translation types for comparison with the values of received MSUs during processing for gateway screening and/or MSU tracing. To do this, enter the last translation type of the range in the **trans-type-high** field. This field accepts up to three numeric digits.

If you want to produce a singlet (single value) rather than a range, enter the same value in both fields.

You cannot change the value in the trans-type-low field.

The following table shows the translation type codes and associated application/translation groups.

Translation type and associated groups

Translation Type Code	Application/Translation Group
0	Reserved
1	Identification code
2	Reserved
3	Cellular nationwide roaming service
4	Global title = global code
5	Calling name delivery
6	Reserved
7	Message waiting
8	SCP-assisted call processing applications
9-31	Internetwork applications
32-191	Spare
192-250	Network-specific applications
251	Reserved
252	Network-specific applications
253	Reserved
254	Used for internetwork applications, in some cases.
255	Reserved

7 Click **Modify**.

8 If necessary, you can click **view-next-set-name** to open the associated window for your next set.

—End—

Deleting AlwTT Rows

Step	Action

At the OAMP Workstation

1 Click *Configuration>gws>criteria-row-alwtt.*

2 Click the **Search** panel tab. Locate the AlwTT row you want to delete. Double click the AlwTT row in the search results to transfer to the administration panel.

3 Click **Delete**.

—End—

Configuring GWS/MSU AlwCdPA (Allowed Called Party) Rows

The AlwCdPA rows enable you to specify the point code and called party SSN values for MSU field matching. As part of the AlwCdPA row, you can also specify the SCMG format id if the CdPA SSN is set to 1.

Perform the following procedures to add, modify, and delete AlwCdPA rows.

Adding AlwCdPA rows

Step	Action
At the OAMP workstation	
1	Click **Configuration>gws>criteria-row-alwcdpa.**
2	Click the Administration tab and click **New**.
3	Select the criteria-name for the **criteria-name** drop-down list.
4	Enter the set name in the **set-name** box or select a set using the … box.
5	To change the gws-action, click the **gws-action** drop-down list and make a selection. If you want to continue gateway screening from this set to another set, select “continue”. If you do not want to continue gateway screening from this set, select “stop”. Select “ignore” to specify that MSUs received with matching OPC values should be discarded.

ATTENTION
If you choose “ignore”, the reject log normally associated with an MSU is not generated. However, OMs are updated.

6	To change the trace-action, click the **trace-action** drop-down list and make a selection. If you want to trace received MSUs that have values within the range specified by this row, select “stop-trap”. If you want to continue MSU tracing from this set to another, select “continue”. If you do not want to continue MSU tracing from this set and do not want to trace received MSUs, click “stop-no-trap”.
7	If you selected “continue” either for the **gws-action** or for the **trace-action**, enter a valid **next-set-name**. The next-set-name refers to the set of rules to be applied for screening/tracing after

this set. Valid next set types that can be entered are shown in the following table.

Next set definitions

Current set type	Possible next set types
alwCdPA and CdPA SSN=1	alwPC/SSN

8 Specify a range (or singlet) of point codes for comparison with the point code values of received MSUs during processing for gateway screening and/or MSU tracing. To do this, enter the first point code of the range in the **pointcode-low** field and enter the last point code of the range in the **pointcode-high** field. These fields accept up to nine numeric digits and two hyphens.

If you want to produce a singlet (single value) rather than a range, enter the same value in both fields.

9 Specify a subsystem number (SSN) for comparison with the SSNs of received MSUs during processing for gateway screening and/or MSU tracing. To do this, enter the SSN in the **cdpa-ssn** field.

The following table shows subsystem numbers and associated SCCP user functions.

Subsystem numbers and associated SCCP functions

Subsystem Number	SCCP User Function
0	SSN not known/not used
1	SCCP management
2	reserved
3	ISDN user part
4	OMAP
5	Mobile application part (MAP)
6	Home location register (HLR)
7	Visited location register (VLR)
8	Mobile switching center (MSC)
9	Equipment identification register (EIR)
10	Authentication center (AC for ANSI, AUC for ITU)
11-254	Spare
255	Reserved for expansion

10 If you entered 1 in the **cdpa-ssn** field, enter an SCCP management (SCMG) format in the scmg-format-id. Refer to the following table for additional information about each available choice for this field.

SCMG format ID expansions

SCMG Format ID	Expansion
Not Specified	
SSA (1)	Subsystem available
SSP (2)	Subsystem prohibit
SST (3)	Subsystem test
SOR (4)	Subsystem out-of-service routing
SOG (5)	Subsystem out-of-service grant
SBR (253)	Subsystem backup routing
SNR (254)	Subsystem normal routing
SRT (255)	Subsystem routing status test

ATTENTION
Do not enter an SCCP management format ID unless you entered 1 in the **cdpa-ssn** box.

11 Click **Add**.

12 If necessary, you can click **view-next-set-name** to open the associated window for your next set.

—End—

Modifying AlwCdPA rows

Step	Action

At the OAMP workstation

1 Click **Configuration>gws>criteria-row-alwcdpa.**

2 Click the **Search** panel tab. Locate the AlwCDPA row you want to modify. Double-click the AlwCDPA row in the search results to transfer to the Administration panel.

3 To change the gws-action, click the **gws-action** drop-down list and make a selection. If you want to continue gateway screening from this set to another set, select “continue”. If you do not want to continue gateway screening from this set, select “stop”. Select

"ignore" to specify that MSUs received with matching OPC values should be discarded.

ATTENTION
If you choose ignore, the reject log normally associated with an MSU is not generated. However, OMs are updated.

4 To change the trace-action, click the **trace-action** drop-down list and make a selection. If you want to trace received MSUs that have values within the range specified by this row, select "stop-trap". If you want to continue MSU tracing from this set to another, select "continue". If you do not want to continue MSU tracing from this set and do not want to trace received MSUs, select "stop-no-trap".

5 If you selected "continue" either for the **gws-action** or for the **trace-action**, enter a valid **next-set-name**. The next-set-name refers to the set of rules to be applied for screening/tracing after this set. Valid next set types that can be entered are shown in the following table.

Next set definitions

Current set type	Possible next set types
alwCdPA and CdPA SSN=1	alwPC/SSN

6 If you wish, specify a new range (or singlet) of point codes for comparison with the point code values of received MSUs during processing for gateway screening and/or MSU tracing. To do this, enter the last point code of the range in the pointcode-high field. These fields accept up to nine numeric digits and two hyphens.

If you want to produce a singlet (single value) rather than a range, enter the same value in both fields.

You cannot change the value in the pointcode-low field.

7 Click **Modify**.

8 If necessary, you can click **view-next-set-name** to open the associated window for your next set.

—End—

Deleting AlwCdPA rows

Step	Action
	At the OAMP workstation
1	Click **Configuration>gws>criteria-row-alwcdpa.**
2	Click the **Search** panel tab. Locate the AlwCDPA row you want to delete. Double-click the AlwCDPA row in the search results to transfer to the Administration panel.
3	Click **Delete**.

—End—

Configuring GWS/MSU PC_SSN (Allowed Point Code/Subsystem Number) Rows

The PC_SSN row allows you to specify the SCCP SCMG affected point code and subsystem number values for MSU field matching, in either a range or singlet (single value) form.

Adding PC_SSN Rows

Step	Action
	At the OAMP Workstation
1	Click **Configuration>gws>criteria-row-alwpcssn**.
2	Click the Administration tab and click **New**.
3	Select the criteria-name for the **criteria-name** drop-down list.
4	Enter the set name in the **set-name** box or select a set using the … box.
5	To change the gws-action, click the **gws-action** drop-down list and make a selection. If you want to continue gateway screening from this set to another set, select “continue”. If you do not want to continue gateway screening from this set, select “stop”. Select “ignore” to specify that MSUs received with matching OPC values should be discarded.

ATTENTION
If you choose “ignore”, the reject log normally associated with an MSU is not generated. However, OMs are updated.

6	To change the trace-action, click the **trace-action** drop-down list and make a selection. If you want to trace received MSUs that have values within the range specified by this row, select “stop-trap”. If you want to continue MSU tracing from this set to another, select “continue”. If you do not want to continue MSU tracing from this set and do not want to trace received MSUs, click “stop-no-trap”.
7	Specify a range (or singlet) of affected point codes for comparison with the point code values of received MSUs during processing for gateway screening and/or MSU tracing. To do this, enter the first point code of the range in the **pointcode-low** field and enter the last point code of the range in the **pointcode-high** field. These fields accept up to nine numeric digits and two hyphens.

If you want to produce a singlet (single value) rather than a range, enter the same value in both fields.

8 Specify a range (or singlet) of affected SSNs for comparison with the SSNs of received MSUs during processing for gateway screening and/or MSU tracing. To do this, enter the first SSN of the range in the ssn-low field and enter the last SSN of the range in the ssn-high field. These fields accept up to three numeric digits.

If you want to produce a singlet (single value) rather than a range, enter the same value in both fields.

The following table shows subsystem numbers (SSN) and associated SCCP user functions.

Subsystem numbers and associated SCCP functions

Subsystem Number	SCCP User Function
0	SSN not known/not used
1	SCCP management
2	reserved
3	ISDN user part
4	OMAP
5	Mobile application part (MAP)
6	Home location register (HLR)
7	Visited location register (VLR)
8	Mobile switching center (MSC)
9	Equipment identification register (EIR)
10	Authentication center (AC for ANSI, AUC for ITU)
11-254	Spare
255	Reserved for expansion

9 Click **Add**.

—End—

Modifying PC_SSN Rows

Step	Action

At the OAMP Workstation

1 Click **Configuration>gws>criteria-row-alwpcssn**.

2 Click the **Search** panel tab. Locate the AlwPCSSN row you want to modify. Double click the AlwPCSSN row in the search results to transfer to the administration panel.

3 To change the gws-action, click the **gws-action** drop-down list and make a selection. If you want to continue gateway screening from this set to another set, select “continue”. If you do not want to continue gateway screening from this set, select “stop”. Select “ignore” to specify that MSUs received with matching OPC values should be discarded.

ATTENTION

If you choose “ignore”, the reject log normally associated with an MSU is not generated. However, OMs are updated.

4 To change the trace-action, click the **trace-action** drop-down list and make a selection. If you want to trace received MSUs that have values within the range specified by this row, select “stop-trap”. If you do not want to trace received MSUs, select “stop-no-trap”.

5 If you wish, specify a new range (or singlet) of affected point codes for comparison with the point code values of received MSUs during processing for gateway screening and/or MSU tracing. To do this, enter the last point code of the range in the pointcode-high field. This field accepts up to nine numeric digits and two hyphens.

If you want to produce a singlet (single value) rather than a range, enter the same value in both fields.

You cannot change the value in the pointcode-low field.

6 If you wish, specify a new range (or singlet) of affected SSNs for comparison with the SSNs of received MSUs during processing for gateway screening and/or MSU tracing. To do this, enter the last SSN of the range in the ssn-high field.

If you want to produce a singlet (single value) rather than a range, enter the same value in both fields.

You cannot change the value in the ssn-low field.

The following table shows subsystem numbers (SSN) and associated SCCP user functions.

Subsystem numbers and associated SCCP functions

Subsystem Number	SCCP User Function
0	SSN not known/not used
1	SCCP management
2	reserved
3	ISDN user part
4	OMAP
5	Mobile application part (MAP)
6	Home location register (HLR)
7	Visited location register (VLR)
8	Mobile switching center (MSC)
9	Equipment identification register (EIR)
10	Authentication center (AC for ANSI, AUC for ITU)
11-254	Spare
22	Reserved for expansion

7 Click **Modify**.

8 Click **Yes** in the confirmation window that displays.

—End—

Deleting PC_SSN Rows

Step	Action

At the OAMP Workstation

1 Click **Configuration>gws>criteria-row-alwpcssn.**

2 Click the **Search** panel tab. Locate the AlwPCSSN row you want to delete. Double click the AlwPCSSN row in the search results to transfer to the administration panel.

3 Click **Delete**.

—End—

Configuring GWS/MSU, AlwISUP (Allowed ISDN User Part) Rows

The AlwISUP rows enable you to specify the ISUP message type values for MSU field matching, in either a range or singlet (single value) form.

Adding AlwISUP Rows

Step	Action
	At the OAMP Workstation
1	Click **Configuration>gws>criteria-row-alwisup**.
2	Click the Administration tab and click **New**.
3	Select the criteria-name for the **criteria-name** drop-down list.
4	Enter the set name in the **set-name** box or select a set using the ... box.
5	To change the gws-action, click the **gws-action** drop-down list. If you do not want to continue gateway screening from this set, select stop. Select ignore to specify that MSUs received with matching OPC values should be discarded.

ATTENTION
If you choose ignore, the reject log normally associated with an MSU is not generated. However, OMs are updated.

6	To change the trace-action, click the **trace-action** drop-down list and make a selection. If you want to trace received MSUs that have values within the range specified by this row, select "stop-trap". If you do not want to trace received MSUs, click "stop-no-trap".
7	Specify a range (or singlet) of ISUP message types for comparison with the ISUP message types of received MSUs during processing for gateway screening and/or MSU tracing. To do this, enter the first ISUP message type of the range in the isup-msg-type-low field and enter the last ISUP message type of the range in the isup-msg-type-high field. If you want to produce a singlet (single value) rather than a range, enter the same value in both fields. The following table shows ISUP message type numbers and names.

