Carrier VoIP

USP Security and Administration

NN10159-611

Document status: Standard
Document version: 07.04
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 sections detail what's new in *USP Security and Administration* (NN10159-611) for release (I)SN09U.

Features

There are no feature changes that affect *USP Security and Administration* (NN10159-611) for this release.

Other changes

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

Modified procedure, Restoring a system configuration from a data snapshot stored on your alternate boot server

To improve clarity, minor changes were made to "Restoring a system configuration from a data snapshot stored on your alternate boot server" (page 34) .

Modified procedure, Configuring an automated backup

In "Configuring an automated backup" (page 27) a link was added to navigate to the required command line syntax.

USP Security and Administration

Logging in and out of the system

The following procedure provides the instructions to log in and out of a USP system that is installed on either a Windows-based workstation or the CS 2000 Management Tools (CMT) server.

Logging into the system

Step	Action

At your workstation

1 Log in to the USP GUI.

If the USP GUI is installed on	Do
a Windows-based OAMP workstation	step 2
the CMT server	step 5

At the windows-based OAMP workstation

2 Click the Windows **Start** button on your desktop.

3 Select **Programs->Universal Signaling Point->Universal Signaling Point GUI**.

The USP Interface Client window appears with either the Session-Login or Site Manager dialog box displayed in the window.

4 Proceed to step 10

At your workstation

5 Launch your web browser.

6 In the Address field, enter the name or IP address of the CMT server.

The Application Launch Point page appears.

7 Click **Application Launcher**.

The Login window appears.

8 Enter your user name and password, then click **Log In**.

The Application Launch Point window appears after a valid login.

9 Click the **Universal Signaling Point Interface Client** link to launch the GUI.

The USP Interface Client window appears with either the Session-Login or Site Manager dialog box displayed in the window.

10 Use the following table to determine your next step.

If the	Do
Site Manager dialog box appears	step 11
Session-Login dialog box appears	step 14

11 Click **New**, and enter the site name, the rtc-12 ipaddress and rtc-15 ipaddress.

12 Click **Apply**.

13 Click **OK**.

The Session-Login dialog box appears.

14 Enter the login account and password.

15 You have completed this procedure. If applicable, return to the higher level task or procedure that directed you to this procedure.

—End—

Logging out of the system

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

—End—

Security: User Accounts

ATTENTION

To provide emergency technical assistance and recovery, Nortel Networks support staff require a valid user account and password that is available 24/7. The system is distributed with a default account (FIELD). If this account is changed or disabled and no other valid account is available during a technical issue, Nortel Networks support staff will be unable to provide assistance as they will not be able to log into the system. It is the customer's responsibility to ensure that appropriate measures are in place to ensure this account information is available at all times.

Nortel Networks recommends that you change the default password for the FIELD user account after the initial installation is complete.

ATTENTION

Refer to "Changing your password" (page 10) for a list of conditions and restrictions on User IDs and passwords.

User accounts give users access to the system that is maintained from their OAMP workstation. Each user account is assigned command classes, which dictate the type of commands a user can execute. Depending on the command classes assigned to a user account, the user can execute one or more of the following types of commands:

- read
- provisioning
- maintenance
- other

Command classes are defined in the command class form. The command class form contains all the available commands, which are categorized under subsystems and tables. In USP 10.0, the command class form contains the following new tables:

Subsystem	Table
administration	syslog-delivery
llcp	lcgpa-replace
	overlap-outpulse
	release-cause
	abort-cause
	llcp-timer
	tc-relay

Subsystem	Table
	callgap-criteria
	callgap-profile
	callgap-profile-group
	callgap-traffic-rate
	country-code
	aoc-bypass

All USP GUI users must have the command classes associated with the following tables:

- cli-session
- table-change-notification
- prov-reference-count

Following are procedures to add a user account to the system, modify user account information, delete users, and change a password.

Adding users

Step	Action
	At the OAMP workstation
1	Click **Security>user-account**.
2	Click **Administration**.
3	Click **New**.
4	Enter the user id (a maximum of 32 characters) in the **user-id** box.
5	Enter the full name of the user (a maximum of 32 characters) in the **user-name** box.
6	Enter a description of the user in the **user-description** box. You can enter a maximum of 80 characters.
7	Enter the Class Map in the **class-map** dialog box. The class map assigns user permissions as defined in the Command Class form.
8	Click the **enable-option** checkbox to activate the account.
9	Enter the password for the user account (a maximum of 32 characters) in the **user-password** box.

10 Re-enter the user account password in the **confirm-user-password** box.

11 Click **Add**.

—End—

User account information

The following user account information can be modified:

- User Name
- User Description
- User Password
- Class Map
- Enable Option

To modify the information for a user account, perform the following steps:

Modifying user account information

Step	Action
	At the OAMP workstation
1	To modify user account information, click **Security>user-account**.
2	Select an account from the User Accounts list. To do this, open the **Search** panel and select an account from the **Retrieval results** window. Double-click the record to transfer it to the Administration panel.
3	To change the name of the user, modify the text in the **user-name** box. You can enter a maximum of 32 characters.
4	To change the description of the user account, modify the text in the **user-description** box. You can enter a maximum of 80 characters.
5	To change the privileges for the user account, enter the Class Map in the **class-map** dialog box. The class map assigns user permissions as defined in the Command Class form. The User Privileges list cannot be modified for the FIELD user account unless a new root account exists.
6	Use the **enable** checkbox to activate or deactivate the account.
7	To change the password for the user account, modify the text in the **User Password** box. Highlight the **Confirm User Password**

box and enter the modified user password. The box can contain a maximum of 32 characters.

ATTENTION
Nortel Networks recommends that you change the default password for the FIELD user account after the initial installation is complete.

8 Click **Modify**.

—End—

Deleting users

Step	Action
	At the OAMP workstation
1	Click **Security>user-account**.
2	Select an account from the User Accounts list. To do this, open the **Search** panel and select an account from the **Retrieval results** window. The FIELD user account cannot be deleted.
3	Click **Delete**.

—End—

Changing your password

Step	Action
	At the OAMP workstation
1	Click **Security>user-account**.
2	Click **Search** and select the account you want to change. Double-click on the account to transfer to the Administration panel.
3	Enter the new password in the **user-password** box. The following conditions and restrictions apply to all passwords and User IDs on the USP. Existing User accounts created during previous releases are not exempt from these restrictions. • User IDs and passwords are case-sensitive.

- Passwords must be a minimum of six characters in length, and contain at least one letter, one number and any special character except for "~", "!", or "#".
- Passwords cannot contain the associated User ID.

ATTENTION
The conditions and restrictions listed below apply to passwords only if the password aging feature is enabled in USP.

- A history of the last 5 passwords is maintained. Users are not allowed to change their password if the new password matches any of their past 5 passwords.
- Lifespan of a password can be configured only by the Administrator. Its value ranges between 20 and 90 days and the default is 30 days.
- Grace login count for erroneous logins can be configured only by the Administrator. Its value ranges between 1 and 3 login attempts and the default is 3. The ability to turn this feature ON or OFF can only be set by the Administrator and the default is OFF.
- Users can to change their password even after password lifespan expiry, for logins up to the grace count.
- User accounts are locked when password lifespan and grace login count expires.
- Users are notified how many times a login is allowed before changing password and after password lifespan is expired.
- Logs will be issued when:
  - password lifespan is expired
  - grace login count is expired
  - account is locked

4 Re-enter the new user password in the **user-password-confirm** box.

5 Click **Modify**.

—End—

ATTENTION

The password aging features are not intended for applications using Remote Authentication.

Only Administrators can enable and set the password-aging options. The procedures are detailed below.

Password-Aging provisioning

Step	Action
	At the OAMP workstation
1	Click **Security>user-security-admin**.
2	Click the **password-aging-enabled option** checkbox to activate the password aging features.
3	Enter the desired **password-aging-interval**. The lifespan value ranges between 20 and 90 days and the default is 30 days.
4	Enter the desired number of **grace-period-logins**. The value ranges between 1 and 3 login attempts and the default is 3.
5	Click **Modify**.

—End—

Security: User Session

During a user session, you can perform the following functions:

- View the list of users currently logged into the system.
- Send messages to other users who are currently logged into the system, if your user account has administrative privileges.
- Log off users.

Viewing the user session list

Step	Action
	At the OAMP workstation
1	Click **Security>user-session**.
2	View the User Session list. To do this, click **Realtime**.
	—End—

This window displays the user account names and session data of the users who are currently logged in to the system.

Sending messages to current users

Step	Action
	At the OAMP workstation
1	Click **Security>user-session**. This window displays the user account names and session data of the users who are currently logged in to the system.
2	View the User Session list. To do this, click **Realtime**.
3	Select the session associated with the user(s) to whom you want to send a message. Double-click on the session to transfer to the Administration panel.
4	Click **Message**.
5	Enter a message (a maximum of 80 characters) in the Message box.
6	Click **OK**.
	—End—

Logging out current users

Step	Action
	At the OAMP workstation
1	Click **Security>user-session**. This window displays the user account names and session data of the users who are currently logged in to the system.
2	Click **Administration**.
3	View the User Session list. To do this, click **Realtime**.
4	Select the session associated with the user(s) you want to log out of the system. Double-click on the session to transfer to the Administration panel.
5	Click **force-out**.
6	Enter a message (a maximum of 80 characters) in the Message box (optional).
7	Click **OK**.

—End—

Security: Command Classes

The Command Class table assigns command classes to the command set for each table. Commands are grouped into read commands, provisioning commands, and maintenance commands.

Provisioning a command class for a table command

Step	Action
	At the OAMP workstation
1	Click **Security>command-class**.
2	Click the **Search** tab. Double-click on the record that contains the command(s) for the required table and subsystem to transfer to the Administration panel.
3	Enter a value for Command Class in the **Command Class** dialog box. Valid range is 0 to 31.
4	Click **Modify**.
	—End—

Security: Remote Authentication

Remote Authentication enables the USP to verify a user ID and password with a Remote Authentication server for the CLI and GUI sessions.

When you choose Remote Authentication, the provisioning data on the Remote Authentication Server must match the remote user group on the USP. You must add the remote user group on the USP and ensure that the user is provisioned on the Remote Authentication Server. For information about adding remote user groups, see "Security: Remote User Groups" (page 20). For information about provisioning the user on the Remote Authentication Server, see *IEMS Administration and Security* (NN10336-611).

Enabling remote authentication

Step	Action
	At the OAMP workstation
1	Click **Security>remote-authentication**.
2	Check the **enabled-option** checkbox.
3	Enter the IP Address at he primary remote authentication server in the **primary-ipaddress** box.
4	Enter the IP Address of the secondary remote authentication server in the **secondary-ipaddress** box.
5	Select an emergency access user ID from the **emergency-access-userid** drop down list.
6	Click **Modify**.
	—End—

Disabling remote authentication

Step	Action
	At the OAMP workstation
1	Click **Security>remote-authentication**.
2	Uncheck the **enabled-option** checkbox.
3	Click **Modify**.

—End—

Security: Authentication Methods

When you enable authentication, you can use either Standard Authentication or a Central Authentication Server. For direct connections, you can use 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 the Central Authentication Server.

Central Authentication Server

When you choose Central Authentication Server as the authentication method, the provisioning data on the Central Authentication Server must match the remote user group on the USP. Add the remote user group on the USP, and ensure that the user is provisioned on the Central Authentication Server. For information about adding remote user groups on the USP, see "Security: Authentication Methods" (page 18). For information about provisioning the user on the Central Authentication Server, see *IEMS Security and Administration* (NN10336-611).

The Integrated Element Management System (IEMS) provides the PAM + Proxy authentication mechanism for the Central Authentication Server scheme. When the user selects Central Authentication Server authentication, the USP GUI uses the supplied IP address and port to establish an HTTPS connection on the IEMS server. For information on provisioning log delivery to the IEMS, see *USP Fault Management* (NN10071-911).

Configuring the Central Authentication Server

Step	Action
	At the OAMP workstation
1	Click **File>site manager** to access the Site Manager window.
2	Select the site that you want to configure.
3	Select Central Authentication Server to perform PAM + Proxy authentication using HTTPS.
4	Enter the IP address and port number of the authentication server. The default port value is 8443.
5	Click on the **enable proxy** checkbox.
6	Select either Telnet or SSH as the protocol for the connection.

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

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

8 Enter port of the proxy server in **proxy-port** box.

9 Click **Modify**.

—End—

Configuring Standard Authentication

Step	Action
	At the OAMP workstation
1	Click **File>site manager** to access the Site Manager window.
2	Select the site that you want to configure.
3	Select Standard Authentication to perform authentication at the USP.
4	Click **Modify**.

—End—

Security: Remote User Groups

To isolate the Z-USP type's internal representation of command class privileges, a mapping function allows an administrator to specify a mapping between the remote user authentication server's user groups and the internal Z-USP type's command class privileges. This mapping function is provided by the remote-usergroup's table.

Adding a remote user group

Step	Action
	At the OAMP workstation
1	Click **Security>remote-usergroup**.
2	Click **Administration**.
3	Click **New**.
4	Enter the remote usergroup name in the **remote-usergroup** box.
5	Enter the internal class bit map in the **internal-class-bitmap** box.
6	Enter the internal class map in the **internal-class-map** box.
7	Click **Add**.