ISUP message information

Message Type Number	Message Type Name
1	Initial address
2	Subsequent address
3	Information request
4	Information
5	Continuity
6	Address complete
7	Connect
8	Forward transfer
9	Answer
10	UBM
11	ATREL
15	RLSD
12	Release
13	Suspend
14	Resume
16	Release complete
17	Continuity check request
18	Reset circuit
19	Blocking
20	Unblocking
21	Blocking Acknowledgment
22	Unblocking Acknowledgment
23	Circuit Group Reset
24	Circuit Group Blocking
25	Circuit Group Unblocking
26	Circuit Group Blocking Acknowledgment
27	Circuit Group Unblocking Acknowledgment
28	Call modification request
29	Call modification completed
30	Call modification reject
31	Facility request

Message Type Number	Message Type Name
32	Facility accepted
33	Facility reject
34	Facility deactivated
35	Facility information
36	Loop back acknowledgment
37	Closed user group selection and validation request
38	Closed user group selection and validation response
39	Delayed release
40	Pass along
41	Circuit group reset acknowledgment
42	Circuit query
43	Circuit query response
44	Call progress
45	User-to-user information
46	Unequipped circuit identification code
47	Confusion
48	Overload
49	CRG2
233	Circuit reservation acknowledgment
234	Circuit reservation
235	Circuit validation response
236	Circuit validation test
237	Exit
239	A7LPA
251	FVBF
252	FVB
253	FANG
254	EIN
255	AUF

8 Click **Add**.

—End—

Modifying AlwISUP Rows

Step	Action

At the OAMP Workstation

1 Click **Configuration>gws>criteria-row-alwisup**.

2 Click the **Search** panel tab. Locate the AlwISUP row you want to modify. Double click the AlwISUP row in the search results to transfer to the administration panel.

3 To change the gws-action, click the **gws-action** drop-down list and make a selection. Select ignore to specify that MSUs received with matching OPC values should be discarded. If you did not select ignore, select stop.

> **ATTENTION**
> If you choose ignore, the reject log normally associated with an MSU is not generated. However, OMs are updated.

4 To change the trace-action, click the **trace-action** drop-down list and make a selection. If you want to trace received MSUs that have values within the range specified by this row, select "stop-trap". If you do not want to trace received MSUs, select "stop-no-trap".

5 If you wish, specify a new range (or singlet) of ISUP message types for comparison with the ISUP message types of received MSUs during processing for gateway screening and/or MSU tracing. To do this, enter the last ISUP message type of the range in the isup-msg-type-high field.

If you want to produce a singlet (single value) rather than a range, enter the same value in both fields.

You cannot change the value in the isup-msg-type-low field.

The following table shows ISUP message type numbers and names.

ISUP message information

Message Type Number	Message Type Name
1	Initial address
2	Subsequent address
3	Information request

Message Type Number	Message Type Name
4	Information
5	Continuity
6	Address complete
7	Connect
8	Forward transfer
9	Answer
10	UBM
11	ATREL
15	RLSD
12	Release
13	Suspend
14	Resume
16	Release complete
17	Continuity check request
18	Reset circuit
19	Blocking
20	Unblocking
21	Blocking Acknowledgment
22	Unblocking Acknowledgment
23	Circuit Group Reset
24	Circuit Group Blocking
25	Circuit Group Unblocking
26	Circuit Group Blocking Acknowledgment
27	Circuit Group Unblocking Acknowledgment
28	Call modification request
29	Call modification completed
30	Call modification reject
31	Facility request
32	Facility accepted
33	Facility reject
34	Facility deactivated
35	Facility information
36	Loop back acknowledgment

Message Type Number	Message Type Name
37	Closed user group selection and validation request
38	Closed user group selection and validation response
39	Delayed release
40	Pass along
41	Circuit group reset acknowledgment
42	Circuit query
43	Circuit query response
44	Call progress
45	User-to-user information
46	Unequipped circuit identification code
47	Confusion
48	Overload
49	CRG2
233	Circuit reservation acknowledgment
234	Circuit reservation
235	Circuit validation response
236	Circuit validation test
237	Exit
239	A7LPA
251	FVBF
252	FVB
253	FANG
254	EIN
255	AUF

6 Click **Modify**.

—End—

Deleting AlwISUP Rows

Step	Action
	At the OAMP Workstation
1	Click **Configuration>gws>criteria-row-alwisup**.
2	Click the **Search** panel tab. Locate the AlwISUP row you want to modify. Double click the AlwISUP row in the search results to transfer to the administration panel.
3	Click **Delete**.
	—End—

Configuring the MSU Trace Viewer

The MSU Trace Viewer is a tool that enables you to view traced MSUs passing through your network in real time.

Tracing Current Messages

Step	Action
	At the OAMP Workstation
1	Click **Configuration>gws>msu-trace**.
2	Click the **Realtime** tab.
3	You can establish a limit for the number of MSU trace records that display. Click the drop-down list in the box located in the lower left corner of the Realtime window and make a selection.
4	To view current messages, click the **Start** button and then click **Yes** in the confirmation window that displays. The MSU trace records display sequentially as table rows. If you want to change the order of display, click in any of the parameter column headings in the Retrieval Results pane. An arrow displays within the column heading indicating the direction of the order, either first to last or last to first. To reverse the order, click within the column heading. Refer to the following table for a description of each MSU Trace table column.

MSU trace viewer information

Column Name	Description
date-time	The date and time of the MSU
linkset-name	The associated linkset name
slc	Signaling link code
direction	The direction of the link
network-indicator	National or international
service-indicator	Service indicator code
destination-pointcode	The destination point code
originating-pointcode	The originating point code
message-type	A sub-field of the service indicator
raw-data	Hex format of raw bytes of the message

5 To end the current MSU trace viewer session, click the **Stop** button and then click **Yes** in the confirmation window that displays.

6 You can post a single MSU trace record, a selection of MSU trace records, or all the MSU trace records that display to an HTML file. To select a single MSU trace record, place the cursor over the record and click. To select a range of contiguous records, press the Shift key and hold it down while you move the cursor over the range of records that you wish to select, and then release the Shift key; the range of selected records is highlighted. To select the entire list of records, place the cursor over the first record in the list and click, use the scroll bar to scroll to the end of the list, and then press and hold down the shift key while clicking on the last record in the list; the entire list is highlighted.

To select a range of non-contiguous MSU trace records, press the Ctrl key and hold it down while you click on individual records that you wish to select; the range of selected records is highlighted.

a. After you have selected the MSU trace records to post, click the **Post** button.

b. In the top right-hand corner of the window, click the "Export posted records" icon.

c. In response to the confirmation window that displays, click **Yes**.

d. In the Export window that displays, select a location for the file on your workstation, select a name for the file that will be posted, and then click **Save**.

7 To display the complete information about an MSU trace record, double-click the MSU trace record in the display.

—End—

Message Trace Tool

The USP message trace tool is used to monitor and decode SS7 messages. This tool has a GUI interface that enables users to monitor and decode incoming and outgoing ANSI messages, including M3UA, MTP3, SCCP, and ISUP on a per-link or per-ASP basis. This tool complements, but does not replace, the existing MSU trace tool, that is part of the gateway screening subsystem.

Prior to USP 10.0, third-party software running on PCs was used to monitor traffic between the USP and other network nodes. This method was not the preferred way to debug the network on the customer site and resulted in discarding messages unnecessarily.

ATTENTION

The activation of the message trace functionality impacts the capacity of the link. The scope of the impact varies depending on the rate of traffic and the type and size of the messages to be decoded. You should not activate the message trace tool on congested links.

The message trace tool provides the following two methods to define message tracing criteria:

- The tool enables filtering of messages by providing byte string to match with a given offset to the message and the length of the given byte string.
- The tool enables specific field/value matching as a filter. The fields that can be used as filters are listed in the following table:

Filtered fields		
Originating Point Code	M3UA Message Types	SCCP GT Translation Type
Destination Point Code	ISUP Message Types	SCCP GT Nature of Address
Network Indicator	Affected Point Code in SCMG messages	SCCP Addressing Information (dialed digits)
Message Priority	Affected Point Code in M3UA messages	SCMG Format Identifier
MTP3 Network Management Message Types H0H1	SCCP Subsystem Number	ISUP Circuit Identification Code
SCCP Message Types	SCCP Point Code	ISUP IAM CdPN (dialed digits)

Configuring the Message Trace Tool

The message trace tool is configured from USP GUI interface. From the msg-trace menu, accessible from the USP Configuration menu, you can perform the following tasks:

- Add and delete a message trace ruleset.
- Create a new set of message trace rules, modify existing rules, and delete a current record.
- Assign message trace controls.
- Monitor message trace data.

Configure message trace rulesets

The message trace ruleset definition is used to determine the rules for tracing. Perform the following procedures to add, modify, and delete a message trace ruleset.

Adding message trace rulesets

Step	Action
	At the OAMP workstation
1	Open the message trace ruleset window. To do this, click **Configuration>msg-trace>msg-trace-ruleset.**
2	Click the **Administration** tab.
3	Click **New**.
4	In the **ruleset-name** field, enter a name for the new ruleset. The name can be up to 16 alphanumeric characters in length.
5	Click **Add**.
	—End—

Modifying message trace rulesets

You cannot modify message trace rulesets.

Deleting message trace rulesets

Step	Action
	At the OAMP workstation

1 Click **Configuration>msg-trace>msg-trace-ruleset.**

2 Click the **Search** tab and double-click the ruleset name you want to delete to transfer to the Administration window.

3 Click **Delete**.

—End—

Configure message trace rules

When you have defined your ruleset, you can perform the following procedures to add, modify, and delete message trace rules. You then apply these rules to any link or path using the msg-trace-control screen. The message will only be captured and forwarded to the USP GUI if all of the rules are satisfied.

Adding new message trace rules

Step	Action
	At the OAMP workstation
1	Click **Configuration>msg-trace>msg-trace-rule.**
2	Click the **Administration** tab.
3	Click **New**.
4	Select the ruleset name for which you want to add message trace rules from the **ruleset-name** drop-down menu.
5	Enter a value to identify the rule in the **rule-id** field.
6	Select a protocol from the **protocol** drop-down menu. For tracing on IPS7 links, select M3UA. For tracing on SS7 links, select MTP3, SCCP, or ISUP.
7	Select a match type from the **match-type-selector** drop-down menu. If you select a match type of **match-field**, proceed to . If you select a match type of **match-raw**, proceed to Step 11.
8	Select a field name from the **field-name** drop-down menu.
9	Select a condition from the **condition** drop-down menu.

10 Enter value in the value field. Refer to the following table for a list of valid field name values and condition combinations. After you enter a value, proceed to Step 13.

Conditions									
Field names	**EQ**	**NE**	**GT**	**GE**	**LT**	**LE**	**SW**	**EW**	**CNT**
m3ua msg type	A	A	NA	NA	NA	NA	NA	NA	NA
m3ua apc	PC	PC	PC	PC	PC	PC	NA	NA	NA
mtp opc	PC	PC	PC	PC	PC	PC	NA	NA	NA
mtp dpc	PC	PC	PC	PC	PC	PC	NA	NA	NA
mtp ni	N	N	N	N	N	N	NA	NA	NA
mtp priority	N	N	N	N	N	N	NA	NA	NA
snm msg type	A	A	NA	NA	NA	NA	NA	NA	NA
snm apc	PC	PC	PC	PC	PC	PC	NA	NA	NA
sccp msg type	A	A	NA	NA	NA	NA	NA	NA	NA
cdpa pc	PC	PC	PC	PC	PC	PC	NA	NA	NA

Legend A = Alpha characters are valid
N = Numeric characters are valid
A/N = Alpha numeric mix is valid
PC = Point code is valid
NA - Not applicable for that field name/condition combination

Conditions EQ = Equal to
NE = Not equal to
GT = Greater than
GE = Greater than or equal to
LT = Less than LE = Less than or equal to
SW = Starts with
EW = Ends with CNT = Contains

Valid entries for rules include:
m3ua msg type: err, ntfy, data, duna, dave, daud, scon, dupu, drst, aspup, aspdn, beat, aspupack, aspdnack, aspac, aspia, aspacack, aspiaack
All point code fields: Must be a complete point code. Partial point codes will not be accepted.
snm msg type: All valid SNM message types supported by ANSI protocols. For example: sltm, slta, coo, coa, tfp
sccp msg type: All valid SCCP message types supported by ANSI protocols. For example: cr, cc, cref, udt
scmg msg type: All valid SCCP Management message types supported by ANSI protocols. For example: ssa, sst, ssp
isup msg type: All valid ISDN User Part message types supported by ANSI protocols. For example: iam, anm, acm

Conditions									
Field names	**EQ**	**NE**	**GT**	**GE**	**LT**	**LE**	**SW**	**EW**	**CNT**
cdpa ssn	N	N	N	N	N	N	NA	NA	NA
cdpa tt	N	N	N	N	N	N	NA	NA	NA
cdpa noa	N	N	N	N	N	N	NA	NA	NA
cdpa gta	NA	NA	NA	NA	NA	NA	N	N	N
cdpa pc	N	N	N	N	N	N	NA	NA	NA
cgpa ssn	N	N	N	N	N	N	NA	NA	NA
cgpa tt	N	N	N	N	N	N	NA	NA	NA
cgpa noa	N	N	N	N	N	N	NA	NA	NA
cgpa gta	NA	NA	NA	NA	NA	NA	N	N	N
scmg msg type	A	A	NA	NA	NA	NA	NA	NA	NA
scmg apc	PC	PC	PC	PC	PC	PC	NA	NA	NA
scmg assn	N	N	N	N	N	N	NA	NA	NA
isup msg type	A	A	NA	NA	NA	NA	NA	NA	NA

Legend A = Alpha characters are valid
N = Numeric characters are valid
A/N = Alpha numeric mix is valid
PC = Point code is valid
NA - Not applicable for that field name/condition combination

Conditions EQ = Equal to
NE = Not equal to
GT = Greater than
GE = Greater than or equal to
LT = Less than LE = Less than or equal to
SW = Starts with
EW = Ends with CNT = Contains

Valid entries for rules include:
m3ua msg type: err, ntfy, data, duna, dave, daud, scon, dupu, drst, aspup, aspdn, beat, aspupack, aspdnack, aspac, aspia, aspacack, aspiaack
All point code fields: Must be a complete point code. Partial point codes will not be accepted.
snm msg type: All valid SNM message types supported by ANSI protocols. For example: sltm, slta, coo, coa, tfp
sccp msg type: All valid SCCP message types supported by ANSI protocols. For example: cr, cc, cref, udt
scmg msg type: All valid SCCP Management message types supported by ANSI protocols. For example: ssa, sst, ssp
isup msg type: All valid ISDN User Part message types supported by ANSI protocols. For example: iam, anm, acm

Conditions									
Field names	**EQ**	**NE**	**GT**	**GE**	**LT**	**LE**	**SW**	**EW**	**CNT**
isup cic	N	N	N	N	N	N	NA	NA	NA
isup cdpn addr	NA	NA	NA	NA	NA	NA	N	N	N

Legend A = Alpha characters are valid
N = Numeric characters are valid
A/N = Alpha numeric mix is valid
PC = Point code is valid
NA - Not applicable for that field name/condition combination

Conditions EQ = Equal to
NE = Not equal to
GT = Greater than
GE = Greater than or equal to
LT = Less than LE = Less than or equal to
SW = Starts with
EW = Ends with CNT = Contains

Valid entries for rules include:
m3ua msg type: err, ntfy, data, duna, dave, daud, scon, dupu, drst, aspup, aspdn, beat, aspupack, aspdnack, aspac, aspia, aspacack, aspiaack
All point code fields: Must be a complete point code. Partial point codes will not be accepted.
snm msg type: All valid SNM message types supported by ANSI protocols. For example: sltm, slta, coo, coa, tfp
sccp msg type: All valid SCCP message types supported by ANSI protocols. For example: cr, cc, cref, udt
scmg msg type: All valid SCCP Management message types supported by ANSI protocols. For example: ssa, sst, ssp
isup msg type: All valid ISDN User Part message types supported by ANSI protocols. For example: iam, anm, acm

11 Enter a value in the **offset** field.

12 Enter a value in the **byte-string** field.

13 Click **Add**.

—End—

Modifying message trace rules

Step	Action

At the OAMP workstation

1 Click **Configuration>msg-trace>msg-trace-rule**.

2 Click the **Search** tab and double-click the ruleset name you want to modify to transfer to the Administration window.

3 Select the field or drop-down options you want to modify.

4 When you have completed the changes, click **Modify**.

—End—

Deleting message trace rules

Step	Action
	At the OAMP workstation
1	Click **Configuration>msg-trace>msg-trace-rul**e.
2	Click the **Search** tab and double-click the ruleset name you want to delete to transfer to the Administration window.
3	Click **Delete**.

—End—

Configure message trace controls

After you have configured the message trace rules, you can apply these rules to links or paths using the msg-trace-control screen. Up to two paths/links per card may be monitored simultaneously. Monitoring more than two links/paths per card is not supported. Perform the following procedures to add and modify message trace controls, or delete an existing message trace control record.

Adding new message trace controls

Step	Action
	At the OAMP workstation
1	Click **Configuration>msg-trace>msg-trace-control.**
2	Click the **Administration** tab.
3	Click **New**.
4	Enter a value in the **trace-id** field to index the trace control.
5	Select a link type from the **ss7-ips7** drop-down menu.

If you select SS7, the asp-name and path-id menus are greyed out. Complete the remaining steps in this procedure except steps 10 and 11.

If you select IPS7, the linkset-name and slc menus are greyed out. Complete the remaining steps in this procedure except steps 8 and 9.

6 Select a direction type from the direction drop-down menu. Inbound, outbound, or both directions are supported.

7 Select the ruleset name for which you want to add message trace controls from the ruleset-name drop-down menu.

8 Select a linkset type from the **linkset-name** drop-down menu.

9 Enter value in the slc field. After you enter a value, proceed to Step 12.

10 Select an ASP type from the **asp-name** drop-down menu.

11 Enter a value in the **path-id** field.

12 Click **Add**.

—End—

Modifying message trace controls

Step	Action

At the OAMP workstation

1 Click **Configuration>msg-trace>msg-trace-control.**

2 Click the **Search** tab and double-click the ruleset name you want to modify to transfer to the Administration window.

3 Select the field or drop-down options you want to modify.

4 When you have completed the changes, click **Modify**.

—End—

Deleting message trace controls

Step	Action

At the OAMP workstation

1 Click **Configuration>msg-trace>msg-trace-control.**

2 Click the **Search** tab and double-click the ruleset name you want to delete to transfer to the Administration window.

3 Click **Delete**.

—End—

Message trace data

You can use the msg-trace screen to monitor and view the real-time traceback of decoded messages passed through the network.

Monitoring message trace data

Step	Action

At the OAMP workstation

1 Click **Configuration>msg-trace>msg-trace.**

2 Click the **Realtime** tab.

3 Click the **Start** and **Stop** buttons to control message trapping on this screen.

4 Double-click on the message for which you want to view message trace data. The message is opened in the Administration view and message trace data is displayed in the Trace Data window and messages are decoded in the decode-tree window.

—End—

Configuring Number Portability for an ANSI Number Portability Database

The Universal Signaling Point (USP) includes an ANSI or ETSI/ITU number portability database (NPDB) to support service provider number portability within a rate center.

ANSI message relay setup is documented in the following sections:

- "NP LSS Misc" (page 271)
- "Service Name Definition" (page 272)
- "NP Service Rules Definition" (page 273)
- "NPGTT Override" (page 276)
- "TT Mapping" (page 277)

ANSI Call-related setup is documented in the following section:

- "NP IN 1.0 Protocol Configuration" (page 279)

ANSI message relay setup

The USP uses the message relay function for both ANSI and ETSI/ITU non-call related network services that are impacted by number portability. Message relay provides rerouting capability for non-call-related signaling messages addressed using the SCCP called party address (CdPA). Message relay obtains routing information from the NP database associated with a particular subscriber number (SN).

Each service is defined by user-configured service identification rules. The rules identify the most likely criteria used to define a particular service. Each service can have more than one rule associated with it and each rule is assigned a priority value.

The ANSI message relay service supports a maximum of six services. Five services are predefined, enabling one new service to be added. You can modify the rules definitions for all supported services, including the five predefined services.

NP LSS Misc

The Number Portability Local Subsystem Miscellaneous window enables you to define general characteristics for your NP system. The LSS Class field is automatically pre-provisioned with the LSS Class selected for your NP subsystem (i.e. NP_ANSI or NP_ITU14) and cannot be modified.

Step	Action
	At the OAMP workstation
1	Click **Configuration>np>np-ansi>np-lss-misc**.
2	Select an **unidentified-service-response** from the pull-down list. The choices are *sccp-udts* or *use-default-gt-routing*. The country-code field is not used for ANSI
3	Click **Modify**.

—End—

Service Name Definition

The Service Name Definition windows can be provisioned if you have provisioned an ANSI or ETSI local subsystem (LSS) type.

Adding a Service Name Definition

Step	Action
	At the OAMP workstation
1	Click **Configuration>np>np-ansi>np-service-name**.
2	Select the local subsystem class *np-ansi* from the **lss-class** box.
3	Enter the service id in the **service-id** box. The id can be any numeric value between 0 and 5.
4	Enter the service name in the **service-name** box. The name can consist of up to eight alpha-numeric characters.
5	Select *Wireless* or *Wireline* from the **Service Characteristics** list. This option is currently used only for ESTI/ITU services but requires datafill in either case.
6	Click **Add**.

—End—

Modifying a Service Name Definition

Step	Action
	At the OAMP workstation
1	Click **Configuration>np>np-ansi>np-service-name**.

2 Click the **Search** panel tab. Locate the service name you want to modify. Double click the result in the search results to transfer to the administration panel.

3 Enter the service name in the **service-name** box. The name can consist of up to eight alpha-numeric characters.

4 Select *Wireless* or *Wireline* from the **Service Characteristics** list.

This option is currently used only for ESTI/ITU services but requires datafill in either case.

5 Click **Modify**.

—End—

Deleting a Service Name Definition

Step	Action
	At the OAMP workstation
1	Click **Configuration>np>np-ansi>np-service-name**.
2	Click the **Search** panel tab. Locate the service name you want to delete. Double click the result in the search results to transfer to the administration panel.
3	Click **Delete**.

—End—

NP Service Rules Definition

The USP uses service identification rules that you create to identify the various network services. You can create more than one rule to identify a particular network service.

You create service identification rules by selecting values for the following SCCP parameters:

- translation type
- subsystem number
- TCAP operation code

You can also assign a unique priority, from 0 to 99, to each service identification rule. The lower the priority value of a rule, the more likely it matches the parameters used to identify a network service.

The USP attempts to find a match between SS7 message SCCP parameter values and values provisioned in one of the service identification rules. The system searches the service identification rules, starting with the rule having the lowest priority value. If there is no match, the system searches each rule in increasing priority value until a match is found. Once a match is found, the message is routed to the identified network service. If the USP does not find a match, it uses the value provisioned in the Unidentified Service Response box on the np-lss-misc form.

Adding a Service Rule Definition

To add a service rule definition, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>np>np-ansi>np-service-rule**.
2	Enter a name for the rule into the **rule-name** box. A rule name can have up to 16 alphanumeric characters.
3	Enter a value into the **service-id** box. Valid entries are decimal numbers from 0 to 5 that must correspond to the service id of the particular service for which you are creating the rule.
4	Enter a value into the **priority** box. Valid entries are decimal numbers from 0 to 99, with 0 having the highest priority (most likely to match) and 99 having the lowest priority (least likely to match).
5	Select a translation type value to match on from the **translation-type** list. The choices are *match-all-translation-types* or *match-on-translation-type*. If you select match-on-translation-type, enter a translation type value in the **of** field using any valid translation type from 0 to 255.
6	Select a subsystem number value from the **ssn** list. The choices are *match-all-ssns* or *match-on-ssn*. For ANSI, you must select only match-all-ssns or your entry is rejected when you click add.
7	Select an opcode value from the **opcode** list. The choices are *match-all-opcodes* or *match-on-opcode*. For ANSI, you must select only match-all-opcodes or your entry is rejected when you click add.
8	Click **Add**.

—End—

Modifying a Service Rule Definition

To modify a service rule definition, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>np>np-ansi>np-service-rule**.
2	Click the **Search** panel tab. Locate the rule you want to modify. Double click the result in the search results to transfer to the administration panel.
3	Enter a value into the **priority** box. Valid entries are decimal numbers from 0 to 99, with 0 having the highest priority (most likely to match) and 99 having the lowest priority (least likely to match).
4	Select a translation type value from the **translation-type** list. The choices are *match-all-translation-types* or *match-on-translation-type*. If you select match-on-translation-type, enter a translation type value in the of field using any valid translation type from 0 to 255.
5	Select a subsystem number value from the **ssn** list. The choices are *match-all-ssns* or *match-on-ssn*. For ANSI, you must select only match-all-ssns or your entry is rejected when you click add.
6	Select an opcode value from the **opcode** list. The choices are *match-all-opcodes* or *match-on-opcode*. For ANSI, you must select only match-all-opcodes or your entry is rejected when you click add.
7	Click **Modify**.

—End—

Deleting a Service Rule Definition

To delete a rule definition, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>np>np-ansi>np-service rule**.
2	Click the **Search** panel tab. Locate the rule you want to delete. Double click the result in the search results to transfer to the administration panel.
3	Click **Delete**.

—End—

NPGTT Override

Number Portability Global Title Translation (NPGTT) Override is an optional feature that can reduce the number of times a non-call related (message relay) message needs to be processed in a local network. Ported subscriber records stored in the USP NPDB contain default routing information from the NPAC data used for routing incoming messages sent to the NP local subsystem. NPGTT Override enables default routing information to be overridden for numbers that are ported to a local network.

Once a message is determined to be for a ported number, a second lookup is performed in the NP database to retrieve the LRN associated with the subscriber DN. The NPGTT Override database is checked using the LRN as a key to see if the subscriber has ported to the local network. If the user has ported to the local network then the GTT results from the NPGTT Override table are used in lieu of those provided by NPAC. The available GTT result types are PC only, PC/SSN, and PC/GTT.

Adding an NPGTT Override Record

To add an NPGTT Override record, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>np>np-ansi>np-gtt-override**.
2	Choose a system identity from the **system-id** list.
3	Enter the location routing number into the **lrn** field. This field accepts up to ten decimal digits.
4	Enter a translation type into the **translation -type** field using any valid translation type between 0 and 255.
5	Click the ... button beside the **result-name** list. Select the desired GTT result from the list.
6	Click **Add**.

—End—

Modifying an NPGTT Override Record

To modify an NPGTT Override record, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>np>np-ansi>np-gtt-override**.
2	Click the **Search** panel tab. Locate the record you want to modify. Double click the result in the search results to transfer it to the administration panel.
3	Click the ... button beside the **result-name** list. Select the desired GTT result from the list and click **Select**.
4	Click **Modify**.
	—End—

Deleting an NPGTT Override Record

To delete an NPGTT Override record, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>np>np-ansi>np-gtt-override**
2	Click the **Search** panel tab. Locate the record you want to delete. Double click the result in the search results to transfer it to the administration panel.
3	Click **Delete**.
	—End—

TT Mapping

Translation type mapping is an optional feature that helps prevent circular routing of non-call related messages between networks. During the message relay (MR) process, translation type mapping changes the translation type of an outgoing message. Changing the translation type prevents a second MR process from being initiated at the receiving network. GTA replacement can help reduce the global title translation (GTT) datafill required for the new translation type. The global title address (GTA) of the outgoing message can be replaced with the LRN associated with the original GTA. GTA replacement is available only for ported numbers.

Adding a Translation Type Mapping Record

To add a translation type mapping record, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>np>np-ansi>np-translation-type-mapping**.
2	Select a system identity from the **system-id** list.
3	Click the ... button beside the **remote-pc** list. Select the desired Remote PC from the list and click **Select**.
4	Enter a translation type in the **translation-type** field using any valid translation type between 0 and 255.
5	Enter a mapped translation type in the **mapped-trans-type** field using any valid translation type between 0 and 255.
6	Use the **gta-replacement-option** checkbox to enable or disable this feature. The default is off (unchecked). Enabling this feature overwrites the GTA of the outgoing message with the LRN associated with the original GTA.
7	Click **Add**.

—End—

Modifying Translation Type Mapping Record

To modify a translation type mapping record, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>np>np-ansi>np-translation-type-mapping**.
2	Click the **Search** panel tab. Locate the record you want to modify. Double click the result in the search results to transfer to the administration panel.
3	Enter a mapped translation type in the **mapped-trans-type** field using any valid translation type between 0 and 255.
4	Use the **gta-replacement-option** checkbox to enable or disable this feature. The default is off (unchecked). Enabling this feature overwrites the GTA of the outgoing message with the LRN associated with the original GTA.
5	Click **Modify**.