—End—

Modifying a remote user group

Step	Action
	At the OAMP workstation
1	Click **Security>remote-usergroup**.
2	Click the **Search** tab and find the remote user group you want to modify.
3	Double-click on the remote user group that you want to modify to transfer to the Administration panel.
4	Enter the new internal class bit map in the **internal-class-bitmap** box.
5	Enter the new internal class map in the **internal-class-map** box
6	Click **Modify**.

—End—

Deleting a remote user group

Step	Action
	At the OAMP workstation
1	Click **Security>remote-usergroup**.
2	Click the **Search** tab and find the remote user group you want to modify.
3	Double-click on the remoter user group that you want to modify to transfer to the Administration panel.
4	Click **Delete**.

—End—

Security: Prompt Level

The Z-USP type JAVA GUI can be configured to provide different levels of user prompting to confirm commands issued by the GUI. The prompt levels are listed as follows:

- all commands The user is prompted to confirm every command issued through the GUI.
- service impacting only The user is prompted to confirm service affecting commands issued through the GUI.
- no prompting The user is not prompted to confirm any command.

Configuring the prompt level

Step	Action
	At the OAMP workstation
1	Click **Security>prompt-level**.
2	Select a prompt level from the radio button options that appear: • all commands • service impacting only • no prompting

—End—

Security: Session Lockout

The USP JAVA GUI locks a user session if the session is idle for a predefined length of time. The user must provide their password to the system to resume their session. The lockout options are listed as follows:

- lock session now - Immediately locks the GUI.
- 5 mins of inactivity - Locks the GUI after 5 minutes of idle time.
- 15 mins of inactivity - Locks the GUI after 15 minutes of idle time.
- 30 mins of inactivity - Locks the GUI after 30 minutes of idle time.
- disabled - Does not allow the lockout to occur.

Configuring session lockout

Step	Action
	At the OAMP workstation
1	Click **Security>session-lockout**.
2	Select a prompt level from the radio button options that appear: • lock session now • 5 mins of inactivity • 15 mins of inactivity • 30 mins of inactivity • disabled

—End—

Administration: Manual Backup

If you change the external IP address of an Real-time Controller (RTC) system node in your system (or perform any other data provision changes on your system), you should immediately perform a backup operation and delete any data snapshots that were made before you changed the IP address. This ensures proper communication with your OAMP workstations.

Performing a backup operation

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.
3	Click the corresponding checkboxes to activate the following options, as appropriate: • *transfer snapshot to alternate boot server* Nortel Networks recommends that you enable this option. If you don't select this option, a warning dialog box appears. Click **Yes** to continue. • *set as active snapshot on alternate boot server* Nortel Networks recommends that you enable this option. If you don't select this option, a warning dialog box appears. Click **Yes** to continue. • *delete oldest snapshot on alternate boot server if maximum reached (16)* • *delete oldest snapshot on rtc if maximum reached (5)*
4	Click **Create** to create the data snapshot. This can take several minutes, depending on system activity.
5	Click **Close** to close the Backup Active RTC window and return to the Administration window.
6	If you selected **transfer snapshot to alternate boot server** on alt boot server, go to step 12.
7	Click **Administration>file-manager**. The File Manager window appears.

8 Select the active RTC system node from the **Destination** list in the right window pane.

9 Select the new data snapshot from the **Snapshot** box in the Destination portion of the window. Make note of the timestamp of the data snapshot.

10 Copy the snapshot to your alternate boot server by clicking <--. An hourglass appears while the data snapshot is copied. The boxes in the **Source** portion (left window) of the window are updated with the information for the copied data snapshot when the copy operation is complete.

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

11 When the file is transferred, click **Close**.

12 Update the Alternate Boot Snapshot using the ABS Settings ABS window:

a. Open the Alternate Boot Server (ABS) Configuration Manager window by clicking **ABS Settings** on the Administration>alternate-boot-server window.

b. Select an alternate snapshot by clicking the arrow button.

c. Click **Modify** to save your changes and close the window.

13 Your backup is complete.

—End—

Using the Command Line Interface

The same backup procedure may be performed via the CLI. The command syntax is:

admin backup create

"snapshot-description" abs-transfer-option abs-active-option rtc-delete-oldest-option abs-delete-oldest-option

where:
snapshot-description can be up to 32 characters and the other four options are set by entering either **y** (for enabled) or **n** (for disabled).

See "Administration: Manual Backup" (page 24) for option descriptions.

The following example creates a snapshot named "*my snapshot*", transfers it to the ABS and sets it as active. It also deletes the oldest snapshot on the rtc or abs, if the maximum number of snapshots is reached on either:

admin backup create "my snapshot" y y y y

A list of possible CLI return codes is as follows:

Rcode	Rcode text
0x40100001	snapshot-description must be string, length(1 - 32), no additional character filter
0x40100002	rtc-delete-oldest-option must be string, length(1 - 1), boolean (Y, y, N, n)
0x40100003	abs-transfer-option must be string, length(1 - 1), boolean (Y, y, N, n)
0x40100004	abs-active-option must be string, length(1 - 1), boolean (Y, y, N, n)
0x40100005	abs-delete-oldest-option must be string, length(1 - 1), boolean (Y, y, N, n)
0x80100001	missing snapshot-description
0x80100002	insufficient disk space on rtc
0x80100003	maximum number of snapshots reached on rtc
0x80100004	maximum number of snapshots reached on abs
0x80100005	unable to delete oldest snapshot on rtc
0x80100006	unable to delete oldest snapshot on abs
0x80100007	unable to transfer snapshot to abs
0x80100008	unable to set snapshot as active on abs
0x80100009	unable to connect to abs, run abs test for details
0x8010000A	invalid combination of command options

Administration: Automated Backup

To capture the current configuration of the USP, a snapshot (backup) is created. The snapshot contains all configuration data, as well as logs and operational measurements. A snapshot can be initiated via a GUI connection or via a CLI session. The length of time required to create a snapshot depends on system activity and the amount of configuration data present but will be typically between 5 and 20 minutes.

To perform an automated backup, use the scheduler facility to execute a CLI command. To provision the system to run a scheduled CLI command, perform the following steps.

Configuring an automated backup

Step	Action
	At the OAMP workstation
1	Open the CLI Command Scheduler window. Click **Administration>Scheduler**.
2	Enter a **schedule-id** using any decimal value from 0 to 99.
3	In the **cmd-string** portion of the window, enter the desired CLI command and click the **enabled** checkbox. See "Using the Command Line Interface" (page 25) for command syntax. CLI commands can be scheduled but will not run until you enable them.
4	Click the calendar icon and select a date for the CLI command to begin from the **start-date** list.
5	Click the clock and select a starting time from the **start-time** box. The time must be in the form of a 24-hour clock (hh:mm:ss).
6	Enter the length of the CLI command window, in minutes, in the **start-window** Box.
7	Enter a Recurrence Pattern: • Select **none** to prevent automated backups. • Select the **daily** radio button and enter the desired interval. • Select the **weekly** radio button and enter the desired recurrence interval, then select a day of the week for the backup to occur from the drop down menu. • Select the **monthly** radio button and enter the desired interval.

8 To provision exempt days when the command does not run (such as holidays or other high-traffic days), click **Exempt Days**.

9 Click **Add**.

10 If you want the system to run the CLI command immediately, click **Run Now**.

—End—

Administration: Backup USP Data to CD-RW in Solaris

This procedure enables you to back up onto CD-RW the snapshots that are created and transferred from RTC to your OAMP workstation.

ATTENTION
This procedure is used only for Solaris-based non-SPFS OAMP workstations. Root privilege is required to perform this procedure.

Performing a USP data backup

Step	Action

At the Solaris-based OAMP workstation

1 Make a directory to store backup files by entering the following command at the prompt (only need to do once):

mkdir /backup

2 Make a directory to temporarily store USP backup data (do this each time you back up USP data).

You can use the current date to name the temporary directory, for example: 20051115.

mkdir /backup/<temporary directory>

Example
mkdir /backup/20051115

3 Back up USP data files to a dumped file and save the file to the <temporary directory> by entering the following command:

ufsdump 5uf /backup/<temporary directory>/<dumped filename> <USP data directory>

The default <USP data directory> is ../ntssgusp/abs/sites if you selected the "transfer snapshot to alternate boot server" option when you created the snapshot.

Example
ufsdump 5uf /backup/20051115/usp_data_20051115.dmp /opt/usp/ntssgusp/abs/sites

4 Backup DHCP configuration files to a dumped file and save the file to the <temporary directory> by entering the following command:

ufsdump 5uf /backup/<temporary directory>/<dumped filename><DCHP configuration directory>

Example
ufsdump 5uf /backup/20051115/dhcp_20051115.dmp /var/dhcp

5 Copy the NFS configuration file to the <temporary directory>.

cp /etc/dfs/dfstab /backup/<temporary directory>

Example
cp /etc/dfs/dfstab /backup/20051115

6 Create an ISO file for writing the backup files to CD-RW.

mkisofs -r -o /backup/<temporary directory>/<ISO filename> /backup/<temporary directory>

Example
mkisofs -r -o /backup/20051115/iso_20051115.img /backup/20051115

7 Insert a blank CD-RW to the CD-RW drive.

To check whether the CD-RW is blank, you can enter the following command:

cdrw -M

To erase the contents of the CD-RW, you can enter the following command:

cdrw -b all

8 Write the ISO file to the CD-RW by entering the following:

cdrw -i /backup/<temporary directory>/<ISO filename>.

Example
cdrw -i /backup/20051115/iso_20051115.img

9 Remove the /<temporary directory>/by entering the following:

rm -Rf /backup/<temporary directory>

Example
rm -Rf /backup/20051115/

10 Remove the CD-RW from the CD-RW drive. Label it and store it in a safe place.

11 You have completed this procedure.

—End—

Administration: OAMP Workstation Backup

You can perform two types of backup on your OAMP workstation, manual and automatic. Manual backups are performed from the desktop by manually initializing the backup process. Automatic backups are performed according to the settings defined in the tape drive application.

ATTENTION
Nortel Networks recommends that you use the automatic backups to ensure that the data that is stored on the tapes is up-to-date.

The OAMP workstation is equipped with a tape drive, software to support tape backup, and five blank data tapes. These tapes enable approximately one month's worth of backups to be kept on-site.

ATTENTION
Nortel Networks recommends that you label the tapes to indicate the OAMP workstation associated with the backups to ensure that any recovery operations are performed from the correct tape.

Backup schedule

You should create a schedule for your automatic backups to ensure up-to-date storage of the system configuration of your OAMP workstation.

ATTENTION
Nortel Networks recommends that you perform a full system backup once a week and modified (differential) backups once a day.

Manual backup

Nortel Networks recommends that you perform a manual backup of your OAMP workstation after initial installation.

To perform a manual backup of the system configuration for your OAMP workstation, refer to the documentation provided with your Colorado or Veritas software.

Automatic backup configuration

There are two types of automatic backup: full system backup and modified (differential) system backup.

The full system backup saves all the files contained in the hard disk on your OAMP workstation.

The modified (differential) system backup saves only the files on the hard disk that have been modified since the last full system backup.

When you are using automatic backup, you must leave your OAMP workstation turned on with Windows running and ensure that there is a tape in the tape drive.

During the initial installation of your system, the tape drive application was configured to perform an automatic full system backup once a week, every Saturday at 1:00am. However, you can modify the settings in the tape drive application to suit your needs.

If you do not change the default setting for automatic full system backup, you need to swap out the tape every Friday.

In order for automatic backups to work, the tape drive scheduler icon must be active in the notification box in the taskbar with the automated daily backups option enabled, your OAMP workstation must remain on with Windows active, and a tape must be in the tape drive.

Verify the current modified system backup settings

There is a tape drive configuration file associated with the modified system backup. To verify that the current settings in the configuration file matches the system requirements, refer to the tape drive documentation provided with the OAMP workstation.

View the current automatic backup schedule

To view the current settings for automatic backup in the tape drive application, refer to the tape drive documentation provided with the OAMP workstation.

Administration: Restore Operations

You can use the restore operation to return your system to a configuration that was saved during a backup operation. The typical use of the restore operation is as follows:

- An emergency situation occurs that requires you to restore a system configuration from a stored data snapshot.
- You use the file manager function to ensure that there are copies of the data snapshot to be restored on both RTC system nodes.
- You make the data snapshot the boot snapshot for both RTC system nodes.
- You deactivate the linksets and change the path state of the application server process (ASP) paths to Down for your system, as appropriate.
- You perform a complete office recovery (COR) on your system, which means that you unseat the RTC system nodes, turn off both power switches on the shelf, reseat the RTC system nodes, and then restore power. Your stored data snapshot is now the running data snapshot.

Complete the following procedures to restore data snapshots stored on your alternate boot server or on the RTC system nodes.

CAUTION
Performing a COR on your system is service affecting. Nortel recommends that you do this during off-peak hours and that you ensure that a mated system is available.

CAUTION
Do not power down the shelf when the SCSI disk light on the RTC system node is on. To do so could cause a disk failure.

CAUTION
Wear wrist straps, and use standard antistatic precautions.

Restoring a system configuration from a data snapshot stored on your alternate boot server

Step	Action
	At the OAMP workstation
1	Click **Administration>file-manager**.
2	Modify the boot data configuration at RTC12. For more information about modifying boot data configuration see, *USP Configuration Management* (NN10093-511).
3	Modify the boot data configuration at RTC15. For more information about modifying boot data configuration see, *USP Configuration Management* (NN10093-511).
4	Deactivate the linksets for your system. Deactivating the linksets aids in shutting down the application because the Network Elements connected to the USP can take action accordingly. For more information about deactivating linksets, see *USP Configuration Management* (NN10093-511).
5	Change the path state of the ASP paths to Down. Changing the path state of the ASP paths to down aids in shutting down the application because the Network Elements connected to the USP can take action accordingly. For more information about changing the state of an ASP path, see *USP Configuration Management* (NN10093-511).
6	Perform the following steps on the inactive RTC (slot15). a. If the RTC system node is locked, proceed to step 6b. Otherwise, click **Lock** and proceed to step 6b. b. If the RTC system node is offline, proceed to step 7. Otherwise, click **Offline** and proceed to step 7.
7	Make note of which RTC system node is the active RTC system node. This information is required later in the procedure.
8	Change the alternate boot snapshot. Go to "Performing a backup operation" (page 24).
9	To perform a COR on your system, do the following: a. Unseat the RTC mission card for the inactive RTC system node. Ensure that the LED is off for the SCSI Disk Drive associated with this RTC system node before unseating the mission card.

To unseat the mission card, press outward on the top and bottom latches of the mission card to release it from the Communications Application Module (CAM) shelf.

Grasp the top and bottom latches of the mission card and gently pull it toward you to disconnect it from the associated TM. Do not remove the mission card from the CAM shelf.

Unseating the RTC card stops the write and read access to the SCSI card to avoid SCSI failure.

b. Repeat step 9a for the RTC mission card for the active RTC system node.

c. If there are extension shelves in the system, turn off the A and B power switches on the extension CAM shelves one by one from the maximum shelf number to the minimum shelf number. For example; shelf 4, shelf 3, and then shelf 2.

d. Turn off both the A and B power switches on the rear of the control CAM shelf of your system.

e. Reseat the RTC mission card for an RTC system node. To do this, gently slide the mission card back into place. Apply pressure to the faceplate until you feel resistance.

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

f. Repeat step 9e for the RTC mission card for the other RTC system node.

g. Return power to the shelf. To do this, turn on both the A and B power switches on the rear of the control CAM shelf of your system.

Refer to the note recorded earlier in the procedure to know which RTC system node is active and which one is inactive.

System start up can take several minutes, depending on the configuration of your system.

h. If there are extension shelves in the system, you must turn on both the A and B power switches on the rear of the extension shelves of the system one by one from the minimum shelf number to the maximum shelf number. For example; shelf 2, shelf 3, and then shelf 4.

System start up can take several minutes, depending on the configuration of your system.

10 Wait for the GUI to re-establish a connection after the USP recovers. To view system node status:

a. Click **Configuration>platform>node**.

b. Click the **Graphical View** tab.

c. Confirm that all system nodes are enabled (green status light).

ATTENTION
Nortel recommends that you do not attempt any provisioning changes until all system nodes recover.

If the GUI fails to log in when it is re-establishing the connection, the boot snapshot may not contain the current user's user-account. Provide another valid user-account that is configured in the snapshot have just booted

11 Log into your system.

12 Open the RTC system node administration tab for the RTC system node in slot 12. To do this, click **Configuration>platform>node**. Click the **Graphical view** tab, then select slot 12.

If the table is opened before the GUI reconnects to the RTC, the old data is displayed. After the GUI reconnects to the RTC, reload the table.

13 If the data snapshot descriptions match, proceed to step 20. If the snapshot descriptions do not match, return to step 1 and attempt the procedure again. If the procedure has failed twice in row, contact your next level of support.

For the current active snapshot the snapshot-date and snapshot-version fields are empty.

14 Update the system time settings in the Set Date/Time window, click **Administration> Set Date/Time**.

ATTENTION
This step is not required if simple network time protocol (SNTP) is enabled for this system.

—End—

CAUTION
This procedure can overwrite existing data files on your workstation. Make sure you have a current data backup before you begin this procedure.

Performing a restore operation from a backup tape

Step	Action
	At the Windows-based OAMP workstation
1	Insert the tape containing the data that you want to restore.
2	Double-click the **Backup Exec** icon on the desktop if you are running a Veritas program or the **Colorado Backup II** icon if you are running a Colorado program.
3	Select **Restore files using the Restore Wizard**.
4	Click **OK**.
5	Click **Next**.
6	Select from media in the device.
7	Click **Next**. The system loads the information from the backup tape.
8	Select the backup date and time for the data that you want to restore.
9	Click **OK**. The system loads the information from the backup tape.
10	Click the **+** button on the tree control to expand the tree box next to the C: drive. Select any directories that you want to restore.
11	Click **Next**.
12	Click **Next** a second time.
13	Select **Always replace the file on my computer**.
14	Click **Start**. The system restores the backup data.
15	Click **OK**.
16	The data restore procedure is complete.

—End—

CAUTION
This procedure can overwrite existing USP data files on your workstation. Make sure you have a current data backup before you begin this procedure.

ATTENTION

Before performing this procedure, ensure that the ABS is installed in the workstation.

The root privilege is required to perform this procedure.

Performing a restore operation from a backup CD-RW

Step	Action

At the Solaris-based OAMP workstation

1 Remove the current USP data by entering the following command at the prompt:

rm -Rf <USP data directory>

Example
rm -Rf /opt/usp/ntssgusp/abs/sites

2 Insert the CD-RW containing the USP data that you want to restore into the CD-ROM drive.

3 Go to the partition where the ABS is installed by entering the following:

cd <partition>

Example
cd /

The ABS is installed in the root partition by default.

4 Restore the USP data by entering the following command:

ufsrestore xf /<cdrom directory>/<dumped filename>

Example
ufsrestore xf /cdrom/cdrom0/usp_data_20051115.dmp

The <cdrom directory> is the directory where your CD-ROM is mounted.

The following is displayed; enter what is in bold text when prompted:

You have not read any volumes yet.

Unless you know which volume your file(s) are on you should start with the last volume and work towards the first.

Specify next volume #:**1**

If the data files are large, it can take several minutes to restore the data.

set owner mode for '.'?[yn] **n**

Directories already exist, set modes anyway? [yn] **n**

5 Go to the root directory by entering the following:

Example
cd /

6 Restore the DHCP configuration data by entering the following command:

ufsrestore xf /<cdrom directory>/<dumped filename>

Example
ufsrestore xf /cdrom/cdrom0/dhcp_20051115.dmp

The following is displayed; enter what is in bold text when prompted:

You have not read any volumes yet.

Unless you know which volume your file(s) are on you should start with the last volume and work towards the first.

Specify next volume #:**1**

If the data files are large, it can take several minutes to restore the data.

Set owner mode for ' . '? [yn] **n**

Directories already exist, set modes anyway? [yn] **n**

7 Copy the NFS configuration file back by entering the following:

cp /<cdrom directory>/dfstab /etc/dfs/dfstab

Example
cp /cdrom/**cdrom0**/dfstab /etc/dfs/dfstab

8 Restart the NFS server by entering the following commands:

/etc/init.d/nfs.server stop

/etc/init.d/nfs.server start

9 The data restore procedure is complete. Remove the CD-RW from the CD-ROM drive and return it to its regular storage location.

10 You have completed this procedure.

—End—

Administration: Netping Configuration

The netping table allows you to provision netping entries which enable the Real Time Controller to ping external devices and raise alarms when these devices are not reachable.

Adding a netping entry

Step	Action
	At the OAMP workstation
1	Click **Administration>netping**.
2	Click the **Administration** tab.
3	Click **New**.
4	Enter device name in the **device-name** dialog box.
5	Enter the IP address for the device in the **ip-address** dialog box.
6	Select an alarm severity from the **alarm-severity** box to associate with this device becoming unreachable.
7	Click **Add**.

—End—

ATTENTION
It is not possible to modify a netping entry.

Deleting a netping entry

Step	Action
	At the OAMP workstation
1	Click **Administration>netping**.
2	Click the **Search** tab.
3	Search for the device you want to delete.
4	Double-click on the netping entry you want to delete to transfer the record to the **Administration** panel.
5	Click **Delete**.

—End—

Maintenance: Scheduler

The Z-USP type provides a generic scheduler facility. You can use the scheduler to automatically execute most CLI commands on a preset schedule and/or interval. For a full list of commands that are supported, see the CLI Interface Specification.

You can use the scheduler facility to perform the following tasks:

- Provision the system to run a scheduled CLI command.
- Modify a schedule.
- Delete a scheduled command.
- Provision days using the exempt days feature, on which the system does not run the command, such as holidays or other high-traffic days.
- De-provision exempt days where the system does not run the command.

Adding a scheduler entry

Step	Action
	At the OAMP workstation
1	Open the CLI Command Scheduler window. Click **Administration>Scheduler**.
2	Enter a schedule-id using any decimal value from 0 to 99.
3	In the **cmd-string** portion of the window enter the desired CLI command and click the **Enabled** checkbox if desired. CLI commands can be scheduled but do not run until enabled.
4	Click the calendar icon and select a date for the CLI command to begin from the **Start Date** list.
5	Click the clock and select a starting time for the CLI command in the **Start Time** box. The time must be in the form of a 24-hour clock (hh:mm:ss).
6	Enter the length of the CLI command window, in minutes, in the **Start Window** box.
7	In the Recurrence Pattern portion of the window, select a recurrence option for the CLI command. The recurrence options depend on the

option selected on the left-hand side of the window. The following table describes the information that must be entered for each option.

Option	Information Requirement
None	No information required. The command runs once at the start date and time provisioned.
Daily	Enter the number of days between command. For instance, if you want the test to run every day, enter 1.
Weekly	Enter the number of weeks between commands. As well, in the Day drop box, select a day or days of the week for the command to run.
Monthly	Select one of the following options: • Click Day. Select a day number in the month, and enter the number of months between commands. • Click the radio button beside The, select a sequence from the first list, select a day of the week from the second list, and enter a number of months between commands.

8 To provision exempt days when the command does not run (such as holidays or other high-traffic days), click **Exempt Days**. See "Provisioning exempt days in the command scheduler" (page 45).

9 Click **Add**.

10 If you want the system to run the CLI command immediately, click **Run Now**.

—End—

Modifying a schedule

Step	Action

At the OAMP workstation

1 Open the CLI Command Scheduler window. Click **Administration>Scheduler**.

2 Click **Search**. Locate and highlight the scheduled command that you want to modify in the field CLI Command field at the bottom of the window.

3 Click the calendar icon and select a date for the series to begin from the **Start Date** list.

4 Click the clock and select a starting time in the **Start Time** box. The time must be in the form of a 24-hour clock (hh:mm:ss).

5 Enter the length of the command window, in minutes, in the **Start Window** box.

6 In the **Recurrence Pattern** portion of the window, select a recurrence option for the command. The recurrence options depend on the option selected on the left-hand side of the window. The following table describes the information that must be entered for each option.

Option	Information Requirement
None	No information required. The command runs once at the start date and time provisioned.
Daily	Enter the number of days between commands. For instance, if you want the test to run every day, enter 1.
Weekly	Enter the number of weeks between command. As well, in the Day drop box, select a day or days of the week for the command to run.
Monthly	Select one of the following options: • Click Day. Select a day number in the month, and enter the number of months between command. • Click the radio button beside The, select a sequence from the first list, select a day of the week from the second list, and enter a number of months between command.

7 To provision exempt days when the command does not run (such as holidays or other high-traffic days), click **Exempt Days**. See "Provisioning exempt days in the command scheduler" (page 45).

8 Click **Modify**.

9 If you want the system to run the CLI command immediately, click **Run Now**.

—End—

Deleting a schedule

Step	Action
	At the OAMP workstation
1	Open the CLI Command Scheduler window. Click **Administration>Scheduler**.
2	Click **Search**. Locate and highlight the scheduled command that you want to delete.
3	Click **Delete**.

—End—

Provisioning exempt days in the command scheduler

Step	Action
	At the OAMP workstation
1	Click **Administration>Scheduler-exempt day**.
2	Enter the scheduler id in the **scheduler-id** dialog box.
3	Click the calendar icon and select a date.
4	Click **Add**.

—End—

Deleting exempt days in the command scheduler

Step	Action
	At the OAMP workstation
1	Click **Administration>Scheduler-exempt day**.
2	Enter the scheduler id in the **scheduler-id** dialog box.
3	Click the calendar icon and select a date.
4	Click **Delete**.

—End—

Command status information

The fields in the Command Status portion of the window are automatically updated when the command schedule is enabled. The following table describes the information in each of the fields.

Field	Description
Current Status	This field shows the status of the command, such as scheduled, not scheduled, and About to Start. This information is also displayed at the bottom of the main menu.
Last Response	This field indicates the results of the last command. If the test was rejected, this field lists the rule or rules under which the test was rejected.
Last Start	This field indicates the date and time at which the last command ran.
Next Start	This field indicates the date and time at which the next command will run.
Scheduled By	This field indicates the user identification of the user who scheduled the command, as well as the IP address of the workstation at which the command was scheduled.

Administration: Date and Time

If your user account has administrative privileges, you can set the date and time information for a system. The date and time information includes month-day-year, hour-minute-second, and time zone data. In addition, you can configure the system to automatically adjust the clock settings when daylight savings time begins and ends.

You need to manually reset the date/time information if both of the RTC system nodes should go offline at the same time for any length of time. This usually occurs for one of the following reasons:

- if you perform a restore operation
- if you perform a complete office recovery (COR) on your system
- if your system is booted from an alternate boot snapshot

You can set your USP to use the simple network time protocol (SNTP) to query a network time protocol server. Each time the USP queries the network time protocol server, the USP resets its time accordingly. The SNTP protocol enables the USP to obtain the accurate time of day and keep the same time as other elements in the network.