—End—

Deleting a Translation Type Mapping Record

To delete a translation type mapping record, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>np>np-ansi>np-translation-type-mapping**.
2	Click the **Search** panel tab. Locate the record you want to delete. Double click the result in the search results to transfer to the administration panel.
3	Click **Delete**.
	—End—

ANSI Call Related Setup

The USP provides the ability to query a high-performance database to determine the true location of a subscriber who has ported from one carrier to another for both wireline and wireless networks. This is achieved in the ANSI market through a query launched to the USP requesting Location Routing Number (LRN) information on a subscriber that indicates to which network and switch the subscriber has ported. Once an NP database lookup has completed, an LRN is returned in the appropriate parameter if the subscriber is found to be ported. If the subscriber is non-ported, an appropriate message that does not include an LRN is returned

NP IN 1.0 Protocol Configuration

Use the NP IN 1.0 Protocol Configuration window to enter carrier identification codes (CIC) and billing indicator information. The provisioned values are used for IN 1.0 query responses. Each ANSI system identity has IN 1.0 configuration data associated with it.

Modifying NP IN 1.0 Protocol Configuration

Step	Action
	At the OAMP workstation
1	Click **Configuration>np>np-ansi>np-in-config**.
2	Click the **Search** panel tab. Locate the IN config entry against the system identity you want to modify. Double click the result in the search results to transfer to the administration panel.

3 Enter a value into the **carrier-id-code** box. You can enter either three or four decimal digits.

4 Enter a value into the **ama-call-type** box. You can enter up to three decimal digits.

5 Enter a value into the **service-feature-id** box. You can enter up to three decimal digits.

6 Click **Modify**.

—End—

Configuring Number Portability for an ETSI/ITU Number Portability Database

The Universal Signaling Point (USP) includes an ANSI or ETSI/ITU number portability database (NPDB) to support service provider number portability within a rate center.

ETSI/ITU message relay setup is documented in the following sections:

- "NP LSS Misc" (page 282)
- "Service Name Definition" (page 282)
- "NP Service Rule Definition" (page 284)
- "NP Service Misc" (page 286)
- "Message Relay Looping Prevention" (page 288)

ETSI/ITU call-related setup is documented in the following sections:

- "NP INAP Configuration" (page 291)
- "NP ITU general" (page 293)
- "NP Call SRF" (page 295)
- "NP NoA RN" (page 298)
- "NP RN to IMSI" (page 299)
- "NP Local RN" (page 300)

ETSI/ITU message relay setup

The USP uses the message relay function for non-call related network services that are impacted by number portability. Message relay provides rerouting capability for non-call related signaling messages addressed using the SCCP called party address (CdPA). Message relay obtains routing information from the NP database associated with a particular subscriber number (SN).

Each service is defined by user-configured service identification rules. The rules identify the most likely criteria used to define a particular service. Each service can have more than one rule associated with it and each rule is assigned a priority value. The ETSI/ITU message relay service supports a maximum of four user-defined services. There are no predefined services for ETSI/ITU. You can modify the rules definitions for all supported services.

NP LSS Misc

The Number Portability Local Subsystem Miscellaneous window enables you to define general characteristics for your NP system. The LSS Class field is automatically pre-provisioned with the LSS Class selected for your NP subsystem (i.e. NP_ANSI or NP_ITU14) and cannot be modified.

Modifying Number Portability Local Subsystem Miscellaneous

Step	Action
	At the OAMP workstation
1	Click **Configuration>np>np-itu>np-lss-misc**.
2	Enter a **country-code** value. Valid entries can be up to 3 decimal digits from 0 to 999.
3	Select an **unidentified-service-response** from the pull-down list. The choices are *sccp-udts* or *use-default-gt-routing*.
4	Click **Modify**.

—End—

Service Name Definition

The Service Name Definition windows can be provisioned if you have provisioned an ANSI or ETSI local subsystem (LSS) type.

Adding a Service Name Definition

Step	Action
	At the OAMP workstation
1	Click **Configuration>np>np-itu>np-service-name**.
2	Select the local subsystem class *np-itu14* from the **lss-class**.
3	Enter the service id in the **service-id** box. The id can be any numeric value between 0 and 3. The field allows 4 and 5 to be typed but these values are rejected if an add is performed.
4	Enter the service name in the **service-name** box. The name can consist of up to eight alpha-numeric characters.
5	Select *wireless* or *wireline* from the **service-characteristics** list based on your network type.
6	Click **Add**.

—End—

Modifying a Service Name Definition

To modify a Service Name record, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>np>np-itu>np-service-name**.
2	Click the **Search** panel tab. Locate the service name you want to modify. Double click the result in the search results to transfer to the administration panel.
3	Enter the service name in the **service-name** box. The name can consist of up to eight alpha-numeric characters.
4	Select *wireless* or *wireline* from the **service-characteristics** list based on your network type.
5	Click **Modify**.

—End—

Deleting a Service Name Definition

To delete a Service Name record, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>np>np-ansi>np-service-name**.
2	Click the **Search** panel tab. Locate the service name you want to delete. Double click the result in the search results to transfer to the administration panel.
3	Click **Delete**.

—End—

NP Service Rule Definition

The USP uses service identification rules that you create to identify the various network services. You can create more than one rule to identify a particular network service. You create service identification rules by selecting values for the following SCCP parameters:

- translation type
- subsystem number
- TCAP operation code

You can also assign a unique priority, from 0 to 99, to each service identification rule. The lower the priority value of a rule, the more likely it matches the parameters used to identify a network service. The USP attempts to find a match between SS7 message SCCP parameter values and values provisioned in one of the service identification rules. The system searches the service identification rules, starting with the rule having the lowest priority value. If there is no match, the system searches each rule in increasing priority value until a match is found. Once a match is found, the message is routed to the identified network service. If the USP does not find a match, it uses the value provisioned in the Unidentified Service Response box.

Adding a Service Rule Definition

To add a rule definition, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>np>np-itu>np-service-rule**.
2	Enter a name for the rule into the **rule-name** box. A rule name can have up to 16 alphanumeric characters.
3	Enter a value into the **service-id** box. Valid entries are decimal numbers from 0 to 3 that must correspond to the service id of the particular service for which you are creating the rule. The field allows 4 and 5 to be typed but these values are rejected if an add is performed.
4	Enter a value into the **priority** box. Valid entries are decimal numbers from 0 to 99, with 0 having the highest priority (most likely to match) and 99 having the lowest priority (least likely to match).
5	Select a translation type value to match on from the **translation-type** list. The choices are *match-all-translation-types* or *match-on-translation-type*. If you select match-on-translation-type,

enter a translation type value in the **of** field using any valid translation type from 0 to 255.

6 Select a subsystem number value to match on from the **ssn** list. The choices are *match-all-ssns* or *match-on-ssn*. If you select match-on-ssn, enter a subsystem number value in the **of** field using any valid ssn from 0 to 255

7 Select an opcode value to match on from the **opcode** list. The choices are *match-all-opcodes* or *match-on-opcode*. If you select match-on-opcode, enter an operation code value in the **of** field using any valid opcode up to 9 decimal digits in length.

8 Click **Add**.

—End—

Modifying a Service Rule Definition

To modify a rule definition, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>np>np-itu>np-service-rule**.
2	Click the **Search** panel tab. Locate the rule you want to modify. Double click the result in the search results to transfer to the administration panel.
3	Enter a value into the **priority** box. Valid entries are decimal numbers from 0 to 99, with 0 having the highest priority (most likely to match) and 99 having the lowest priority (least likely to match).
4	Select a translation type value to match on from the **translation-type** list. The choices are *match-all-translation-types* or *match-on-translation-type*. If you select match-on-translation-type, enter a translation type value in the **of** field using any valid translation type from 0 to 255.
5	Select a subsystem number value to match on from the **ssn** list. The choices are *match-all-ssns* or *match-on-ssn*. If you select match-on-ssn, enter a subsystem number value in the **of** field using any valid ssn from 0 to 255
6	Select an opcode value to match on from the **opcode** list. The choices are *match-all-opcodes* or *match-on-opcode*. If you select match-on-opcode, enter an operation code value in the **of** field using any valid opcode up to 9 decimal digits in length.

7 Click **Modify**.

—End—

Deleting a Service Rule Definition

To delete a rule definition, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>np>np-itu>np-service-rule**.
2	Click the **Search** panel tab. Locate the rule you want to delete. Double click the result in the search results to transfer to the administration panel.
3	Click **Delete**.

—End—

NP Service Misc

This screen provisions miscellaneous parameters associated with Message Relay processing on the USP. If the result of an NPDB query indicates that a service is ported and returns a routing number (RN) value, a second GTT is performed on the RN or RN+DN or CC+RN+DN. The ETSI/ITU Services window enables you to select the GTA format for the second GTT. Its also enables the user to turn on and off the Message Relay Looping Prevention capability that uses a special NoA value in the message to indicate that a previous lookup has been performed. This avoids the possibility of a non-call related message from being repeatedly passed back and forth between networks.

Adding an np service misc definition

Step	Action
	At the OAMP workstation
1	Click **Configuration>np>np-itu>np-service-misc**.
2	Select a system identity from the **system-id** list.
3	Enter a value into the **service-id** box. Valid entries are decimal numbers from 0 to 3 that must correspond to the service id of the particular service for which you are creating the entry.

The field allows 4 and 5 to be typed but these values are rejected if an add is performed.

4 Select a value for the **gta-format-for-second-gtt** field. Valid entries are *RN_only, Concatenated_(RN+DN)* or *Concatenated_(CC+RN+DN)*.

5 Click the **noa-looping-prevention-option** checkbox if you require message relay looping prevention to be enabled for this service.

ATTENTION
If this option is enabled, further datafill is required in the np-service-message-relay-looping-prevention screen to fully configure this capability. You must complete this procedure for each service that uses Message Relay Looping Prevention and performs an outgoing second GTT.

6 Click **Add**.

—End—

Modifying an np service misc definition

To modify a Service Misc entry, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>np>np-itu>np-service-misc**.
2	Click the **Search** panel tab. Locate the rule you want to modify. Double click the result in the search results to transfer to the administration panel
3	Select a value for the **gta-format-for-second-gtt** field. Valid entries are *RN_only, Concatenated_(RN+DN)*, or *Concatenated_(CC+RN+DN)*.
4	Click the **noa-looping-prevention-option** checkbox if you require message relay looping prevention to be enabled for this service.

ATTENTION
If this option is enabled, further datafill is required in the np-service-message-relay-looping-prevention screen to fully configure this capability. You must complete this procedure for each service that uses Message Relay Looping Prevention and performs an outgoing second GTT.

5 Click **Modify**.

—End—

Deleting an np service misc definition

To delete a Service Misc entry, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>np>np-itu>np-service-misc**.
2	Click the **Search** panel tab. Locate the rule you want to delete. Double click the result in the search results to transfer to the administration panel
3	Click **Delete**.

—End—

Message Relay Looping Prevention

This screen enables you to provision the parameters associated with looping prevention functionality for the ETSI/ITU Message Relay services. Individual values can be set up for national and international messages with special NoA entries associated with each. The (inter)national-noa-indicating previous-lookup field is the value that is set when a lookup is first performed or checked when a message arrives to check if a previous lookup has been performed at the n-1 network. The (inter)national-corresponding-original-noa value is used to reset the NoA value to its original normal value once it has been determined that a previous lookup has been performed and the message is being forwarded to the local network.

The following restrictions apply to this procedure:

- If you select two different values for the national (Natl) and international (Intl) NoA Indicating Previous NP Lookup fields, you must select two different values for the Natl and Intl Corresponding Original NoA fields as well.
- The set of values provisioned in this window apply to any service for which looping prevention is enabled. You cannot use different values for different services.

Adding or Modifying Service Message Relay Looping Prevention

To provision Message Relay Looping Prevention functionality, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>np>np-itu>np-service-message-relay-looping-prevention**.
2	Enter a value for the **national-noa-indicating-previous-np-lookup** field. Valid entries are 0 to 127.
3	Enter a value for the **national-corresponding-original-noa** field. Valid entries are 0 to 127.
4	Enter a value for the **international-noa-indicating-previous-np-lookup** field. Valid entries are 0 to 127.
5	Enter a value for the **international-corresponding-original-noa** field. Valid entries are 0 to 127.
6	Click **Modify**.

ATTENTION

Before looping prevention functions, it must be enabled for each desired service using the NP-Service-Misc screen.

—End—

Service PCSSN

NP Service PCSSN enables the user to modify the information relating to PC SSN results found in the NP database during non-call related services. The UNPM, by default, uses the same system id and NoA values for an outgoing non-call related message as was received in the incoming message. This table must be datafilled to redirect the message to a destination in a different system id or with a different NoA than the incoming message. Changes to the system id and NoA are performed against each possible porting status result from the NP database. The default is set by the system as "no change" for all services and all porting status' in this table. To process an outgoing non-call related message base on this table, the UNPM database needs to have the GTT service data filled as DPC/SSN format instead of RN format.

Modifying np-service-pcssn

Step	Action

At the OAMP workstation

1 Click **Configuration>np>np-itu>np-service-pcssn**.

2 Click the **Search** panel tab. Locate the record corresponding to the porting status and service id that you want to modify. Double click the result in the search results to transfer to the administration panel.

3 Select a value from the **system-id** list. The choices are *do-not-change-system-id* and *change-system-id*. If you select change-system-id, you must also enter a valid system id in the to field from the drop-down menu.

4 Select a value from the **Nature of Address** list. The choices are *do-not-change-noa*, *change-noa* and *use-incoming-noa*. If you select the change-noa choice, you must also enter a valid Nature of Address in the to field. Valid entries are decimal values from 0 to 127.

5 Click **Modify**.

—End—

ETSI/ITU Call Related Setup

The USP provides the ability to query a high-performance database to determine the true location of a subscriber who has ported from one carrier to another for both wireline and wireless networks. This is achieved in the ETSI/ITU market through various supported mechanisms including Call Related Signaling Relay Functionality (SRF) and Intelligent Network Application Protocol (INAP) query functionality. For Call Related SRF, a message is launched to the USP for processing. Depending on the routing scheme provisioned, either a response is returned to the querying switch or the message is forwarded to the SRF function node in the subscription network which then responds.