ATTENTION

If simple network management protocol (SNMP) is not enabled for your system, verify the time settings for your system weekly to ensure that the system time is synchronized with the time on your OAMP workstation.

Setting Date/Time information

Step	Action

At the OAMP workstation

1 Click **Administration>Date/Time** window. The current date and time settings for the system appear.

2 Determine if you want your USP to use SNTP.

If:	Do:
No	Proceed to step 3.
Yes, user defined	Check Enable SNTP Time Sync (User defined) in the SNTP portion of the window. Add an IP address for the SNTP server in the SNTP Server Address field. The information in the Time portion of the window is greyed out. Proceed to step 5.

3 To set the date, click the calendar icon and highlight the day corresponding to today's date.

4 To set the time of day, click the clock icon. Use the spin boxes to set hour, minutes and seconds.

5 To set the local time zone, click the **Time Zone** drop-down menu. A world-wide list of time zones appears. Select the time zone listing that matches the local time zone.

The daylight savings time boxes are unavailable when the time zone you select does not use daylight savings time.

6 To enable or disable the automatic system clock adjustment for daylight savings time, click the **Adjust clock for daylight savings changes** box.

If you are enabling the automatic system clock adjustment for daylight savings time for the first time, make sure you perform step 7 to step 13.

7 Set the starting month for daylight savings time, click **dst-start-month**. Select the month in which daylight savings time starts.

8 Set the starting day in the **dst-start-day** spinbox.

9 Set the starting hour in the **dst-start-hour** spinbox.

10 Set the ending month for daylight savings time, click **dst-end-month**. Select the month in which daylight savings time ends.

11 Set the ending day in the **dst-end-day** spinbox.

12 Set the ending hour in the **dst-end-hour** spinbox.

13 Click **OK**.

—End—

Administration: SNMP

The Simple Network Management Protocol (SNMP) feature enables the USP to deliver alarms to a remote Network Management application. The SNMP feature is pre-configured with default values that might not apply to your system.

Modifying the SNMP configuration

Step	Action
	At the OAMP workstation
1	Click **Administration>snmp**.
2	To change the Network Manager name, enter the new name in the **manager-name** box. The Manager Name can be a maximum of 16 characters, and cannot contain spaces or special characters except an underscore. This name is for reference only. The default system name is "AltBootPC".
3	To change the IP address of the Network Manager, enter the new address in the **manager-ip** box. The default system IP Address is "192.168.1.50". The manager-ip address must match the virtual-ip address of the IEMS. To obtain the virtual-ip address of the IEMS, enter the command **`getpip.ksh iems`** at the IEMS UNIX prompt.
4	To change the number of the UDP port used by the Network Manager for receiving SNMP notifications, edit the **trap-port** box and enter the UDP port number. The default system port number is "162". The trap-port number must match the port number that is configured in **<IEMS Home>/conf/trapport.conf**.
5	To change the SNMP Notification User Name used by the Network Manager application for receiving SNMP notifications, edit the **trap-community-string** box. The User Name can be a maximum of 16 characters, and cannot contain spaces or special characters except an underscore. The default system name is "FIELD".
6	To change the SNMP Get/Set User Name used by the Network Manager Application for sending SNMP Get/Set requests, edit the **get-community-string** box. The User Name can be a maximum of 16 characters, and cannot contain spaces or special characters except an underscore. The default system name is "FIELD".
7	Select the **SNMP** version. Select V3 or v2c.

8 Click **Modify**.

—End—

Log Delivery to IEMS

The introduction of log delivery to the Integrated Element Management System (IEMS) enhances the functionality of Z-USP type by supporting the delivery of security and audit logs to the IEMS syslog server or any other application.

Unformatted Z-USP type log data is sent to the IEMS using syslog. Currently, the Z-USP type only sends alarms through the SNMP interface (integrated into IEMS, Micromuse, and customer OSS) and this functionality remains unchanged in USP11.

The current Z-USP type log format and the data contained in the Z-USP type logs do not change.

Security and audit logs

With log delivery to IEMS, the user has the flexibility of selecting delivery options for security or audit logs, or can choose to deliver both log types to the IEMS server.

Security logs include events related to the security subsystems including user authentication, authorization and administration activities, and other security-related events. Security logs alert security administrations of possible security threats, or improper use or configuration of the security features.

Audit logs include all recorded user-initiated events. These events include login and logout, maintenance, configuration, software management, and other operations-related activities. On the Z-USP type, all of these activities are captured by journaling logs.

The following table lists and describes the logs delivered to the IEMS.

Log title	Description
FTP full access enabled	This log indicates that the FTP server access privileges for a given user have been changed from secure to full access.
FTP full access disabled	This log indicates that the FTP server access privileges for a given user have been changed from full access to secure access.
User login successful	The System Administration subsystem generates this log when a user has successfully logged into a system interface.

Log title	Description
User logout successful	The System Administration subsystem generates this log when a user has successfully logged out of a system interface.
User session timeout	The system generates this log when a user session has been inactive for too long, typically five minutes.
Authentication server response string parse error	This log is generated by the authentication routine used to authenticate users when they log into the system. It is generated when communicating with the Remote Authentication server and the response for the server does not follow the prearranged format.
Max CLI sessions reached	The system generates this log when the maximum number of concurrent CLI sessions has been reached on the specified RTC.
Journal file entry	This log reports any OAM provisioning command execution. This log is used only by Nortel Networks technical support. This log is generated for all provisioning and maintenance actions on the Z-USP type. For this feature, the User Account and User Session provisioning must be provided to the IEMS as a security log, while all other provisioning and maintenance actions are audit logs.
CLI-Debug session logout	The system generates this log when a user logs out of a CLI debug session.
User account provisioned	The system generates this log when a user has successfully provisioned a user account.
User session force-out	The system generates this log when user has been forced out of a session.
Password expired	This log indicates that the user's password is expired and it must be changed before account gets locked.
User account locked	This log indicates that the user has not changed the password within the allowed days of password expiration and has exhausted all the grace period logins. Hence user is locked.

Log delivery provisioning

Users can provision syslog server information using the Z-USP type GUI form. This form includes the following parameters:

- Log delivery enable/disable option

- Primary IP address of the IEMS server
- Optional backup IP address of the IEMS server
- Non-editable transport protocol (for example, UDP/TCP) used to deliver logs
- Non-editable port number (default is 514)
- Log category (for example, security and audit logs) to be delivered

To modify the parameters for log delivery to IEMS, complete the following procedure.

Modifying the Z-USP type GUI for IEMS log delivery

Step	Action
	At the OAMP workstation
1	Open the Z-USP type syslog-delivery window. To do this, click **Administration>syslog-delivery**. The syslog-delivery window opens and displays the default values obtained from the Z-USP type. The values for the transport-protocol and port-number fields are set by default and cannot be modified.
2	To enable IEMS log delivery, ensure that the **log-delivery-option** checkbox is selected. To enable the log-delivery-option checkbox, you must select at least one log option that you want to modify. To disable this option, deselect the **log-delivery-option** checkbox. (The log-delivery-option checkbox is deselected by default.)
3	Enter a primary IP address for the IEMS server in the **primary-ipaddress** field.
4	Enter a optional secondary IP address for the IEMS server in the **secondary-ipaddress** field.
5	To enable the delivery of security logs, select the **security-log-option** checkbox. To disable this option, deselect the **security-log-option** checkbox.
6	To enable the delivery of audit logs, select the **audit-log-option** checkbox. To disable this option, deselect the **audit-log-option** checkbox.
7	Click **Modify** to input your changes.
8	Click **Yes** to confirm your changes.

—End—

Security: Remote Access, Adding a User Account

You must have a user account on the Remote Access Server (RAS) in order to remotely access a system. Your system was configured with one RAS user account during initial installation. This RAS user account is named FIELD and its password is SERVICE.

ATTENTION

Nortel Networks recommends that you modify the password for the FIELD account immediately after installation.

Add user accounts to the Shiva LAN Rover

If your RAS is a Shiva LAN Rover, you can add user accounts to the RAS. You must know the administrative password to access the user database. To add a user account to the RAS, perform the following steps:

Adding user accounts to the RAS

Step	Action
	At the OAMP workstation
1	Double-click the **Shiva Net Manager** icon on your desktop. The Device List window appears.
2	Click the device name for your local RAS.
3	Click the **Security** menu and select **Get User List**. The Enter Administrator Password window appears.
4	Enter the appropriate password in the Administrator Password box.
5	Click **OK**. The User List window appears.
6	Click **Add** to display the Add Users window.
7	Enter your user name in the User box.
8	In the Password portion of the window, enter your password in the Password box.
9	In the Password portion of the window, re-enter your password in the Confirm box.
10	Enable the check boxes in the Permissions portion of the window as appropriate for the access restrictions of the user.
11	Select the appropriate option for the user from the Dial Back list in the Permissions portion of the window.

Dial Back is a security measure for remote access. When it is enabled and you attempt a LAN-to-LAN connection to a remote system, the remote RAS terminates the connection and dials your local RAS back, based on its user list, to open the LAN-to-LAN session.

ATTENTION
Nortel Networks recommends that you select required as the dial back setting to enhance security for your network.

12 If you did not enable dial back on the user account, proceed to step 13. If you did enable dial back on the user account, enter your dial back phone number in the Required box of the Permissions portion of the window.

13 Click **OK** save the addition to the user database and return to the User List window.

—End—

Change the Passwords for the Contivity 100

The Contivity 100 supports two user accounts: administration and login. Use the administration password when you are changing the configuration of the Contivity 100. Use the login password when you want to use the Contivity 100 to connect to the system.

Changing the administration password

Step	Action
	At the OAMP workstation
1	Establish a telnet session to the Contivity 100.
2	Log into the Contivity 100 using your administrator password.
3	To change the administration password, type **`Password`** and press the Enter key.
4	At the prompt, enter the new password and press the Enter key. Enter the password and press the Enter key a second time.

ATTENTION
Note the new password for future reference. If the administration password is lost, you must reset and reconfigure the Contivity 100.

5	To save the changes, type **`commit`** and press the Enter key.

6 End the telnet session to the Contivity 100.

—End—

Changing the login password

Step	Action

At the OAMP workstation

1 Establish a telnet session to the Contivity 100.

2 Log into the Contivity 100 using your administrator password.

3 To change the login password, type

```
ppp dialup1 username <username> password <password>
ppp dialup2 username <username> password <password>
commit
```

and press the Enter key. In this case, the variable **<username>** is the new name for the login identification and the variable **<password>** is the new login password.

4 End the telnet session to the Contivity 100.

—End—

Security: Remote Access

Your system enables OAMP workstations to access remote systems using LAN-to-LAN or dial-up connections.

You can also access your system using a remote Windows or UNIX workstation that is not running the GUI software.

A LAN-to-LAN connection is established using a remote access server (RAS). A dial-up connection is established using the internal modem in your OAMP workstation. You can see a graphical representation of the elements of the system by clicking the icon to the left.

ATTENTION

If your system RAS is a Shiva LAN Rover, Nortel Networks recommends that you use the LAN-to-LAN connection as your primary method of remote access. The dial-up connection should be used only in instances when you cannot establish a LAN-to-LAN connection. Data delivery times are faster for the LAN-to-LAN connection than for the dial-up connection. The Contivity 100 does not support LAN-to-LAN connections.

The system supports four different remote access scenarios. In each scenario, the OAMP workstation is connected concurrently to two systems, which is the maximum number of remote access sessions when the two-port RAS(NTST32AA) is equipped. If you have the eight port RAS(NTST32BA) equipped, you can maintain up to four concurrent sessions (one local and three remote access or four remote access).

In the first scenario, your local OAMP workstation connects to the local system through the Ethernet hubs and connects to a remote system through the RAS.

In the second scenario, an OAMP workstation in a support organization connects to two remote systems through a local RAS. This scenario is used by Nortel Networks and customer technical support organizations.

In the third scenario, an off-site OAMP workstation is used by support personnel to connect to an RAS maintained by the support organization. From that RAS, the support personnel further connects to two remote systems through their RAS. This scenario is used by Nortel Networks and customer technical support organizations.

In the fourth scenario, your local OAMP workstation connects to the local system through the Ethernet hubs and connects by means of the internal modem in your OAMP workstation to a remote system through its RAS.

ATTENTION
Nortel Networks recommends that the fourth scenario be used only when you are unable to establish a LAN-to-LAN connection. Data delivery times are faster for the LAN-to-LAN connection than for the dial-up connection.

LAN-to-LAN or dial-up connection

A LAN-to-LAN or dial-up connection is established between a local RAS and the RAS of a remote system. The following sections describe how to set the administrator password, modify the IP address data for the local RAS, add an RAS user account, add a remote access site, establish a LAN-to-LAN connection to a remote system, and test your LAN-to-LAN connections.

If you are equipped with or use the standard two-port RAS, you can maintain up to two concurrent sessions (one local and one remote access or two remote access). If you use the optional eight-port RAS, you can maintain up to four concurrent sessions (one local and three remote access, or four remote access).

The Contivity 100 does not support LAN-to-LAN connections.

Setting the administrator password

Access to configuration information for the RAS is controlled by an administrator password. The system has a default administrator password of SYSTEM.

ATTENTION
Nortel Networks recommends that you modify your default administrator password immediately after initial installation is completed.

To set the administrator password for the RAS, perform the following steps:

If:	Do:
your RAS is a Shiva LAN Manager	the procedure in "Setting the password on a Shiva LAN Rover" (page 59).
your RAS is a Contivity 100	the procedure in "Setting the password on a Contivity 100" (page 60).

Setting the password on a Shiva LAN Rover

Step	Action
	At the OAMP workstation
1	Double-click the **Shiva Net Manager** icon from your desktop. The Device List window appears.
2	Click the device name for your local RAS.

3 Click the **Security** menu and select **Set Administrator Password**. The Set Administrator Password window appears.

4 Enter the current administrator password in the Current Password box.

5 Click the **New Password** box and enter your new administrator password.

6 Click the **Confirm** box and re-enter your new administrator password.

7 Click **OK** to save the new administrator password.

—End—

Setting the password on a Contivity 100

Step	Action

At the OAMP workstation

1 Establish a telnet connection to the Contivity 100.

2 Log into the unit using the administrator password.

3 Type `Password` and press the Enter key.

4 At the prompt, type your new password and press the Enter key. At the prompt, type your new password a second time and press the Enter key.

5 Type `commit` and press the Enter key to apply the new password.

6 Exit from the telnet session.

—End—

Modifying the IP address data for the Shiva LAN Rover or Contivity 100

When you want to modify the IP address data for the local RAS, you must modify the gateway address settings in the RTC system nodes, your OAMP workstations, and the Shiva LAN Rover application (if applicable). Modify the gateway address settings from the OAMP workstation configured as an alternate boot server.

CAUTION
Changing the IP address information for a piece of equipment can result in that equipment becoming inaccessible. 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, perform the procedures in the General System Provisioning section in the Site-Specific Datafill Guide.

ATTENTION
If your RAS is a Contivity 100, only part of this procedure applies to your system. Perform this procedure, as well as the procedure in "Modifying the gateway address settings" (page 61).

Changing the gateway address requires that you update the Distinct BOOTP server.

Modifying the gateway address settings

Step	Action

At the OAMP workstation

1 Click **Configuration>Platform>Node**.

2 Click the icon for the inactive RTC system node.

3 Enter the new external gateway address in the **Ext-gateway** box.

4 Click **Modify**.

5 You must load the RTC system node to re-initialize the site information. To do this, perform the following steps:

a. Determine if your RTC system node is locked.

If:	Do:
the RTC system node is locked	proceed to step 5b.
the RTC system node is not locked	click **Lock** and proceed to step 5b.

b. In the Maintenance portion of the window, click **Load** to download the RTC system node boot image and re-initialize the RTC system node.

6 Once the initialization of the inactive RTC system node is complete, click **SWACT** to make the inactive RTC system node active.

7 Repeat step 1 to step 6 for the newly inactive RTC system node.

8 Determine if your system RAS is a Shiva LAN Rover or a Contivity 100.

If:	Do:
your system is a Shiva LAN Rover	step 9
your system is a Contivity 100	"Modifying the gateway address settings" (page 61).

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

ATTENTION
This step applies to Shiva LAN Rovers. If your RAS is a Contivity 100, do not perform this step.

a. Double-click the **Shiva LAN Rover** 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.

The new gateway address setting must match the gateway address setting entered in step 3.

f. If the IP addresses for the ports have changed as well, proceed to step 9g. If the IP addresses for the ports have not changed, proceed to step 9m.

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. A confirmation window can display and inform 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.

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.

step 9a to step 9n must be repeated for any other OAMP workstations that use the local RAS. When this is complete, go to step 10.

10 Modify the gateway address settings in your alternate boot server. To do this, perform the following steps:

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

b. Log into the server as the administrator. To do this, click the **Configure** menu, select **Administrator**, and then select **Login**. The Distinct 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. Highlight the contents of the Default Gateway box and enter the new gateway address (should match the setting entered in step 3).

g. Click **Modify** to save the change.

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

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

j. Right-click the **Network Neighborhood** icon on your desktop and select **Properties** from the pop-up window. 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. Select the **Gateway** tab window.

n. Select the contents of the Installed gateway box and click **Remove** to delete the old gateway address.

o. Enter the new external gateway address (should match the setting entered in step 3) in the New gateway box and click **Add**. The new gateway address is added to the list of installed gateways.

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

q. Click **OK** to close the Network window. You will be prompted to choose whether you want to restart your computer to have the new settings take effect.

r. Click **Yes** to restart your alternate boot server.

step 10j to step 10r must be repeated for each OAMP workstation configured for your system.

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

12 Log into your system. To do this, perform the following steps:

a. Click **File>Session login**.

b. Select a site from the **Site** drop-down menu.

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

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

e. Click **Login**.

13 Load the RTC system nodes to activate the new settings. To do this, perform the following steps:

a. Click **Configuration>Platform>Node**.

b. Verify the administrative state of the RTC system node. If the RTC system node is locked, proceed to step 13c. If the RTC system node is not locked, click **Lock** and proceed to step 13c.

c. Click **Load** to reload the RTC system node.

d. Click **Unlock**.

e. Open the RTC system node administration tab for the active RTC system node. To do this, Click **Configuration>Platform>Node**. and click the icon for the active RTC system node.

f. Repeat step 13b to step 13d. This causes the inactive RTC system node to become active, and the formerly active RTC system node is reloaded.

g. Perform a swtich activity (SWACT).

14 Perform a backup operation. To do this, follow the procedure in "Performing a backup operation" (page 24).

15 Log into your system. To do this, perform the following steps:

a. Select your system site from the **Site** list.

b. Enter your user account name in the **User ID**box.

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

d. Click **Login**.

16 Nortel Networks recommends that you delete any data snapshots from your system that were created before you modified the gateway address, to prevent the possibility of restoring your system using one of these older data snapshots. If you restored your system using an old data snapshots, you could affect communication with your local RAS.

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 you changed the gateway address from the Snapshot box in the Source portion of the window.

19 Click **Delete** to delete the data snapshot. An hourglass appears while the snapshot is being deleted. When the deletion operation is complete, the boxes in the Source portion update. This removes that data snapshot from your alternate boot server.

20 Repeat for each data snapshot that was created before you changed the gateway address.

21 Select a data snapshot that was created before you changed the RTC system node(s) from the Snapshot box in the Destination portion of the window.

22 Click **Delete** to delete the data snapshot. An hourglass appears while the snapshot is being deleted. When the snapshot is deleted, the boxes in the Destination portion update. This removes that data snapshot from the active RTC system node.

23 Repeat for each data snapshot that was created before you changed the gateway address.

24 In the Destination list, select the inactive RTC system node.

25 Select a data snapshot that was created before you changed the gateway address from the Snapshot box in the Destination portion of the window.

26 Click **Delete** to delete the data snapshot. An hourglass appears while the snapshot is being deleted. When the snapshot is deleted, the boxes in the Destination portion update. This removes that data snapshot from the inactive RTC system node.

27 Repeat for each data snapshot that was created before you changed the gateway address.

—End—

Modifying the IP address for the Contivity 100

If your system RAS is a Contivity 100, you must perform the procedure in this section.

ATTENTION

If your system RAS is a Shiva Net Manager, this procedure does not apply.

If your system RAS is a Contivity 100, you must also perform the previous procedure "Modifying the IP address data for the Shiva LAN Rover or Contivity 100" (page 60). When the procedure directs you to do so, move to this procedure, then return to the procedure that sent you to this procedure.

CAUTION

When changing the IP address of the Contivity 100, make sure that you do not change the IP addresses of the dialup1 and dialup2 interfaces. A change to the dialup interfaces prevents remote access to the system.

Modifying the IP address

Step	Action

At the OAMP workstation

1 Establish a telnet connection to the Contivity 100.

2 Log into the system using your administrator user identification and password.

3 To change the IP address of the Contivity 100, type **ifconfig eth1 ipaddress <ipaddress> <subnetmask> commit**.

and press the Enter key. In this case, the variable **<ipaddress>** is the new IP address for the RAS and **<subnetmask>** is the name of the new subnet mask.

4 Exit the telnet session to the Contivity 100.

5 Return to step 10 in the procedure that directed you to this procedure.

—End—

Addition of a remote access site

You must know the administrative password to add a remote access site to the Shiva Net Manager software. To add a remote access site to the Shiva Net Manager, perform the following steps:

ATTENTION
This section does not apply to Contivity 100.

Adding a remote access site

Step	Action
	At the OAMP workstation
1	Double-click the **Shiva Net Manager** icon on your desktop. The Device List window appears.
2	Double-click the device name for your local RAS. The Enter Administrator Password window appears.
3	Enter the appropriate password in the Administrator Password box.
4	Click **OK**. The Configuration window appears.
5	In the Configure list, select **LAN-to-LAN Sites**. The window changes to display the list of remote access sites configured for your local RAS.
6	Click **Add** and the LAN-to-LAN Sites window appears.
7	In the Display box, select **Features** and perform the following steps:

a. Double-click or select the default value in the Site name box and insert the name of the site to which you want to have remote access.

b. In the Protocols portion of the window, ensure that the IP and IPX check boxes are selected.

c. In the Remote User/Password portion of the window, enter the name and password of the user who is set up at the remote RAS for LAN-to-LAN connections. This is the user name used any time that a LAN-to-LAN session is initiated from your local RAS to this remote site.

d. In the Connection Time portion of the window, select a radio button based on the connection time limitations you want to place on the user account.

8 In the Display box, select **Phone Numbers** and the window changes, displaying a list of the ports and their associated remote phone numbers that are assigned to this LAN-to-LAN connection. Perform the following steps:

a. In the Local port name list, select the desired local port name.

b. Enter the phone number of the remote RAS in the Remote phone number box.

c. Click **Add** to add the local port name and related remote phone number to the list.

d. If you want to add additional phone numbers for access to the remote RAS, repeat the above steps.

9 Click **OK** to return to the Configuration window.

10 Click the **Actions** menu and select **Set Configuration** to save your changes.

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

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

—End—

LAN-to-LAN connections

Use this procedure to establish a LAN-to-LAN connection if the OAMP workstation is running Windows 2000. This procedure requires that both a RAS site and RAS user account have been defined.

ATTENTION

This section does not apply to Contivity 100.

Establishing a LAN-to-LAN connection manually

Step	Action

At the OAMP workstation

1 Telnet into the Shiva from the Windows 2000 workstation:

a. Open the Run window by clicking on the Windows **Start** button, and selecting Run...

b. Type the command **`telnet <RAS_IP>`** where <RAS_IP> is the IP address of a defined remote access site.

2 Log in to the Shiva:

a. Enter the user name for a defined user account at the "Userid" prompt.

b. Enter the password for the defined user account at the "Password" prompt.

3 Issue the command **`lan connect <site_name>`**, where **`<site_name>`** is the name of the defined LAN-to-LAN connect site.

4 To terminate the manual LAN-to-LAN connection, issue the command **`lan disconnect <site_name>`** where **`<site_name>`** is the name of the defined Lan-to-Lan connect site.

—End—

Modify RAS configuration information

If you know the administrative password, you can modify other aspects of the configuration information for the RAS. Refer to the online documentation for the Shiva LAN Rover for more information on modifying specific elements of the configuration for the RAS.

ATTENTION

This section does not apply to Contivity 100

Test your LAN-to-LAN connections

You should test your LAN-to-LAN connections monthly by dialing into the remote site(s). To test the LAN-to-LAN connection(s), perform the following steps:

ATTENTION

This section does not apply to Contivity 100.

Testing your connections

Step	Action
	At the OAMP workstation
1	Double-click the **Shiva LanConnect** icon on your desktop. The Shiva LanConnect window appears.
2	Click the **File** menu and select **Open**. The Open LAN-to-LAN Document window appears.
3	Select the LAN-to-LAN document from the list that defines the connection to the remote system you want to access.
4	Click **OK** to return to the Shiva LanConnect window. The boxes update with the settings for your LAN-to-LAN connection as defined in the document.

—End—

Security: Remote Access Dial-up Connection

The OAMP workstation comes equipped with an internal modem configured to enable you to remotely access a system in your network or dial into your local system when an Ethernet problem disrupts communication between your OAMP workstation and the control CAM shelf. The following sections describe the steps necessary to configure a dial-up connection, establish a dial-up connection with a remote or local system, and test your dial-up connection.

If:	Do:
your RAS is a Shiva LAN Rover	the procedures in "Configuring a Shiva LAN Rover for dial-up connection" (page 71).
your RAS is a Contivity 100	the procedures in "Configure Contivity 100 for a remote connection" (page 81).

ATTENTION

Nortel Networks recommends that you use the dial-up connection only in instances when you cannot establish a LAN-to-LAN connection. Data delivery times are faster for the LAN-to-LAN connection than for the dial-up connection. This is only an option if your system RAS is a Shiva LAN Rover; the Contivity 100 does not support LAN-to-LAN connections.

Configuring a Shiva LAN Rover for dial-up connection

Step	Action

At the OAMP workstation

1 Double-click the **Dial-In Networking** icon on the desktop of your OAMP workstation. The Dial-In Networking window appears.

2 Double-click the **Make New Connection** icon to start the New Connection wizard. The New Connection Wizard window appears.

3 Enter a name for this dial-up connection in the New connection name box. The name can contain any information that you find relevant.