For INAP, a query is launched to the USP requesting Routing Number (RN) information on a subscriber that indicates the network and switch to which the subscriber has ported. Once an NP database lookup has completed, an RN is returned in the appropriate parameter if the subscriber is found to be ported. For a non-ported subscriber on an ITU network the message returned is either *Connect* that contains an DN, and *Continue* that does not include an RN or DN.

NP INAP Configuration

This screen enables the user to provision parameters associated with INAP message processing for call-related messaging.

Adding np-inap-config

To add INAP configuration data, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>np>np-itu>np-inap-config**.
2	Select a system identity from the **system-id** list.
3	Select a value from the **nature-of-address-ported-numbers** list. The choices are *do-not-change-noa* and *change-noa*. If you select change-noa, you must also enter a valid NoA in the to field which can be any decimal value from 0 to 127.
4	Select a value from the **nature-of-address-non- ported-numbers** list. The choices are *do-not-change-noa* and *change-noa*. If you select change-noa, you must also enter a valid NoA in the **to** field that can be any decimal value from 0 to 127.
5	Select a value from the **response-msg-type-non- ported-number** list. This value determines the type of response message to be returned for non-ported numbers only. Valid selections are *continue* or *connect*. Ported numbers always return a value of "Connect".
6	Select a value for the **response-msg-addressing-method** to be used when returning called numbers for non-ported numbers. Valid selections are *Concatenated_RN+DN or RN_Only*.
7	Select **overlap-outpulsing-required-option** if this is used to collect the digits of the called party address. **ATTENTION** Overlap outpulsing is not currently supported on the USP so this entry is not used.
8	Enter a timeout value in seconds into the **inter-digit-collection-time-out-value** box. The range spans 1 to 60 seconds. The default value is 10. **ATTENTION** Overlap outpulsing is not currently supported on the USP so this entry is not used.

Click **Add**.

—End—

Modifying np-inap-config

To modify INAP configuration data, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>np>np-itu>np-inap-config**.
2	Click the **Search** panel tab. Locate the rule you want to modify. Double click the result in the search results to transfer to the administration panel
3	Select a value from the **nature-of-address-ported-numbers** list. The choices are *do-not-change-noa* and *change-noa*. If you select change-noa, you must also enter a valid NoA in the to field which can be any decimal value from 0 to 127.
4	Select a value from the **nature-of-address-non- ported-numbers** list. The choices are *do-not-change-noa* and *change-noa*. If you select change-noa, you must also enter a valid NoA in the to field that can be any decimal value from 0 to 127.
5	Select a value from the **response-msg-type-non- ported-number** list. This value determines the type of response message to be returned for non-ported numbers only. Valid selections are *continue* or *connect*. Ported numbers always return a value of "Connect".
6	Select a value for the **response-msg-addressing-method** to be used when returning called numbers for non-ported numbers. Valid selections are *Concatenated_RN+DN or RN_Only*.
7	Select **overlap-outpulsing-required-option** if this is used to collect the digits of the called party address. **ATTENTION** Overlap outpulsing is not currently supported on the USP so this entry is not used.
8	Enter a timeout value in seconds into the **inter-digit-collection-time-out-value** box. The range spans 1 to 60 seconds. The default value is 10.

ATTENTION
Overlap outpulsing is not currently supported on the USP so this entry is not used.

9 Click **Modify**.

—End—

Deleting ETSI INAP Call Related Data

To delete INAP configuration records, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>np>np-itu>np-inap-config**.
2	Click the **Search** panel tab. Locate the record you want to delete. Double click the result in the search results to transfer to the administration panel.
3	Click **Delete**.

—End—

NP ITU general

The NP ITU General screen provides a set of general attributes for various aspects of NP provisioning for both call and non call-related message handling. It is a modify only screen and has default values pre-provisioned.

Modifying np-itu-general

To modify ITU General configuration data, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>np>np-itu>np-itu-general**.
2	Select a value for the **routing-method** field. This field determines what variation of routing is applied for Call-Related SRF processing. The valid selections are *direct-rtg, indirect-rtg-number-range-owner*, and *indirect-rtg-subscription*.
3	Select a value for the **database-record-not-found-treatment** field. This field is used to determine the behavior to exhibit when a record

is not found in the database. The valid selections are *non-ported, not-known-to-be-ported* and *error*.

4 Check the **tariff-non-transparency-option** if you require this capability. If you select this option, you must also enter a valid translation type in the **ati-translation-type** field. Valid values are any decimal number from 0 to 255. This feature enables the USP to accept and respond to a proprietary ATI message received from an SCP looking to determine if a subscriber is ported or not and how to tariff a prepaid call. The USP responds with a proprietary ATI_ack message with an RN.

5 Select a value from the **call-related-srf-noa-for-outgoing-gtt** list. The choices are *do-not-change-noa* and *change-noa*. If you select *change-noa*, you must also enter a valid NoA in the **to** field which can be any decimal value from 0 to 127. This field is used to determine which Nature of Address value is used in the second GTT performed after a Call-Related SRF database lookup is performed.

6 Select a value from the **message-relay-noa-for-outgoing-gtt** list. The choices are *do-not-change-noa* and *change-noa*. If you select change-noa, you must also enter a valid NoA in the **to** field which can be any decimal value from 0 to 127. This field is used to determine which Nature of Address value is used in the second GTT performed after a Message Relay database lookup is performed.

7 Check the **incoming-dn-modification-digit-option** if you require this capability. If you select this option, you must also enter a valid single hexadecimal digit (0 to 9, a to f, A to F) in the **incoming-dn-modification-digit** field. This feature causes the system to search a relayed Call Related SRF or Message Relay message for a leading digit in the DN/MSISDN that matches the provisioned modification digit. If they match, that digit is stripped from the DN/MSISDN before the message is forwarded. If the DN Modification digit is set, the digit is stripped from the DN for the following situations:

- relaying of a MAP SRI to the subscription network using CC+RN+NSN relay format
- when relaying a non-call related message using an MRGT result with GTA of CC+RN+DN
- when relaying a non-call related message using an MRGT result with GTA of RN+CC+DN

An example of use for this capability would be the UK where the digit 7 is used to identify mobile subscribers and must not be passed across network boundaries.

8 Check the **sri-bypass-option** if you require this capability. If selected, all MAP SRI messages are routed based on the initial GTT. No NP processing is invoked, even if the np-gtt-required-option is set in the GT Translation

9 Click **Add**.

—End—

NP Call SRF

The NP Call Related Signaling Relay Function screen provides setup data for the SRF capability on the USP. This screen can only be modified. Call related SRF is one method used in wireless networks to manage ported subscribers. The SRF function intercepts MAP-SRI messages destined for HLRs and responds to the sending MSC with an SRI_ack, or forwards to the subscriber network, or forwards the SRI to the appropriate local HLR. When a subscriber is ported, the routing number returned from the NP database is used by the MSC to determine which network/node to route the call to. The USP automatically provisions default values for some of the fields in this window.

The NP Call Related SRF window enables you to enable or disable NoA looping prevention for Call Related SRF. The Call Related SRF Looping Prevention portion of this window enables you to provision an NoA indicating a previous lookup in the database, as well as the original NoA. The UNPM enables the user to select NoA looping prevention at either the MAP or SCCP levels of the message using the "NoA Level" field.

The "Outgoing MAP NoA" field is only used for MAP level loop Prevention and is the only value used to set the outgoing MAP-level NoA to indicate a lookup has been performed. The "NoA Indicating Previous NP Lookup" field enables the user to specify the NoA value to be set for outgoing messages after an NPDB lookup has been done (except when the MAP level NoA looping prevention is selected, as described above). This field also determines the NoA value to be checked for an incoming messages to determine if a lookup has already been performed. There are separate values for national and international format messages. The "Corresponding Original NoA" field enables the user to specify the NoA to be set in cases where a previous lookup has been performed and the UNPM is forwarding the message to a local HLR. This value should be set to the normal value that the HLR would expect for a national or international format number. There are separate values for national and international format messages.

Modifying np-call-srf

If you want to modify the values in the call related SRF screen, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>np>np-itu>np-call-srf**.
2	Select a format from the **gta-format-for-outgoing-gtt** list. Valid formats are *rn-only, rn+msisdn*, and *cc+rn+msisdn*. The default value is rn-only.
3	Select a format from the **map-msrn-format** list. Valid formats are *concatenated-rn+msisdn_v2+v3, separated-rn+msisdn_v3*, and *concatenated-cc+rn+nsn_v2+ v3*. The default value is concatenated-rn+msisdn_v2+v3.
4	Select a format from the **relayed-sccp-cdpa-format** list. Valid values are *rn+msisdn* and *cc+rn+nsn*. The default is rn+msisdn.
5	Enter a value in the **default-imsi** box. A valid entry is any 5 to 15-digit decimal number from 0 to 999999999999999. This value is used if no RN specific values are provisioned in the NP RN to IMSI screen. This IMSI is used in the response to the MSC. The default IMSI value is 000000.
6	Click **Modify**.

ATTENTION
If looping prevention is desired, follow the steps below.

—End—

Modifying looping-prevention-option

If you want to enable or disable Call Related SRF Looping Prevention function, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>np>np-itu>np-call-srf**.
2	If you want to activate looping prevention, check the **looping-prevention-option** checkbox. If you do not want to activate looping prevention, make sure the **looping-prevention-option** box is not checked. If it is not checked, you cannot enter a value into any of the other fields in the Call Related SRF Looping Prevention portion of the window.

3 Select the NoA level from the **nature-of-address-level** list. The NoA level can be either *map* or *sccp*.

ATTENTION

If you select MAP level looping, all subsequent values can range from 0 to 7. If you select SCCP level looping, all values range from 0 to 127. The screen enables you to enter values greater than 7 when MAP level looping is enabled however they are rejected when modify is entered.

4 If you selected MAP level looping, enter an NoA value in the **outgoing-map-noa** field. The NoA value can be any number from 0 to 7. This value is set in the outgoing message at the MAP level.

5 Enter a value in the **national-noa-indicating-previous- np-lookup** field for national routing lookup. Valid entries are 0 to 7 (MAP level) or 0 to 127 (SCCP level). This value is checked on the incoming message at the MAP or SCCP levels to determine if a previous lookup has been performed. It is also set in the outgoing message if this is the first lookup for SCCP level looping prevention. The outgoing-map-noa is set in the outgoing message if this is the first lookup for MAP level looping-prevention.

6 Enter a value in the **national-corresponding-original-noa** field for national routing lookup. Valid entries are 0 to 7 (MAP level) or 0 to 127 (SCCP level). This value is used in an outgoing message to a local HLR at the MAP or SCCP level when a message arrives in a previously queried state.

7 Enter a value in the **international-noa-indicating-previous-np-lookup** field for international routing lookup. Valid entries are 0 to 7 (MAP level) or 0 to 127 (SCCP level). This value is checked on the incoming message at the MAP or SCCP levels to determine if a previous lookup has been performed. It is also set in the outgoing message if this is the first lookup for SCCP level looping prevention. The outgoing-map-noa is set in the outgoing message if this is the first lookup for MAP level looping-prevention.

8 Enter a value in the **international-corresponding-original-noa** field for international routing lookup. Valid entries are 0 to 7 (MAP level) or 0 to 127 (SCCP level). This value is used in an outgoing message to a local HLR at the MAP or SCCP level when a message arrives in a previously queried state.

9 Click **Modify**.

—End—

NP NoA RN

The Nature of Address RN screen is part of the USP's number normalization function for both non-Call Related Functionality (for example, Message Relay) and Call Related Functionality (for example, Call Related SRF, and INAP query). This screen enables the user to set up a set of valid nature of address (NoA) and routing number (RN) combinations for each ITU system identity that has a local subsystem (LSS) provisioned against it. The Number Normalization combinations are used to:

- validate incoming ITU message relay
- validate call-related SRF queries
- validate call-related INAP queries

In addition, for message relay, when a message arrives at the USP as previously looked-up, it contains a routing number prefix on the SCCP CdPA DN. The USP only stores nationally significant DNs in the database, so the RN prefix must be removed prior to lookup. If a match is found for the NoA and RN in the CdPA, the USP removes those RN digits and extract the remaining DN digits to perform the database lookup.

Only adds and deletes can be performed on this screen.

Adding np-noa-rn

To add a valid NoA/RN combination, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>np>np-itu>np-noa-rn**.
2	Select a system identity from the **system-id** list.
3	Enter an noa value in the **of** box. Valid choices are *match-all-noas* or *match-on-noa*. If you select match-on-noa, enter a value in the noa list. Valid entries are decimal digits from 0 to 127. Overlapping ranges are not allowed.
4	Enter a valid routing number in the **of** box. Valid entries are rn-not-present or rn-present. If you select rn-present, enter a valid Routing number of up to10 hexadecimal digits (0 to 9, a to f, A to F).
5	Click **Add**.

—End—

Deleting np-noa-rn

To delete an existing NoA/RN combination, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>np>np-itu>np-noa-rn**.
2	Click the **Search** panel tab. Locate the record you want to delete. Double click the result in the search results to transfer to the administration panel.
3	Click **Delete**.

—End—

NP RN to IMSI

The Routing Number to IMSI Mapping screen enables you to provision IMSI (International Mobile Subscriber Identity) numbers that are used in outgoing Call Related SRF MAP SRI acknowledgement messages against associated RNs or RN ranges. These "generic" IMSIs represent the subscription network corresponding to their associated RNs. If you know that the IMSI is not used at all by the MSC (Mobile Switching Center), you can provision a default IMSI value on the Call Related SRF screen. This value is set in all outgoing MAP SRI acknowledgement messages if there are no provisioned entries in the RN to IMSI Mapping table.

Adding rn-to-imsi

To assign an RN range to an IMSI, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>np>np-itu>np-rn-to-imsi**.
2	Enter a valid RN value in the **low-rn** field of up to10 hexadecimal digits (0 to 9, a to f, A to F).
3	Enter a valid RN value in the **high-rn** field of up to10 hexadecimal digits (0 to 9, a to f, A to F).
4	Enter a valid IMSI in the **imsi** field of 5 to15-digit decimal digits from 0 to 999999999999999.
5	Click **Add**.