4 Click **Next** to open the Select Modem/Device window.

5 If this is the first time you are configuring a dial-up connection for your system, go to the drop-down list box near the top of the window and select the modem equipped in your OAMP workstation. If this is not the first time you are configuring a dial-up connection for

your system, ensure that the radio button for your default device is selected.

6 If the phone number to access the remote system is in your area code, ensure that the Use area code and country code box is disabled and proceed to step 7.

If the phone number to access the remote system is outside of your area code, ensure that the Use area code and country code box is enabled and proceed to step 8.

7 Enter the phone number for the remote system in the Phone number box and proceed to step 9.

8 Enter the area code and phone number for the remote system in the Area code and Phone number boxes.

9 Select the country in which the remote system is located from the Country code list.

10 Click **Next** to open the Congratulations window. The configuration information for your dial-up connection is listed.

11 If the configuration information is correct, proceed to step 12. If the configuration information is not correct, click Back to return to the previous window(s), correct the information in the appropriate boxes, and click Next to return to the Congratulations window.

12 Click **Finish** to save the dial-up connection configuration information. The Dial-In Networking window appears with a new icon labeled with the name you entered in step 3.

13 Right-click the new icon. A pop-up window appears.

14 Select **Properties**. The Shiva Remote 5.0 - site_name window appears.

15 Click **Dialing Properties**. The Dialing Properties window appears, listing the properties for the default location.

16 If the location you are dialing from is the default location, proceed to step 26. If the location you are dialing from is not the default location, proceed to step 17.

17 Open the **I am dialing from** list. If the location you are dialing from is in the list, select your location and proceed to step 26. If the location you are dialing from is not in the list, close the drop-down list and click New to display the Create New Location window.

18 Enter the name of the new location in the Create a new location named box and click **OK** to return to the Dialing Properties window.

19 Enter the area code that you are dialing from in the**The area code is** box.

20 Select the country from which you are dialing from the**I am in**box.

21 If you do not need to dial a number to access an outside line, proceed to step 22. If you must dial a number to access an outside line from your location, enter the access number for local phone numbers and the access number for long distance phone numbers in the How I dial from this location portion of the window.

22 If you want to use a calling card to dial, refer to the online documentation for the Shiva Remote application for more information on setting up calling card dialing.

23 If the location you are dialing from does not have call waiting, ensure that the call waiting box is disabled.

24 If the location you are dialing from has call waiting, ensure that the call waiting box is enabled and select the appropriate call waiting disabling digits from the list.

25 Click either **Tone dialing** or **Pulse dialing**, appropriate to the type of dialing used by the phone system of the location from which you are dialing.

26 Click **OK** to return to the Shiva Remote 5.0 - site_name window.

27 Select the Protocols tab window.

28 Click **Settings** to open the Advanced TCP/IP Settings window.

29 Click **Advanced** to display the advanced TCP/IP settings.

30 Ensure that the Add default route box is disabled.

31 Click **OK** to close the Advanced TCP/IP Settings window.

32 Click the **File** menu and select **Exit** to close the Shiva Remote 5.0 - site_name window.

—End—

ATTENTION

The next procedure, Establishing a Dial-Up Connection to a Remote System, does not apply to the Contivity 100.

Establishing a dial-up connection to a remote system

Step	Action

At the OAMP workstation

1 Double-click the **Dial-In Networking** icon on your desktop. The Dial-In Networking window appears.

2 If you already have a dial-up connection configuration defined for the remote system, proceed to step 3. If you do not have a dial-up connection configuration defined for the remote system, perform the following steps:

a. Double-click the **Make New Connection** icon to start the New Connection wizard. The New Connection Wizard window appears.

b. Enter a name for this dial-up connection in the New connection name box. The name can contain any information that you find relevant.

c. Click **Next** to open the Select Modem/Device window.

d. If this is the first time you are configuring a dial-up connection for your system, select the modem equipped in your OAMP workstation in the drop-down list box near the top of the window. If this is not the first time you are configuring a dial-up connection for your system, ensure that the radio button for your default device is selected.

e. If the phone number to access the remote system is in your area code, ensure that the Use area code and country code box is disabled and enter the phone number for the remote system in the Phone number box.

f. If the phone number to access the remote system is outside of your area code, ensure that the Use area code and country code box is enabled, enter the area code and phone number for the system in the Area code and Phone number boxes, and select the country in which the system is located from the Country code list.

g. Click **Next** to open the Congratulations window. The configuration information for your dial-up connection is listed.

h. If the configuration information is correct, proceed to next task. If the configuration information is not correct, click Back to return to the previous window(s), correct the information in the appropriate boxes, and click **Next** to return to the Congratulations window.

i. Click **Finish** to save the dial-up connection configuration information. The Dial-In Networking window appears, with a new icon labeled with the name you entered earlier.

j. Right-click the icon for the dial-up connection for the remote system and select **Properties** from the pop-up menu. The Shiva Remote 5.0 - site_name window appears.

k. Click **Settings** to open the Advanced TCP/IP Settings window.

l. Ensure that the Add default route box is disabled

m. Click **OK** to close the Advanced TCP/IP Settings window.

n. Click the **File** menu and select **Exit** to close the Shiva Remote 5.0 - site_name window.

3 Double-click the icon for the dial-up connection configuration for the remote system. The Shiva Remote Connect To window appears.

4 Enter the name of your user account for the remote RAS in the User name box.

5 Enter the password for your remote RAS user account in the Password box.

6 Ensure that the Save password box is disabled.

7 Click **Connect**. The configuration_name window appears, informing you of the status of the dial-up connection.

When the dial-up connection is complete, the window indicates that you are connected, and displays the rate of the connection, and the duration of the connection.

8 If you want to start up the GUI, proceed to step 12. If you want to modify the configuration of the remote RAS, proceed to step 9.

9 Double-click the **Shiva LAN Rover** icon on your desktop. The Device List window appears. The device name of the remote RAS should appear on the list.

10 Click the remote RAS in the list. You can now modify the configuration of this RAS, if you know the administration password. Refer to the online documentation for the Shiva Net Manager for more information on modifying specific elements of the RAS configuration.

11 When you have completed your modifications to the configuration of the remote RAS, proceed to step 12 if you want to start the system software or proceed to step 16 if you want to terminate your remote access session.

12 Double-click the **BroadBand STP** icon on your desktop to start the GUI. The Login window appears.

13 If you have added the site configuration information in the GUI for the remote system, proceed to step 14.

If you have not added the site configuration information for the remote system, perform the following steps:

a. Click Configure to open the Site Configuration window.

b. Click New to add a new site.

c. Enter the site name of the remote system in the Site Name box.

d. Enter the IP address of the RTC system node in slot 12 of the control CAM shelf of the remote system in the RTC 1 IP Address box.

e. Enter the IP address of the RTC system node in slot 15 of the control CAM shelf of the remote system in the RTC 2 IP Address box.

f. Click OK to return to the Site Configuration window.

g. Click Close to return to the Login window.

14 Connect to the remote system. To do this, select the name of the remote system from the Site Name list, enter your user account name in the User ID box, enter your user account password in the Password box, and click **Connect**. The main menu appears.

15 When you are finished with your remote system session, exit the system session. Proceed to step 16 if you want to terminate the remote access session, or step 9 if you want to modify the configuration of the remote RAS.

16 Return to the configuration_name window. Terminate the connection to the remote system by clicking **Disconnect**.

—End—

Establish a dial-up connection to your local system

When a problem with the Ethernet between your OAMP workstation and the control CAM shelf disrupts communication, you can dial into the control CAM shelf from the internal modem in your OAMP workstation. A dial-up connection should be established to your local system only in the instance describe above.

ATTENTION
This procedure does not apply to the Contivity 100.

Establishing a dial-up connection

Step	Action
	OAMP workstation
1	Disable the Ethernet card in your OAMP workstation. To do this, perform the following steps:
	a. Right-click the **My Computer** icon on your desktop. A pop-up menu appears.
	b. Select **Properties**. The System Properties window appears.
	c. In the Device Manager tab window, click the **Network adapters** icon. A list of the network adapters in your OAMP workstation appears.
	d. Double-click the icon for the Ethernet card. The network_adapter window appears.
	e. From the General tab window, disable the box for the Ethernet card in the Device usage portion of the window. An hourglass appears while the Ethernet card is being disabled. The network_adapter window closes and a red X appears over the icon for the Ethernet card in the System Properties window.
	f. Click **Close** to exit the window.
2	Double-click the **Dial-In Networking** icon on your desktop. The Dial-In Networking window appears.
3	If you already have a dial-up connection configuration defined for the local system, proceed to step 4. If you do not have a dial-up connection configuration defined for the local system, perform the following steps:
	a. Double-click the **Make New Connection** icon to start the New Connection wizard. The New Connection Wizard window appears.
	b. Enter a name for this dial-up connection in the New connection name box. The name can contain any information that you find relevant.
	c. Click **Next** to open the Select Modem/Device window.
	d. If this is the first time you are configuring a dial-up connection for your system, select the modem equipped in your OAMP workstation in the drop-down list box near the top of the window.

If this is not the first time you are configuring a dial-up connection for your system, ensure that the radio button for your default device is selected.

e. Ensure that the Use area code and country code box is disabled

f. Enter the phone number for the local system in the Phone number box.

g. Click **Next** to open the Congratulations window. The configuration information for your dial-up connection is listed.

h. If the configuration information is correct, proceed to the next step. If the configuration information is not correct, click **Back** to return to the previous window(s), correct the information in the appropriate boxes, and click **Next** to return to the Congratulations window.

i. Click **Finish** to save the dial-up connection configuration information. The Dial-In Networking window appears, and contains a new icon labeled with the name you entered earlier.

4 Double-click the icon for the dial-up connection configuration for the local system. The Shiva Remote Connect To window appears.

5 Enter the name of your user account for the local RAS in the User name box.

6 Enter the password for your local RAS user account in the Password box.

7 Ensure that the Save password box is disabled.

8 Click **Connect**. The configuration_name window appears, informing you of the status of the dial-up connection.

When the dial-up connection is complete, the window indicates that you are connected, and displays the rate of the connection, and the duration of the connection.

9 If you want to start up the GUI, proceed to step 13. If you want to modify the configuration of the local RAS, proceed to step 10.

10 Double-click the **Shiva Net Manager** icon on your desktop. The Device List window appears. The device name of the local RAS should appear on the list.

11 Click the local RAS in the list. You can now modify the configuration of this RAS, if you know the administration password. Refer to the online documentation for the Shiva Net Manager for more information on modifying specific elements of the RAS configuration.

12 When you have completed your modifications to the configuration of the local RAS, proceed to step 13 if you want to start the GUI or proceeds to step 16 if you want to terminate your session.

13 Double-click the **Universal Signaling Point** icon on your desktop to start the GUI. The Login window appears.

14 Connect to the local system. To do this, select the name of the local system from the Site Name list, enter your user account name in the User ID box, enter your user account password in the Password box, and click **Connect**. The main menu appears.

15 When you are finished with your local system session, exit the GUI and proceed to step 16 if you want to terminate the session, or proceeds to step 10 if you want to modify the configuration of the local RAS.

16 Return to the configuration_name window. Terminate the connection to the local system by clicking **Disconnect**.

17 Enable the Ethernet card in your OAMP workstation. To do this, perform the following steps:

a. Right-click the **My Computer** icon on your desktop. A pop-up menu appears.

b. Select **Properties**. The System Properties window appears.

c. In the Device Manager tab window, click the Network adapters icon. A list of the network adapters in your OAMP workstation appears.

d. Double-click the icon for the Ethernet card. The network_adapter window appears.

e. From the General tab window, enable the box for the Ethernet card in the Device usage portion of the window.

f. An hourglass appears while the Ethernet card is being enabled. The network_adapter window closes and a red X appears from the icon for the Ethernet card in the System Properties window.

g. Click **Close** to exit the window.

—End—

Test your dial-up connection to a remote system

You should test your dial-up connections to remote systems monthly by dialing into the remote site(s). To check the dial-up connections with the remote systems, perform the following steps:

ATTENTION
This procedure does not apply to the Contivity 100.

Testing your dial-up connection

Step	Action
	At the OAMP workstation
1	Double-click the **Dial-In Networking** icon on your desktop. The Dial-In Networking window appears.
2	Double-click the icon for the dial-up connection configuration for the remote system.
3	The Shiva Remote Connect To window appears.
4	Enter the name of your user account for the RAS in the User name box.
5	Enter the password for your RAS user account in the Password box.
6	Ensure that the Save password box is disabled.
7	Click **Connect**. The configuration_name window appears, informing you of the status of the dial-up connection. When the dial-up connection is complete, the window indicates that you are connected, the baud rate of the connection, and the duration of the connection.
8	Double-click the **Shiva Net Manager** icon on your desktop. The Device List window appears.
9	Double-click the name of the RAS associated with this remote system. If the Configuration window for this RAS appears, your dial-up connection is functioning correctly.
10	Return to the configuration_name window. Terminate the connection to the remote system by clicking Disconnect.
11	Repeat step 1 to step 10 for any additional dial-up connections that you have configured.

—End—

Configure Contivity 100 for a remote connection

Before connecting to the Contivity 100 it is important that you disable any network cards installed on your PC because they can interfere with the connection to the Contivity 100.

If:	Do:
your workstation is a Windows 2000 machine	"Disabling network cards in Windows 2000" (page 81).

Disabling network cards in Windows 2000

Step	Action

At the OAMP workstation

1 From thew Windows system tray, select **Start>Settings>Control Panel>System**.

2 Select the **Hardware** tab.

3 Click on the **Device Manager** button.

4 Click on the **+** next to the **Network Adapters** line.

5 Double-click on your network card.

6 Select **Do not use this device (disable)** from the combo box at the bottom of the window.

7 Click **OK**.

ATTENTION

To re-enable the network card when you are complete, repeat the following steps, except during step 6 select **Use this device (enable)**.

—End—

Configuring the dial-up connection

If your system RAS is a Contivity 100, select the workstation type, and perform the appropriate procedure.

If:	Do:
your workstation is a Windows 2000 machine	"Configuring a Windows 2000 workstation to connect to Contivity 100" (page 82).

Configuring a Windows 2000 workstation to connect to Contivity 100

Step	Action

At the OAMP workstation

1 Select **Start > Settings > Network and Dial-up Connections >Make a New Connection**.

2 Click **Next**.

3 Select the **Dial-up to a Private Network** radio button.

4 Click **Next**.

5 Enter the telephone number for the line connected to the Contivity 100.

6 Select the **For All Users** radio button.

7 Click **Next**.

8 Enter a name for the connection.

9 Click **Finish**.

10 Right-click on the newly added connection.

11 Select **Properties**.

12 Select the Networking tab.

13 Select Internet Protocol (TCP/IP). The properties button becomes active.

14 Select **Properties**.

15 Select the **Use the following IP address** radio button.

16 Determine if you are setting up a connection for the first or second line on the Contivity 100.

If:	Do:
you are entering information for line 1	enter 192.168.0.3.
you are entering information for line 2	enter 192.168.0.4.

17 Click **OK**.

18 Click **OK** a second time to save the changes and exit the window.

19 Repeat step 1 to step 18 to create a connection for the second line.

—End—

Clear connectivity lost alarm

After modifying the Contivity 100 RAS, customers can experience the following alarm:

```
Connectivity lost:  Remote_Access_Server xxx.xxx.xxx.xxx
```

(where xxx.xxx.xxx.xxx is the IP address of the Contivity 100). To clear this alarm, refer to the CLI Specification document.

Maintenance: Provisioning a REx Test

Although many CLI commands can be scheduled, special treatment is required for automated regular exercise (REx) testing since it carries with it a significant set of rules and guidelines.

A REx enables a user to test and verify the stability of the RTC system nodes through regularly scheduled tests of the system node. The REx runs diagnostic procedures, such as querying the RTC database and monitoring the serial port and counter/timer.

You can provision and schedule a REx test from the GUI. A popup screen displays a warning that the REx test will run five minutes before the REx test begins.

The following restrictions apply to your system during the execution of the REx test:

- You cannot run a REx test during a software upgrade.
- You cannot perform a manual SWACT during a REx test.
- Nortel Networks recommends that you do not perform any provisioning or maintenance activities while a REx test is in progress.

Nortel Networks recommends scheduling a weekly full-cycle REx during the least busy off-peak period during the week.

The system also checks a set of rules to ensure system stability during the REx test. If any of the following events occur, the system stops the REx cycle.

- The REx test was aborted through a user request.
- Mated nodes are locked or inactive.
- The system shows a critical alarm.
- An unexpected RTC state occurred.
- The alternate boot audit failed.
- A CLI bulk input is in progress.

REx CLI syntax

The syntax for REx CLI commands is shown as follows:

platform node rex start *shelf slot* {**full-cycle** | **half-cycle**} *final-swact-option*

Where:

- *shelf* - shelf number, integer from 0 to 7 (central shelf has number 0)
- *slot* - slot number, integer from 1 to 18

- **full-cycle** - exercising both RTC cards, first inactive, then swact, then one that became inactive
- **half-cycle** - exercising inactive RTC card only
- *final-swact-option* - **y**[es] or **n**[o] character to perform a SWACT at the end of the REx cycle

Using the REx CLI syntax, you can perform the following maintenance tasks:

- Provision the system to run the REx schedule
- Modify a REx schedule
- Delete a REx schedule
- Provision days, using the exempt days feature, on which the system does not run the REx test, such as holidays or other high-traffic days.
- De-provision exempt days where the system does not run the REx test.

Provisioning the system to run the REx schedule

Step	Action
	At the OAMP workstation
1	Open the CLI Command Scheduler window. Click **Administration>Scheduler**.
2	Enter a schedule-id using any decimal value from 0 to 99.
3	In the **CLI Command Details** portion of the window enter the desired REx command and click the **Enabled** checkbox. See "REx CLI syntax" (page 84) for more information.
4	Click the calendar icon and select a date for the series of REx tests to begin from the **Start Date** list.
5	Click the clock and select a starting time for the REx test in the **Start Time** box. The time must be in the form of a 24-hour clock, hh:mm:ss.
6	Enter a value in the **Start Window** box. This value indicates how long after the provisioned start-time the REX process can begin if the scheduler is delayed.
7	In the **Recurrence Pattern** portion of the window, select a recurrence option for the REx test. The recurrence options depend on the option

selected on the left-hand side of the window. The following table describes the information that must be entered for each option.

Option	Information Requirement
None	No information required. The REx test runs once at the start date and time provisioned.
Daily	Enter the number of days between REx tests. For instance, if you want the test to run every day, enter 1.
Weekly	Enter the number of weeks between rex tests and the day of the week that the rex test should run.
Monthly	Select one of the following options: • Click Day. Select a day number in the month, and enter the number of months between REx tests. • Click the radio button beside The, select a sequence from the first list, select a day of the week from the second list, and enter a number of months between REx tests.

8 Click **Add**.

9 To provision exempt days when the REx test does not run (such as holidays or other high-traffic days), click **Exempt Days**. See the "Provisioning exempt days in the REx schedule" (page 88) for information.

10 If you want the system to run a REx test immediately, click **Run Now**.

—End—

Modifying a REx schedule

Step	Action

At the OAMP workstation

1 Open the CLI Command Scheduler window. Click **Administration>Scheduler**.

2 Click **Search**. Locate and highlight the scheduled test that you want to modify in the field CLI Command field at the bottom of the window.

3 Click the calendar icon and select a date for the series of REx tests to begin from the **Start Date** list.

4 Click the clock and select a starting time for the REx test in the **Start Time** box. The time must be in the form of a 24-hour clock, hh:mm:ss.

5 Enter the length of the REx window, in minutes, in the **Start Window** box.

6 In the **Recurrence Pattern** portion of the window, select a recurrence option for the REx test. The recurrence options depend on the option selected on the left-hand side of the window. The following table describes the information that must be entered for each option.

Option	Information Requirement
None	No information required. The REx test runs once at the start date and time provisioned.
Daily	Enter the number of days between REx tests. For instance, if you want the test to run every day, enter 1.
Weekly	Enter the number of weeks between rex tests and the day of the week that the rex test should run.
Monthly	Select one of the following options: • Click Day. Select a day number in the month, and enter the number of months between REx tests. • Click the radio button beside The, select a sequence from the first list, select a day of the week from the second list, and enter a number of months between REx tests.

7 Click **Modify**.

8 To provision exempt days when the REx test does not run (such as holidays or other high-traffic days), click **Exempt Days**. See the "Provisioning exempt days in the REx schedule" (page 88) for information.

9 If you want the system to run a REx test immediately, click **Run Now**.

—End—

Deleting a REx schedule

Step	Action

At the OAMP workstation

1 Open the CLI Command Scheduler window. Click **Administration>Scheduler**.

2 **Click Search**. Locate and highlight the scheduled test that you want to delete.

3 Click **Delete**.

—End—

Provisioning exempt days in the REx schedule

Step	Action
	At the OAMP workstation
1	Click **Administration>Scheduler-exempt day**.
2	Enter the scheduler name in the **Scheduler-id** dialog box.
3	Click the calendar icon and select a date.
4	Click **Add**.

—End—

De-provisioning exempt days in the REx schedule

Step	Action
	At the OAMP workstation
1	Click **Administration>Scheduler-exempt day**.
2	Click **Search**.
3	Locate and highlight the exempt day that you want to delete.
4	Click **Delete**.

—End—

Command status information

The fields in the Command Status portion of the window are automatically updated when the REx schedule is enabled. The following table describes the information in each of the fields.

Field	Description
Current Status	This field shows the status of the REx test, such as scheduled, not scheduled, and About to Start. This information is also displayed at the bottom of the main menu.
Last Response	This field indicates the results of the last REx test. If the test was rejected, this field lists the rule or rules under which the test was rejected.
Last Start	This field indicates the date and time at which the last REx test ran.
Next Start	This field indicates the date and time at which the next REx test will run.
Scheduled By	This field indicates the user identification of the user who scheduled the REx test, as well as the IP address of the workstation at which the test was scheduled.

Administration: Bulk Input/Output

ATTENTION

Given the potential for merging of Global title translation (GTT) entries, it is possible that the number of GTT entries in the USP post Bulk Input does not match the number of entries in the bulk input file.

There are two types of databases that can be bulk input/output: system databases and service databases. Bulk input/output operations provide an expedient method for getting large amounts of data into the system.

System database

The system database bulk input enables the user to do bulk provisioning or bulk maintenance on the system. This capability provides a fast and efficient way to perform large system provisioning or to conduct repetitive maintenance procedures. Any CLI command that can be manually entered can be included in a bulk input file with the following exceptions:

- Only one bulk input command can be running at any given time in the system.
- To minimize command execution time, it is recommended that the bulk input command be executed on the active RTC. The **`platform node show 0 {12|15}`** command can be used to determine which RTC is active (or Click **Configuration>platform>node** on the GUI). See the table definitions section of this document for more detail on the execution of this command.
- The bulk-input process runs on the RTC that the CLI session is using. Any commands that affect the state of this RTC can cause the bulk-input process to terminate. Two such commands are the **`platform node offline`** command and the **`platform node load`** command. If a bulk-input file is executed that contains these commands for the RTC that the CLI session is using, the session and the bulk input process is terminated as soon as one of these commands is executed.
- The nesting of a bulk-input command within a bulk-input file is not supported.

Performing a bulk input of a system database

Step	Action
	At the OAMP workstation
1	Click **Administration>Bulk-input-system-db**.
2	Enter the name and full path of your bulk input file in the **bulk-file-name** field of up to 128 alphanumeric characters.

3 Enter the remote IP address of the LSMS, NSM, or HLR Provisioning System in the **remote-server-ip-address** field.

4 Enter the user ID in the **remote-userid** field. The remote site system administrator provides this information.

5 Enter the password in the **remote-password** field. The remote site system administrator provides this information.

6 Select the **stop-on-error-option** checkbox if you require that bulk input ceases on the first error encountered. This can be desirable if successive commands depend on earlier commands.

7 Select the **syntax-only-option** checkbox if you want to validate that your bulk load script is syntactically correct. The option runs through the commands and checks to see that the syntax is valid but does not call "semantic (database rules)" or "apply" (that is, it does not execute them).

8 Click **Execute**.

The Bulk Input Status section of the screen can be monitored for bulk progress. The following table describes the fields and their meanings:

Field	Description
start-time	The time that the bulk input was started
session-index	An internal index used to track bulk entry
shelf	Shelf in which the bulk input target resides
slot	Slot in which the bulk input target resides
executed-by	User name of the account initiating the bulk input
executed-from	IP address of the machine initiating the bulk input
commands-executed	Displays a running total of the number of commands that have successfully executed during the bulk input operation
commands-failed	Displays a running total of the number of commands that have failed during the bulk input operation

The system database bulk output enables the user to extract the contents of any provisioning screen on the system and FTP it to an external system. This capability enables the user to extract data for the purposes of transferring it to another system, backups or analysis. Several formats are supported for the bulk output including comma separated format (for spreadsheets), multiline ascii (for human readability), html (for publishing on web pages) or bulk input format (for transfer to other systems or backups).

—End—

Performing a bulk output of a system database

Step	Action
	At the OAMP workstation
1	Click **Administration>bulk-output>bulk-output-system-db**.
2	Enter the full path name of the destination for your bulk output file in the path field of up to 128 alphanumeric characters.

ATTENTION
Contact personnel at the receiving site to ensure that the target directory specified is acceptable and available.

3	Enter a unique tag to be placed as a prefix on the exported files in the file-prefix field of up to 32 alphanumeric characters.
4	Enter the remote IP address of the LSMS, NSM, or HLR Provisioning System in the **remote-server-ip-address** field.
5	Enter the user ID in the **remote-userid** field. The remote site system administrator provides this information.
6	Enter the password in the **remote-password** field. The remote site system administrator provides this information.
7	Select the **subsystem-name** from the drop-down menu. Valid selections are the following: • (All)- all subsystems • administration-all data associated with the administration screens • gtt- all data associated with the global title translation screens • gws- all data associated with the gateway screening screens • ips7- all data associated with the IPS7 (links to application servers) screens

- mtp- all data associated with the message transfer part screens
- np-all data associated with the number portability screens
- om- all data associated with the operational measurement screens
- platform- all data associated with the platform screens
- rm- all data associated with the routemaster screens
- sccp- all data associated with the signalling connection control part screens
- security-all data associated with the security screens
- sip-all data associated with the session initiation protocol screen
- slr-all data associated with the service location register screen

8 Select the **table-name** from the drop-down menu. Valid selections are every individual table associated with the main subsystems mentioned above or a choice of (All).