—End—

Modifying rn-to-imsi

To assign an RN range to an IMSI, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>np>np-itu>np-rn-to-imsi**.
2	Click the **Search** panel tab. Locate the rule you want to modify. Double click the result in the search results to transfer to the administration panel
3	Enter a valid IMSI in the **imsi** field of 5 to15-digit decimal digits from 0 to 999999999999999.
4	Click **Modify**.

—End—

Deleting rn-to-imsi

To modify an RN to IMSI entry, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>np>np-itu>np-rn-to-imsi**.
2	Click the **Search** panel tab. Locate the record you want to delete. Double click the result in the search results to transfer to the administration panel.
3	Click **Delete**.

—End—

NP Local RN

The Local Network RNs screen enables you to specify RN number ranges to which the USP is responsible for routing NP SRF messages. The RN ranges are defined by a low and high RN.

Only adds and deletes are allowed for this screen.

Adding np-local-rn

To add a local network Routing Number range, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>np>np-itu>np-local-rn**.
2	Enter a value in the **low-rn** box of up to10 hexadecimal digits (0 to 9, a to f, A to F).
3	Enter a value in the **high-rn** box of up to10 hexadecimal digits (0 to 9, a to f, A to F). Overlapping ranges are not allowed.
4	Click **Add**.

—End—

Deleting np-local-rn

To delete a local network Routing Number range, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>np>np-itu>np-local-rn**.
2	Click the **Search** panel tab. Locate the record you want to delete. Double click the result in the search results to transfer to the administration panel.
3	Click **Delete**.

—End—

Configuring Application Server Processes

Each application server consists of a primary and secondary ASP. An ASP path is a logical IP connection between the Universal Signaling Point (USP) and a primary or secondary application server process.

Perform the following procedures to add and modify Application Server processes. You can also delete processes that do not have any provisioned ASP paths, or that are not being used by an application server.

Adding Application Server processes

Step	Action
	At the OAMP workstation
1	Click **Configuration>ips7>application-server-process.**
2	Enter a name for the new application server process in the **asp-name** box. Each application server process must have a unique name that can be up to 16 alphanumeric characters in length.
3	Click **snm-broadcast-option** if you want Signaling Network Management messages (for example, DUNA [Destination Unavailable], DAVA [Destination Available]) to be sent to the ASP.
4	Choose an **ipsp-type** from the drop-down list. The ipsp-type options are listed below: • ipsp-se-client • ipsp-se-server • asp • asp-rfc • asp-mate-server (not supported in this release) • asp-mate-client (not supported in this release)
5	Click **Add** to save this new Application Server Process.
	—End—

Modifying Application Server processes

Step	Action
	At the OAMP workstation
1	Click **Configuration>ips7>application-server-process.**
2	Click the **Search** panel tab. Locate the ASP you want to edit. Double click the linkset in the search results to transfer to the Administration panel.
3	Change the **snm-broadcast-option** checkbox or the **ipsp-type** selection.
4	Click **Modify**.
	—End—

Deleting Application Server processes

Step	Action
	At the OAMP workstation
1	Click **Configuration>ips7>application-server-process.**
2	Click the **Search** panel tab. Locate the ASP you want to delete. Double click the ASP in the search results to transfer to the Administration panel.
3	Click **Delete**.
	—End—

Configuring Application Server Process Paths

Paths provide the logical connection between the USP and an Application Server Process. You can add new paths and change or delete existing ones, as well as change path states.

Adding Application Server process paths

ATTENTION
The path needs to be taken down before you modify it.

Step	Action
1	Click **Configuration>ips7>application-server-process-path.**
2	To provision a path, select an ASP from the **asp-name** list. When the ASP type is asp-rfc, only one ASP path can be provisioned in an ASP.
3	Assign an unused path ID for this path by entering one in the **path-id** box. The path ID is a logical representation (0–15) of a logical path. When the ASP type is asp-rfc, path-id must be 0.
4	Enter the shelf in the **shelf** box. Click the ... button to list available cards.
5	Enter the slot in the **slot** box.
6	Enter the IP address of this application server process in the **dest-ipaddr** box.
7	Enter a remote port for this Application Server Process in the **dest-port** box.
8	Choose a protocol from the **transport-protocol** drop-down list. The M3UA variants are listed below. Please choose the variant supported by the far end for proper operation. • M3UAv2/UDP (This is used only when communicating with AS Master (CS2K-based. e.g. 3PC/CS2K/HLR)) • M3UAv2/Sctp-Client (USP-GWC) • M3UAv2/Sctp-Server • M3UArfc/Sctp-Client • M3UArfc/Sctp-Server

ATTENTION
When the ASP type is asp-rfc, only M3UArfc/Sctp-Client or M3UArfc/Sctp-Server can be used as the transport protocol.

9 If the transport protocol chosen uses the SCTP client protocol, select the SCTP Checksum format from the sctp-checksum drop-down list. The choices are:

- adler
- crc32

ATTENTION
When the ASP type is **asp-rfc, sctp-checksum** must be crc32.

10 Choose an SCTP parameter index from the **sctp-parm-index** drop-down list.

Do not use a SIP/UDP protocol. Choose an SCTP parameter.

11 Click **Add** to add this new path.

—End—

Modifying Application Server process paths

Step	Action

At the OAMP workstation

1 Click **Configuration>ips7>application-server-process-path.**

2 Click the **Search** panel tab. Locate the ASP Path you want to edit. Double-click the Application Server Process Path in the search results to transfer to the Administration panel

3 Change the entries in the **dest-ipaddr**, **dest-port, transport-protocol, sctp-checksum, sctp-parm-index** as needed.

4 Click **Modify** to save application server process path changes.

—End—

Deleting Application Server process paths

Step	Action
	At the OAMP workstation
1	Click **Configuration>ips7>application-server-process-path.**
2	Click the **Search** panel tab. Locate the path you want to delete. Double-click the path in the search results to transfer to the Administration panel. You cannot delete a path that is in either the Up or the Restoring state. If the selected path is in either the Up or the Restoring state, change the state of the path to Down before attempting to delete it.
3	Click **Delete** to delete this path.
	—End—

Application Server process path states

The state of a path appears in the Path State box.

A path can be in one of three states:

- Down
- Up
- Restoring

A path is not available to carry traffic when it is in either the “Down” state or the “Restoring” state. A path is available to carry traffic when it is in the “Up” state; however, only paths associated with an Active application server process actually carry traffic.

Up State

Placing a path into the Up state is done in two stages. The USP brings the path into the Restoring state, then an application server process brings the path into the Up state.

If the application server process is unable to bring the path into the Up state, the path remains in the Restoring state. The path remains in the Restoring state until the application server process is able to bring it into the Up state or you place it into the Down state.

Down State

A path can be placed into the Down state when it is in either the Up state or the Restoring state.

Change the state of Application Server process paths

You can stop traffic on a path by changing the path state to Down. You can allow traffic on a path by changing the path state to Up.

ATTENTION

To carry traffic, paths must be in the Up state and be associated with an Active application server process.

Changing the path states

Step	Action

At the OAMP workstation

1 Click **Configuration>ips7>application-server-process-path.**

2 Click the **Search** panel tab. Locate the path you want to delete. Double click the path in the search results to transfer to the Administration panel.

You cannot delete a path that is in either the Up or the Restoring state. If the selected path is in either the Up or the Restoring state, change the state of the path to Down before attempting to delete it.

3 Click Up to change the state of the path to Up or click **Down** to change the state of the path to Down.

You cannot restore an ASP Path if the corresponding AS is not datafilled.

—End—

Configuring Application Servers

Perform the procedures in this section to add an application server and to delete an existing application server. It is not possible to modify an application server.

Adding Application Servers for USP

Step	Action

At the OAMP workstation

1 Click **Configuration>ips7>application-server.**

2 Enter a name for the new application server in the **as-name** box. The name can be up to 16 alphanumeric characters in length.

3 Choose an **as-type** from the drop-down list.

The **as-type** options are listed below.

- **as-rfc** — This as-type is used to provision an Application Server that resides in SSG.
- **as-master** — An Application Server Master represents a Carrier Voice over IP Core that is used in Solutions such as Carrier Voice over IP CS2K and Univity HLR.
- **as** — This as-type is for an ordinary Application Server.

4 Select the Application Server Process (ASP) according to the as-type selected.

If	Go to
as-rfc	Step 5
as-master	Step 6
as	Step 6

5 Eight ASPs can be selected from the drop-down lists. Only ASPs that are asp-rfc type can be selected. Go to Step 13.

6 Select a Primary Application Server Process from the **primary-asp-name** drop-down menu.

7 Select a Secondary Application Server Process from the **secondary-asp-name** drop-down menu.

ATTENTION
The secondary-asp-name is only selected when the as-type is as.

8 Click **Add**.

ATTENTION
Support for the sip-application-option is discontinued from USP 11 release onwards.

—End—

Modifying Application Servers

Step	Action

ATTENTION
It is not possible to modify Application Servers.

At the OAMP workstation

—End—

Deleting Application Servers

Step	Action

At the OAMP workstation

1 Click **Configuration>ips7>application-server.**

2 Click the **Search** panel tab. Locate the ASP you want to delete. Double-click the AS in the search results to transfer to the Administration panel.

3 If you are sure that the application server is not being used by an Application Server Destination (ASD), Application Server Assignment (ASA), Routing Key (RK), or SCCP local subsystem instance (LSSN), click **Delete** to delete the application server.

—End—

Configuring Application Server Destinations

You can provision an application server destination by specifying the USP point code, an ASD name, and routing to the destination. The following section describes how to provision application server destinations. You must assign routesets to the ASD.

Adding Application Server destinations

Step	Action
	At the OAMP workstation
1	Click **Configuration>ips7>application-server-destination.**
2	Enter an application server destination name in the **asd-name** box. You can enter up to 16 alphanumeric characters.
3	Select a system identity from the **system-id** drop-down list.
4	Select an AS from the **as-name** list.
5	Enter a point code for the application server destination in the **dest-pointcode** box.
6	Click **Add**. The new ASD appears in the Application Server Destination Records DPC list.

—End—

Deleting DPC Application Server destinations

Step	Action
	At the OAMP workstation
1	Click **Configuration>ips7>application-server-destination.**
2	Click the **Search** panel tab. Locate the DPC Application Server Destination that you want to delete. Double-click the ASD application server destination in the search results to transfer to the Administration panel.
3	Click **Delete** to delete the selected Application Server Destination.

—End—

Configuring Application Server Assignments

An Application Server Assignments (ASA) assigns a routeset to an application. This allows the USP to route messages to the Application Server using the Originating Point Code (OPC) of the messages.

Adding Application Server assignments

Step	Action
	At the OAMP workstation
1	Click **Configuration>ips7>application-server-assignment.**
2	Select a routeset from the **routeset-name** list.
3	Select an application server from the **as-name** list.
4	Click **Add**.

—End—

Deleting Application Server assignments

Step	Action
	At the OAMP workstation
1	Click **Configuration>ips7>application-server-assignment.**
2	Click the **Search** panel tab. Locate the Application Server Assignment to delete. Double-click on the ASA in the search results to transfer to the Administration panel.
3	Click **Delete**.

—End—

Configuring Routing Keys

A routing key describes a set of SS7 parameters and parameter values that uniquely define the range of signalling traffic to be handled by a particular Application Server (AS).

Perform this procedure to provision a routing key according to the routing configuration of each AS.

Adding a routing key

Step	Action
	At the OAMP workstation
1	Click **Configuration>ips7>routing-key.**
2	Select a system id from the **system-id** drop-down list. Only a system-id that is provisioned as sg-enabled can be selected.
3	Select a routeset from the **routeset-name** drop-down list.
4	Select a service indicator from the **si** drop-down list. The service indicator options are listed below. • ISDN User Part (ISUP) • Telephone User Part (TUP) • Bearer Independent Call Control (BICC) • Signalling Connection Control Part (SCCP) • all If all is selected as the service indicator, then four service indicators are automatically selected.
5	Select an AS from the **as-name** drop-down list.
6	Click **Add** to save this new routing key.

—End—

Modifying a routing key

Step	Action
	At the OAMP workstation
1	Click **Configuration>ips7>routing-key.**
2	Click the **Search** panel tab. Locate the routing key you want to edit. Double-click the routing key in the search results to transfer to the Administration panel.
3	Change the entry for **as-name** as needed.
4	Click **Modify** to save the routing key changes.
	—End—

Deleting a routing key

Step	Action
	At the OAMP workstation
1	Click **Configuration>ips7>routing-key**.
2	Click the **Search** panel tab. Locate the routing key you want to edit. Double-click the routing key in the search results to transfer to the Administration panel.
3	Click **Delete** to delete this routing key.
	—End—

Configuring RouteMaster

The USP Route Master application enables the in-service migration of lines and trunks from Donor to Host switch.

Adding System ID Mapping

To provision a new Route Master System ID mapping, perform the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>rm>system-id-mapping**.
2	Select the Route Master network ID from the **rm-network-id** drop down list.
3	Select the Donor network ID from the **donor-network-id** drop down list.
4	Select the Host network ID from the **host-network-id** drop down list.
5	Select the Route Master phase from the **rm-phase** drop down list. Valid phases are: insert-start, insert-complete, and remove.
6	Click **Add**.

—End—

Modifying ID Mapping

To modify an existing Route Master System ID mapping, perform the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>rm>system-id-mapping**.
2	Click the **Search** panel tab and locate the System ID mapping you want to delete. Double click the System ID mapping to open it in the administration panel.
3	Select the new Route Master phase from the **rm-phase** drop down list. Valid phases are: insert-start, insert-complete, and remove.

4 Click **Modify** to save these changes.

—End—

Deleting System ID Mapping

To delete System ID mappings, perform the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>rm>system-id-mapping**.
2	Click the **Search** panel tab and locate the System ID mapping you want to delete. Double click the System ID mapping to open it in the administration panel.
3	Click **Delete**.

—End—

Adding Trunk Mapping

To provision a new Trunk mapping, perform the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>rm>trunk-mapping**.
2	Enter the routeset associated with the trunk in **routeset-name** box, of select it using the box.
3	Enter the Circuit Identification Code in the **cic** box.
4	Select the mapping state from the **mapping-state** drop down list. Valid states are host and donor.
5	Click **Add**.

—End—

Modifying Trunk Mapping

To modify a Trunk mapping, perform the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>rm>trunk-mapping**.
2	Select the new mapping state from the **mapping-state** drop down list. Valid states are host and donor.
3	Click **Modify** to save these changes.
	—End—

Deleting Trunk Mapping

To delete a Trunk mapping, perform the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>rm>trunk-mapping**.
2	Click the **Search** panel tab and locate the mapping state you want to delete. Double click the mapping state to open it in the administration panel.
3	Click **Delete**.
	—End—

Adding Dial Number Mapping

To provision a new Dial Number mapping, perform the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>rm>dn-mapping**.
2	Enter the dialed number in the **dn** box, from 1 to 10 digits.
3	Select the mapping state from the **mapping-state** drop down list. Valid states are host and donor.
4	Click **Add**.
	—End—

Modifying Dial Number Mapping

To modify an existing Dial Number mapping, perform the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>rm>dn-mapping**.
2	Select the new mapping state from the **mapping-state** drop down list. Valid states are host and donor.
3	Click **Modify** to save these changes.

—End—

Deleting Dial Number Mapping

To delete Dial Number mappings, perform the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>rm>dn-mapping**.
2	Click the **Search** panel tab and locate the Dial Number mapping you want to delete. Double click the DN mapping to open it in the administration panel.
3	Click **Delete**.

—End—

Configuring Service Location Register

The Service Location Register (SLR) routes HLR-bound messaging to the correct HLR based on the subscriber data in the TCAP message. To do this, the USP:

1. intercepts all application MAP BEGIN messages enroute to the HLR
2. performs a TCAP decode on the message
3. performs IMSI to Routing Number (RN) or MSISDN to RN lookups in a high-speed, high capacity database.
4. extracts the RN to use in a outgoing GTT operation to determine the PC and SSN of the destination HLR.

This function enables the mapping of specific subscribers to an HLR as opposed to the current methods of tying IMSI ranges to HLRs. The USP supports up to six SLR LSS instances. Each instance corresponds to one NPC or NPS card

Modifying SLR data

Before modifying the SLR miscellaneous data, a local subsystem of LSS Class SLR must be provisioned. To modify SLR miscellaneous data, complete the following steps:

Step	Action
At the OAMP workstation	
1	Click **Configuration>slr>slr-misc.**
2	Select a value from the translation-type list. Valid choices are do-not-change-tt and change-tt. If you select change-tt, enter a translation type in the **to** box. Valid entries are decimal values from 0 to 255 list.
3	Enter a value in the **country-code** field.
4	Click **Modify**.
—End—	

Configuring SIP information

The USP, when used with Nortel MCS (MultiMedia Communication Server), uses the SIP protocol for communication. Default application timers and domain names are provided for SIP. These can be changed using the following steps.

Modifying application timer values

To modify the application timer values used by SIP, perform the following steps:

ATTENTION
TCAP timeout is not provisionable and has a default value of 2.5 seconds.

Step	Action
	At the OAMP workstation
1	Click **Configuration>sip>application-timers.**
2	Enter a new value for the Call timeout in the **call-timeout** box. Range is from 1 to 24 hours.
3	Click **Modify**.

—End—

Modifying the domain name

To modify the domain name used by SIP, perform the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>sip>domain-name.**
2	Enter a new value for the SS7 Domain in the **ss7-domain** box.
3	Enter a new value for the IP Domain in the **ip-domain** box.
4	Click **Modify**.

—End—

Configuring Low Layer Control Points (LLCP)

The USP provides a Lower Layer Intelligent Network (LLIN) application. This application supports intelligent network services that are based on detection points in the network and their associated called and calling party numbers. You can configure the detection points using the **Configuration>llcp** menu.

Intelligent network services are supported on the Low Layer Controller (LLC) and Low Layer Server (LLS) mission cards.

Provisioning the country code

The USP enables you to specify the country code to be used as the prefix in the LLCP database.

Adding the country code

To provision the country code, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>llcp>country-code.**
2	Select a system id from the **system-id** drop-down menu.
3	Enter the country code in the **country-code** box. The country code can be up to three digits in the range of 0–9.
4	Click **Add**.

—End—

Modifying the country code

To modify the country code, perform the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>llcp>country-code.**
2	Click the **Search** panel tab and locate the country code that you want to modify. Double click the country code to open it in the administration panel.
3	Modify the required fields.

4 Click **Modify**.

—End—

Deleting the country code

To delete an existing country code, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>llcp>country-code.**
2	Click the **Search** panel tab and locate the country code that you want to delete. Double click the country code to open it in the administration panel.
3	Click **Delete**.

—End—

Provisioning overlap outpulse

When the LLIN node receives an insufficient number of digits to complete a database lookup, it requests additional digits from the originator of the call. You can set a timeout value for this process for each system identity.

Adding the overlap outpulse value

To provision the overlap outpulse, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>llcp>overlap outpulse.**
2	Select a system id from the **system-id** drop-down menu.
3	Enter the interdigit timeout value in the **interdigit-timeout** box.
4	Click **Add**.

—End—

Modifying the overlap outpulse value

To modify the overlap outpulse value, perform the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>Ilcp>overlap outpulse.**
2	Click the **Search** panel tab and locate the value that you want to modify. Double click the value to open it in the administration panel.
3	Modify the required fields.
4	Click **Modify**.
	—End—

Deleting the overlap outpulse value

To delete existing overlap outpulse values, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>Ilcp>overlap outpulse.**
2	Click the **Search** panel tab and locate the value that you want to delete. Double click the value to open it in the administration panel.
3	Click **Delete**.
	—End—

Provisioning abort cause parameters

You can provision the parameters to be returned to the originator when an error condition causes a call to abort.

Adding abort cause parameters

To provision the abort cause parameters, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>Ilcp>abort-cause.**
2	Select a system id from the **system-id** drop-down menu.
3	Select a cause from the abort-cause drop-down menu. The options are:

- overlap-outpulsing
- relayed-idp
- t-inap-operation decode
- pabort-received

4 From the **coding standard** drop-down menu, select a coding standard to use when formatting the abort cause information. The options are:

- itu-t-standardized
- iso-iec-standard
- national-standard
- specific-standard

5 Select a location from the location drop-down menu. The location is a value in the range from 1–15. The system displays the valid location values.

6 Enter a cause value from 0–127 in the **cause-value** box or use the … selection box to select a value. The selector box provides an alphabetical list of cause values and their descriptions.

7 Click **Add**.

—End—

Modifying the abort cause parameters

To modify the abort cause parameters, perform the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>llcp>abort-cause.**
2	Click the **Search** panel tab and locate the abort cause parameters that you want to modify. Double click the value to open it in the Administration panel.
3	Modify the required fields.
4	Click **Modify**.

—End—

Deleting the abort cause parameters

To delete existing abort cause parameters, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>llcp>abort-cause.**
2	Click the **Search** panel tab and locate the parameters you want to delete. Double click the parameters to open them in the administration panel.
3	Click **Delete**.

—End—

Provisioning release cause parameters

You can provision the parameters to be returned to the originator when an error condition causes a call to be released.

Adding release cause parameters

To provision the release cause parameters, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>llcp>release-cause.**
2	Select a system id from the **system-id** drop-down menu.
3	Select a cause from the **release-cause** drop-down menu. The options are: • no-routing-instructions-found • overlap-outpulse-interdigit • time-out-expiration • event-report-bcsm-parameter-missing • call-gap-congestion
4	From the coding standard drop-down menu, select a coding standard to use when formatting the release cause information. The options are: • itu-t-standardized

- iso-iec-standard
- national-standard
- specific-standard

5 Select a location from the location drop-down menu. The location is a value in the range from 1–15. The system displays the valid location values.

6 Enter a cause value from 0–127 in the cause-value box or use the … selection box to select a value. The selector box provides an alphabetical list of cause values and their descriptions.

7 Click **Add**.

—End—

Modifying the release cause parameters

To modify release cause parameters, perform the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>llcp>release-cause.**
2	Click the **Search** panel tab and locate the release cause information that you want to modify. Double click the entry to open it in the administration panel.
3	Modify the required fields.
4	Click **Modify**.

—End—

Deleting the release cause parameters

To delete existing release cause parameters, complete the following steps

Step	Action
	At the OAMP workstation
1	Click **Configuration>llcp>release-cause.**

2 Click the Search panel tab and locate the parameters you want to delete. Double click the parameters to open them in the Administration panel.

3 Click **Delete**.

—End—

Provisioning LLCP timers

You can provision values for the timers used by LLCP.

Adding the LLCP timers

To provision the LLCP timers, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>llcp>llcp-timer.**
2	Select a system id from the **system-id** drop-down menu.
3	Enter a value in the **activity-test-timeout** box. The timeout value can range from 1–70 minutes.
4	Enter a value in the **default-gap-interval** box. The timeout value can range from 0–60 000 milliseconds.
5	Enter a value in the **default-gap-duration** box. The timeout value can range from 0–2047 seconds.
6	Click **Add**.

—End—

Modifying the LLCP timers

To modify the LLCP timers, perform the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>llcp>llcp-timer.**
2	Click the **Search** panel tab and locate the timer that you want to modify. Double click the timer to open it in the administration panel.
3	Modify the required fields.

4 Click **Modify**.

—End—

Deleting the LLCP timers

To delete existing timers, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>sccp>remote-pointcode.**
2	Click the **Search** panel tab and locate the timer that you want to delete. Double click the timer to open it in the administration panel.
3	Click **Delete**.

—End—

Provisioning the calling party address

You can modify the calling party address information in the SCCP portion of messages sent from the LLCP

Adding the calling party address

To provision the LCPGA information, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>llcp>lcpga-replace.**
2	Select a system id from the **system-id** drop-down menu.
3	From the **replace-lcgpa** drop-down menu, select the type of address replacement to perform. The options are: • do-not-replace • replace-all • replace-dpc-ssn

The type of address replacement that you select in this step will determine the other configuration options available:

Replacement type	Configurable fields	Steps
do-not-replace	-	Procedure is complete.
replace-all	**routing-indicator** **gt-indicator** **pointcode-included** **ssn-included**	Complete steps 4 though 8.
replace-dpc-ssn	**routing-indicator** **pointcode-included**	Complete steps 4, 6, and 8.

4 Select a routing type to use from the **routing-indicator** drop-down menu. The options are:

- route-pc to route based on the pointcode and SSN in the calling party address
- route-gt to route based on the GT information in the calling party address

If you selected replace-dpc-ssn from the replace-lcgpa drop-down menu in step 3, proceed to step 6 now.

5 Select a value in the range from 1–4 from the **gt-indicator** drop-down menu. When you configure the **gt-indicator** to use in the calling party address, the following options are available:

Option	Description	Enabled by gt-indicator
nature-of-address	A value ranging from 0–127. Specifies the nature of the address to use in the calling party address.	1, 4
gt-address	A string of 3–32 digits, including the numbers 0–9 and hex digits a–f. Specifies the gt address to use in the calling party address.	1, 2, 3, 4
translation-type	A value ranging from 0–255. Specifies the translation type to use in the calling party address.	2, 3, 4
numbering-plan	A value ranging from 0–6. Specifies the numbering plan to use in the calling party address.	3, 4

6 Select the **pointcode-included** box to include the pointcode of the selected system-id in the calling party address. If you selected **replace-dpc-ssn** from the **replace-lcgpa** drop-down menu in step 3, proceed to step 8 now.

7 Select the **ssn-included** box to include the ssn of the LLCP local subsystem in the calling party address.

8 Click **Add**.

—End—

Modifying the calling party address

To modify the calling party address, perform the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>llcp>lcpga-replace.**
2	Click the **Search** panel tab and locate the address information you want to modify. Double click the address to open it in the administration panel.
3	Modify the required fields.
4	Click **Modify**.

—End—

Deleting the calling party address

To delete existing information about the calling party address, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>llcp>lcpga-replace.**
2	Click the **Search** panel tab and locate the address that you want to delete. Double click the address to open it in the administration panel.
3	Click **Delete**.

—End—

Provisioning advice of charge (AOC) bypass

You can provision calling party numbers to be exempt from the advice of charge (AOC) functionality.

Adding the country code

To provision the AOC bypass, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>Ilcp>aoc-bypass.**
2	Select a system id from the **system-id** drop-down menu.
3	In the **inap-cgpa** field, enter the calling party number to exempt from the AOC functionality. The calling party number can be from 1–23 digits and can contain the digits 0–9 and the hex digits a–e.
4	Click **Add**.

—End—

Modifying the AOC bypass

To modify AOC bypass, perform the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>Ilcp>aoc-bypass.**
2	Click the **Search** panel tab and locate the entry that you want to modify. Double click the entry to open it in the administration panel.
3	Modify the required field.
4	Click **Modify**.

—End—

Deleting the AOC bypass

To delete existing RPCs, complete the following steps:

Step	Action

At the OAMP workstation

1 Click **Configuration>llcp>aoc-bypass.**

2 Click the **Search** panel tab and locate the entry that you want to delete. Double click the entry to open it in the administration panel.

3 Click **Delete**.

—End—

Provisioning routing procedures

You can associate a service key from the incoming TCAP message with a routing procedure.

Adding the routing procedure

To provision the routing procedure, complete the following steps:

Step	Action

At the OAMP workstation

1 Click **Configuration>llcp>llcp-tc-relay.**

2 Select a system id from the **system-id** drop-down menu.

3 In the **service-key** box, enter the service key that the routing procedure will apply to. The service key can range from 0–32767.

4 Select a routing procedure from the **tc-type** drop-down menu. The options are **tc-transfer** and **tc-relay**.

5 Click **Add**.

—End—

Modifying the routing procedure

To modify the routing procedure, perform the following steps:

Step	Action

At the OAMP workstation

1 Click **Configuration>llcp>llcp-tc-relay.**

2 Click the **Search** panel tab and locate the entry that you want to modify. Double click the entry to open it in the administration panel.

3 Modify the required fields.

4 Click **Modify**.

—End—

Deleting the routing procedure

To delete existing routing procedure, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>llcp>llcp-tc-relay.**
2	Click the **Search** panel tab and locate the entry that you want to delete. Double click the entry to open it in the administration panel.
3	Click **Delete**.

—End—

Provisioning callgap parameters

You can provisioning callgap information from the Configuration>llcp> **callgap** menu. The options under this menu allow you to provision the parameters used for callgap functionality, including:

- callgap-criteria
- callgap-profile
- callgap-profile-group
- callgap-traffic-rate

Adding the callgap criteria

To provision the callgap criteria, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>llcp>llcp-callgap-criteria.**
2	Select a system id from the **system-id** drop-down menu.

3 Enter a name to identify the criteria in the criteria-name box. The name can be from 1–7 characters.

4 Enter a value from 1–1000 in the traffic-contribution-factor box. The USP uses this value in conjunction with the BHCA value to calculate the gap interval in callgap messages that the LLCP sends to the SSP.

5 Enter a value from 0–2047 seconds in the **gap-duration** box. This value is the duration of the timeout that the SSP needs to apply to support the callgap procedure.

6 Click **Add**.

—End—

Adding the callgap profile

You can provision up to 150 profile names in the USP. You can then use the profile names to build callgap profile groups. To provision the callgap profile, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>llcp>llcp-callgap-profile.**
2	Select a system id from the **system-id** drop-down menu.
3	In the **profile-name** box, enter a name to identify the callgap profile. The name can be from 1–7 characters in length.
4	Click **Add**.

—End—

Adding the callgap profile group

To provision the callgap profile group, complete the following steps:

Step	Action
	At the OAMP workstation
1	Click **Configuration>llcp>llcp-callgap-profile-group.**
2	Select a profile name from the **profile-name** drop-down menu.
3	Select a system id from the **system-id** drop-down menu.

4 Enter the remote pointcode value in the **remote-pointcode** box or use the … selection box to select a remote pointcode that the callgap criteria will apply to.

5 In the **criteria-name** box, enter a name to identify the callgap criteria that will be applied to the remote pointcode or use the … selection box to select from a list of existing criteria names.

6 Click **Add**.

—End—

Adding the callgap traffic rate

To provision the callgap traffic rate, complete the following steps:

Step	Action

At the OAMP workstation

1 Click **Configuration>llcp>llcp-callgap-traffic-rate.**

2 Select a system id from the **system-id** drop-down menu.

3 Select a traffic rate type from the traffic-rate drop-down menu. The options are:

- office-wide
- service-key
- service-key-in-number

The type of traffic rate that you select in this step will determine the remaining configuration options.

4 In the **service-key** box, enter a value from 0–32767 to identify the service key to be matched in the received message.

5 In the **in-number** box, enter the calling party number associated with the service key. The calling party number can be from 1–23 digits and can contain the digits 0–9 and the hex digits a–f.

6 Enter a value in the range from 1–10000 in the **kbhca** box . The USP will apply this value when a matching entry is encountered on the message path.

7 Select a profile name from the **profile-name** drop-down menu.

8 Click **Add**.

—End—

Modifying the callgap parameters

To modify any of the callgap parameters, perform the following steps:

Step	Action

At the OAMP workstation

1 Click **Configuration>llcp>callgap.**

2 Select the required parameter from the submenu. The options are:

- callgap-criteria
- callgap-profile
- callgap-profile-group
- callgap-traffic-rate

3 Click the **Search** panel tab and locate the parameter that you want to modify. Double click the RPC to open it in the administration panel.

4 Modify the required fields.

5 Click **Modify**.

—End—

Deleting the callgap parameters

To delete existing callgap parameters, complete the following steps:

Step	Action

At the OAMP workstation

1 Click **Configuration>llcp>callgap.**

2 Select the required parameter from the submenu. The options are:

- callgap-criteria
- callgap-profile
- callgap-profile-group
- callgap-traffic-rate

3 Click the **Search** panel tab and locate the parameter that you want to delete. Double click the parameter to open it in the administration panel.

4 Click **Delete**.

—End—

Completing a high-speed link cutover

CAUTION
Conduct the cutover during a maintenance window, where the low-speed link traffic is below 0.2 erlang.

To cutover from 16 LSL to two HSLs, the low-speed link traffic must be less than 0.1 erlang.

This section details procedures for converting a Common Channel Signaling System 7 (SS7) low-speed link (LSL) linkset into an high-speed link (HSL) linkset.

Throughout this document, links originating on DS0A, V.35 or Channelized E1/T1 link system nodes are referred to as low-speed links (LSLs). Links originating on high-speed link or SS7 IP link system nodes are referred to as high-speed links (HSL). The ATM high-speed link system node physically consists of the T1/E1 Transition Module (TM) and a link mission card. The computing engine mission card consists of a Power/SCSI/Ethernet (PSE) TM, an SS7 IP link mission card, and an MTP2 E1 HSL.

This section also provides the procedures to transition from low-speed link (LSL) linksets to high-speed link (HSL) linksets.

Hardware requirements

The following hardware is required for ATM high-speed links:

- T1/E1 Transition Module NTST81BA, or NTST81AB
- Link Mission Card
  - NTST10BA (base link card)

The following hardware is required for E1 MTP2 high-speed links:

- T1/E1 Transition Module NTST81BA
- Link Mission Card
  - NTST10CA

The following hardware is required for SS7 IP High-speed links:

- PSE TM NTST09AA, NTST09AB, or NTST09AC
- IP Link Mission Card which includes:
  - NTST11BA (LE3)

For further information about issues related to hardware installations involving high-speed links (HSL), contact the installation prime.

Software requirements

Software release USP 8.0 or later is required for this cutover.

High-speed link guidelines

ATTENTION

Ensure that the network to be converted and all connecting nodes and network connections are in service.

Ensure that all alarms have been cleared before proceeding with the cutover procedure.

Review and coordinate the cutover procedure with other operating companies in the network that are involved in the cutover procedure.

Up to sixteen ATM/E1or MTP2 HSL system nodes can be commissioned on an extension shelf (12 on a control shelf). For IP HSLs, up to eight HSL, can be commissioned on each shelf. On a fully populated system, an LSL link system node must be decommissioned before installing each HSL system node. Existing links on the LSL system node must be moved to other link system nodes or decommissioned. If your system is fully populated, contact your next level of support.

The cutover procedure requires operating company personnel to be present at each office that is affected by a link change during any step of the procedure. Nortel Networks recommends that you appoint a cutover project manager to coordinate all the steps for the cutover.

Note the following guidelines when performing the HSL cutover:

- The high-speed link system node can support HSLs for C-links, B/D links, or A-links.
- Carry out the C-linkset cutover before the signaling transfer point (STP) quad B/D-linkset cutover because only two nodes are involved in the C-linkset cutover.
- An HSL system node provides a single port in the same space that an LSL system node provides four or eight ports. Therefore, on a full system, four or eight LSL ports must be decommissioned for each HSL added.

The HSL cutover applies to:

- C-linkset cutover for a signaling transfer point (STP) pair
- B-linkset cutover for an STP quad
- D-linkset cutover for an STP quad

- A-links-to-service control point (SCP) cutover
- A-links-to-SSP cutover

Nortel Networks recommends performing the C-linkset cutover for an STP pair before attempting the B-linkset and D-linkset cutover for an STP quad.

High-speed link cutover procedures

ATTENTION

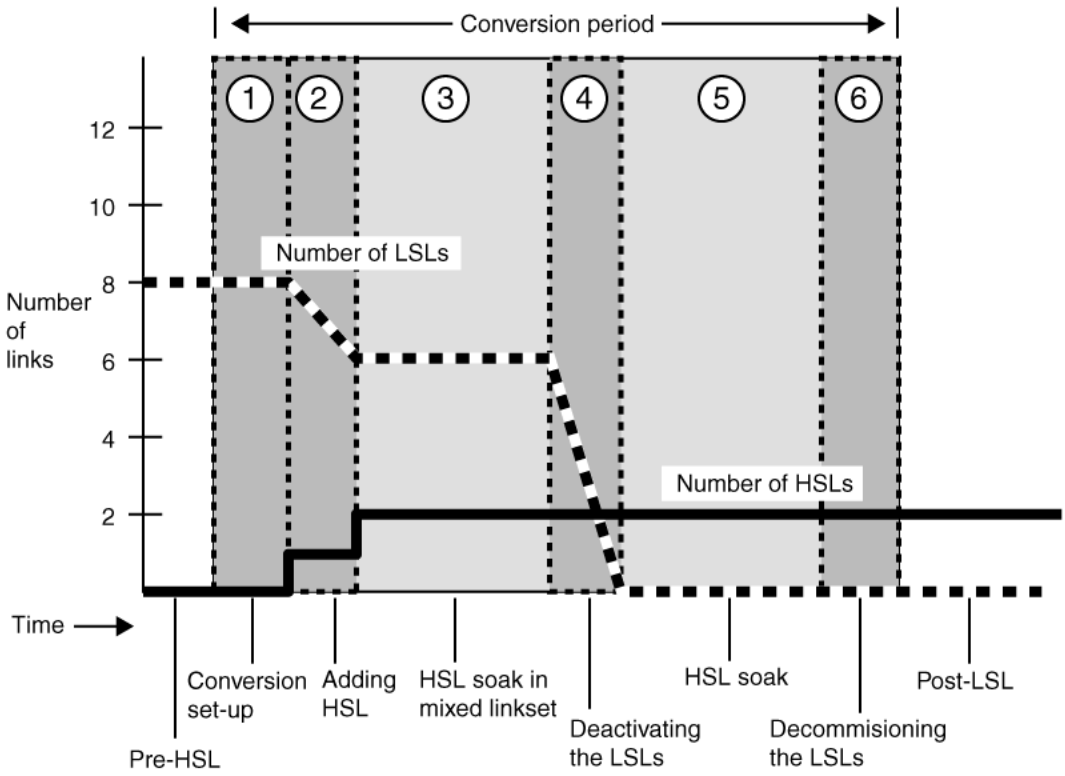
During cutover, HSLs and LSLs are supported in the same mixed linkset. The USP supports mixed HSL and LSL linksets only during the cutover procedure. After the cutover is complete, linksets will be homogeneous.

ATTENTION

Contact your next level of support to determine the correct version of the engineering bulletin and to determine if any other engineering bulletins apply.

The following figure shows the cutover steps.

Link count during cutover



The HSL cutover requires completing the following procedures:

- "Setting up a cutover" (page 340)
- "Adding high-speed links" (page 341)
- "Offlining the low-speed links" (page 341)

Setting up a cutover

Step	Action
1	Configure the HSL system node. For more information, see "Configuring a Network Element System Node" (page 78).
2	Configure ports. For MTP2 E1 HSLs the cable must be connected to RJ45 cable. For more information, see "Configuring Ports" (page 90).
3	Load the HSL system nodes. For more information, see "Adding Links" (page 129).

—End—

Adding high-speed links

Step	Action
1	Configure SAAL timers. For more information, see "Adding a SAAL timer index" (page 108)
2	Configure SAAL parameters. For more information, see "Adding a SAAL parameter index" (page 108).
3	Deactivate LSLs. For more information, see "Activating and Deactivating Links" (page 135).
4	Delete LSLs. For more information, see "Deleting Links" (page 134).
5	Configure HSLs. For more information, see "Adding Links" (page 129).
6	Perform a bit error rate test (BERT) on ATM and E1 MTP2 before RTSing the links. For more information about BERT, see *USP Security and Administration* (NN10159-611).
7	RTS the link. For more information, see "Activating and Deactivating Links" (page 135).
8	Soak the HSLs in a mixed linkset. Refer to the procedure "Soaking the high-speed links" (page 342).

—End—

Offlining the low-speed links

Step	Action
1	Calculate LSL traffic. For more information about USP traffic calculations, see *USP Performance Management* (NN10137-711).

ATTENTION

If the Erlang level is above 0.2 E, contact the personnel responsible for your next level of support. Use Operational Measurements to calculate traffic and to determine if you can proceed with the cutover.

2 Calculate LSL traffic on the mate node. For more information about USP traffic calculations, see *USP Performance Management* (NN10137-711).

ATTENTION
If the Erlang level is above 0.2 E, contact the personnel responsible for your next level of support. Use Operational Measurements to calculate traffic and to determine if you can proceed with the cutover.

3 Deactivate the LSL. For more information, see "Activating and Deactivating Links" (page 135).

4 Deactivate all remaining LSLs in the linkset. For more information, see "Activating and Deactivating Links" (page 135).

5 Deactivate the LSL on the mate node. For more information, see "Activating and Deactivating Links" (page 135).

6 Deactivate all remaining LSLs in the linkset on the mate node. For more information, see "Activating and Deactivating Links" (page 135).

7 Soak the HSLs. Refer to the procedure "Soaking the high-speed links" (page 342).

8 Decommission the LSLs. See procedure, "Deleting Links" (page 134) to complete the following:

- Delete the datafill for the LSLs.
- Delete LSLs for remaining links in the linkset.
- Delete the datafill for the LSLs on the mate node.
- Delete LSLs for remaining links in the linkset on the mate node.

—End—

Soaking the high-speed links

Step	Action

ATTENTION
If a failure occurs at any time during this phase, perform procedure, "Recovering from high-speed link failure" (page 343).

1 Allow the system to soak for one hour.

2 Check the logs for the system. Click **Fault>Logs** on the main menu to open the Logs window.

3 Check the alarms for the system. To view alarms, click the alarm banner. The Alarms window appears. Check for alarms.

4 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

—End—

Recovering from high-speed link failure

Step Action

At the OAMP workstation

ATTENTION
If an HSL fails, traffic is redistributed over the remaining links in the linkset or combined linkset.

1 Deactivate and offline the failed HSL. For more information, see "Activating and Deactivating Links" (page 135).

2 Perform a remote Loopback at the far end of the link. For more information about remote loopback, see *USP Security and Administration* (NN10159-611). On the local end of the link, perform a BERT Operation. For more information about BERT, see *USP Security and Administration* (NN10159-611). Clear any faults before proceeding.

3 RTS the HSL. For more information, see "Activating and Deactivating Links" (page 135).

4 Select one of the following options:

If	Go to
the failure condition exists	Step 5
the failure condition clears	Step 8

5 Provision LSLs. For more information, see "Adding Links" (page 129).

6 RTS the LSLs. For more information, see "Activating and Deactivating Links" (page 135).

7 Contact your next level of support.

8 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

—End—

Carrier VoIP

USP Configuration Management

Publication: NN10093-511
Document status: Standard
Document version: 08.02
Document date: 20 October 2006

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

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