9 Select the **output-format** to be used with the bulk output operation. Valid selections are:

- multi-line-ascii- readable text format
- csv-comma separated format suitable for spreadsheets
- html- web ready format useful for publishing
- bulk-input- same format as required by bulk input useful for backups and transfer of data from one system to another

10 Select the **bulkinput-command-type** to be used for the bulk output. Valid selections are provision and delete. This field is only useful when the bulk-input format is selected in the output-format field.

11 Click the **single-file-only-option** checkbox if you require all the output tables to be contained in the same output file. This is most useful when using the bulk input format as you can then apply a single file for a subsequent bulk input.

12 Click **Execute**.

—End—

Service database

Number Portability (NP) or Service Location Register (SLR) data is stored in the application database on the system. Once the database is established it can be updated dynamically with the SMI interface. There are times, such as during the initial installation of the system, when large amounts of data must be transferred to the database. To complete this data transfer as quickly as possible, a bulk load is performed on the system.

If the system is configured with a local subsystem (LSS) class of NP_ANSI, the Number Portability (NP) database (DB) data is delivered to the USP by a Local Service Management System (LSMS). If the system is configured with an LSS class of NP_ITU, the NPDB data is delivered to the USP by a Network Services Manager (NSM). If the system is configured with an LSS class of SLR, the NPDB data is delivered to the USP by a Home Location Register (HLR) Provisioning System.

To reduce the time of the FTP portion of the bulk load operation, you can compress the data file portion of bulk files. To do that, use the "zlib compressed data format" as described in IETF RFCs 1950 and 1951. A well known implementation of this format is the UNIX gzip and gunzip facility. The USP detects and uncompresses the bulk file as necessary.

The schema file contains the filename of the data file. Any changes to the data filename must be reflected in the schema file. The schema file can be edited using any text editor (such as vi).

To bulk load data to the service database, complete the following procedure:

You cannot perform a bulk load operation until all NP or SLR LSS instances are deactivated.

Performing a bulk input of a service database

Step	Action
	At the OAMP workstation
1	Click **Configuration>sccp>shared-local-subsystem**.
2	Deactivate the LSS. To do this, complete the following steps: a. Click the **Search** panel tab. Locate the LSS that you want to deactivate. Double-click the result in the search results to transfer to the administration panel. b. Click **Deactivate**.
3	Click **Configuration>sccp>shared-local-subsystem-instance**.
4	Deactivate the LSSIs. To do this, complete the following steps:

a. Click the **Search** panel tab. Locate the LSS instances that you want to deactivate. Double-click the result in the search results to transfer to the administration panel.

b. Click **Deactivate.**

c. Repeat **a** and **b** for all instances that you want to deactivate.

5 Click **Administration>bulk-input>bulk-input-services-db**.

A full bulk load is a complete reload of the application database. All existing records are deleted and replaced with the records located on the remote system.

An incremental bulk load preserves any existing records in the application database. It adds the records contained in the incremental bulk load file to the contents of the database.

When the incremental bulk load contains records that already exist in the database, the existing record is replaced by the record specified in the bulk load file *if no chains are present*. If chains are present, this corrupts the database. Only new records are allowed with chains.

Perform an incremental bulk load when it is necessary to populate the application database on the system with records from more than one LSMS, NSM, or HLR Provisioning System database. In this case, designate the first bulk load as a full bulk load and the subsequent ones as incremental bulk loads.

6 Enter the full path name of your bulk input schema file in the **bulk-file-name** field of up to 128 alphanumeric characters.

Two files are transferred: a schema file and a data file. The schema file describes the structure of the larger data file and contains the file name of the data file.

ATTENTION

Contact personnel at the LSMS, NSM, or HLR Provisioning System site to ensure that this file is prepared.

7 Enter the remote IP address of the LSMS, NSM, or HLR Provisioning System in the **remote-server-ip-address** field.

8 Enter the user ID in the **remote-userid** field. The remote site system administrator provides this information.

9 Enter the password in the **remote-password** field. The remote site system administrator provides this information.

10 Select a **sub-system** type from the pull down menu. Valid selections are **NP_ANSI, NP_ITU14** and **SLR**.

11 Select a **load-type** from the pull down menu. Valid selections are **incremental-load** and **full-load**

12 Click **Execute**.

The Bulk Load Progress window appears. The Transfer field indicates the status of the FTP action from the LSMS, NSM, or HLR Provisioning System to the system. The Import field indicates the status of the file conversion and database loading on the system. The bulk load completes when the Transfer and Import fields both indicate 100 percent.

13 If you need to **abort** a bulk load operation, click Abort on the Bulk Load Progress window. The LSS Class reverts to its previous status.

14 Activate the local LSS and all LSS instances at both the SCCP Local Subsystem Instance and at the SCCP Local Subsystem windows. To do this, complete the following steps:

a. Click **Configuration>sccp>shared-local-subsystem**.

b. Click the **Search** panel tab. Locate the LSS that you want to activate. Double-click the result in the search results to transfer to the administration panel.

c. Click **Activate**.

d. Click **Configuration>sccp>shared-local-subsystem-instance**.

e. Click the **Search** panel tab. Locate the LSS Instances that you want to activate. Double-click the result in the search results to transfer to the administration panel.

f. Click **Activate**.

g. Repeat step 14e and step 14f for all instances that you want to activate.

—End—

Performing a bulk output of a service database

Step	Action

At the OAMP workstation

1 Click **Configuration>sccp>shared-local-subsystem**.

2 Deactivate the LSS. To do this, complete the following steps:

a. Click the **Search** panel tab. Locate the LSS that you want to deactivate. Double-click the result in the search results to transfer to the administration panel.

b. Click **Deactivate**.

3 Click **Configuration>sccp>shared-local-subsystem-instance**.

4 Deactivate all LSSIs. To do this, complete the following steps:

a. Click the **Search** panel tab. Locate the LSS you want to deactivate. Double-click the result in the search results to transfer to the administration panel.

b. Click **Deactivate**.

c. Repeat step 4a and step 4b for all instances that you want to deactivate.

5 Lock the NPC cards:

a. Click **Configuration>platform>node**.

b. Click **Graphical View**.

c. Select the NPC node you want to lock.

d. Click **Lock**.

6 Click **Administration>bulk-output>bulk-output-services-db**.

7 Enter the full path name of the destination for your bulk output file in the path field of up to 128 alphanumeric characters.

Two files are transferred: a schema file and a data file. The schema file describes the structure of the larger data file and contains the file name of the data file

ATTENTION
Contact personnel at the LSMS, NSM, or HLR Provisioning System site to ensure that the target directory specified is acceptable and available

8 Enter the a unique tag to be placed as a prefix on the exported files in the file-prefix field of up to 32 alphanumeric characters.

9 Enter the remote IP address of the LSMS, NSM, or HLR Provisioning System in the **remote-server-ip-address** field.

10 Enter the user ID in the **remote-userid** field. The remote site system administrator provides this information.

11 Enter the password in the **remote-password** field. The remote site system administrator provides this information.

12 Select a sub-system type from the pull down menu. Valid selections are NP_ANSI, NP_ITU14 and SLR.

13 Click **Execute**.

14 Activate the local LSS and all LSS instances at both the SCCP Local Subsystem Instance and at the SCCP Local Subsystem windows. To do this, complete the following steps:

a. Click **Configuration>sccp>shared-local-subsystem**.

b. Click the **Search** panel tab. Locate the LSS that you want to activate. Double-click the result in the search results to transfer to the administration panel.

c. Click **Activate**.

d. Click **Configuration>sccp>shared-local-subsystem-instance**.

e. Click the **Search** panel tab. Locate the LSS Instances that you want to activate. Double-click the result in the search results to transfer to the administration panel.

f. Click **Activate**.

g. Repeat steps **e** and **f** for all instances that you want to activate.

—End—

Maintenance: Routine Procedures

To keep your USP performing optimally, Nortel Networks recommends that you perform a few regular maintenance tasks daily, monthly, weekly, and annually.

Daily

Back up the OAMP workstation data.

Weekly

Back up the OAMP workstation data to tape (full).

Monthly

Test the LAN-to-LAN remote access connection.

Test the dial-up remote access connection.

Annually

Tighten screws on cable connections, power cables, and shelf mounting.

Maintenance: Activities on an RTC System Node

The following maintenance activities can be performed on an RTC system node:

- Diagnostics
- Switch activity (SWACT)
- Lock
- Off-line
- Load
- Unlock
- Restart

RTC system node diagnostic tests

You can run diagnostic tests on the inactive RTC system node to check for hardware faults. On an RTC system node, diagnostics verify communication to the RTC system node and internal operation of the RTC system node.

Running diagnostic tests on an RTC system node

Step	Action
	At the OAMP workstation
1	Open the RTC node window. To do this: a. Click **Configuration>platform>node**. b. Click **Graphical view**. c. Double-click on the icon for the RTC system node you want to test to open the Administration view.
2	Click **Lock** to lock the RTC system node.

ATTENTION

You must make sure that the RTC node is inactive before you lock it. To ensure that the node is inactive, perform a SWACT first.

3 Click **Load**.

If:	Do:
you receive a database sync alarm	contact your next level of support.
the test does not pass or the RTC fails to load	replace the mission card for the RTC.

—End—

CAUTION
Wear wrist straps and use standard antistatic precautions.

Replacing the mission card of the RTC

Step Action

At the OAMP workstation

1 Open the RTC node window. To do this:

a. Click **Configuration>platform>node**.

b. Click **Graphical view**.

c. Double-click on the inactive RTC system node to open the provisioning window.

ATTENTION
If the new mission card and TM have different PECs than the ones you are replacing, you must change the PEC in the Administration tab before loading the card.

2 Click **Lock**.

ATTENTION
You must make sure that the RTC node is inactive before you lock it. To ensure that the node is inactive, perform a SWACT first.

3 Click **Offline**.

4 Obtain new mission cards, verify they have the correct PEC labels, and ensure the top and bottom latches are in the outward position.

5 Press outward on the top and bottom latches of the mission card to release it from the CAM shelf. Two audible clicks can be heard when the mission card is released completely.

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

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

8 Apply pressure to the faceplate until you feel resistance.

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

10 On the front and rear of the CAM shelf, press the Lamp Test buttons. If the LEDs do not light for the system node you just replaced, ensure the mission card is seated properly by repeating step 7 to step 9 again.

11 On the associated system node Administration tab, click **Load** and wait for the system node to enable, click **Unlock** to ensure the system node returns to full service, and click **Graphical View**.

12 On the shelf_name window, ensure that the green LED indicator is lit for the system node.

13 Check Alarms. If the alarm is still displayed for the same system node, contact your next-level support.

—End—

RTC system node manual SWACT operations

The active RTC system node handles all system processing and stores a record of all system data. The inactive RTC system node acts as a backup, and when it is enabled, is ready to assume the active role at any time. The SWACT operation switches the active and inactive RTC system nodes.

Automatic SWACT operations are performed if you lock the active RTC system node when the inactive RTC system node is unlocked and enabled or if the active RTC system node should fail. Both RTC system nodes must be in the same availability state (locked or unlocked) and enabled to be able to perform a manual SWACT operation.

ATTENTION

If an automatic or manual SWACT operation is performed while you are loading an offline system node, the load operation will be unsuccessful and the offline system node will remain offline. You will have to load the system node once again.

Switching the active RTC system node manually

Step	Action

At the OAMP workstation

1 Open the RTC node window. To do this:

a. Click **Configuration>platform>node**.

b. Click **Graphical view**.

c. Double-click on the icon for the RTC system node for which you want to perform the SWACT to open the Administration view.

2 Click **SWACT** to switch the active RTC system node.

ATTENTION

You must make sure that the RTC node is inactive before you lock it. To ensure that the node is inactive, perform a SWACT first.

—End—

RTC system node lock operations

You must lock an RTC system node when you are going to perform RTC system node maintenance operations. Locking the RTC system node makes the IP paths unavailable.

Locking a RTC system node

Step	Action

At the OAMP workstation

1 Open the RTC node window. To do this:

a. Click **Configuration>platform>node**.

b. Click **Graphical view**.

c. Double-click on the icon for the RTC system node you want to lock to open the Administration view.

2 Click **Lock** to lock the RTC system node.

—End—

RTC system node offline operations

You can take a locked RTC system node offline. You must take a RTC system node offline before replacing any of its hardware.

Taking an RTC system node offline

Step	Action
	At the OAMP workstation
1	Open the RTC node window. To do this: a. Click **Configuration>platform>node**. b. Click **Graphical view**. c. Double-click on the icon for the RTC system node you want to take offline to open the Administration view.
2	If the RTC system node is locked, proceed to step 3. If the RTC system node is Unlocked, click **Lock** in the Maintenance portion of the window and proceed to step 3.
3	Click **Offline** to take the RTC system node offline.

—End—

RTC system node load operations

You can perform a load operation to download the boot images and re-initialize the RTC system node. Only a locked and enabled or a disabled RTC system node can be loaded.

Loading a RTC system node

Step	Action
	At the OAMP workstation
1	Open the RTC node window. To do this: a. Click **Configuration>platform>node**. b. Click **Graphical view**. c. Double-click on the icon for the RTC system node you want to load to open the Administration view.

2 If the RTC system node is locked, proceed to step 3. If the RTC system node is Unlocked, click Lock in the Maintenance portion of the window and proceed to step 3.

3 Click **Load** to download the RTC system node boot images and reboot the RTC system node.

—End—

RTC system node unlock operations

You can unlock a locked RTC system node, as long as it is not offline at the same time.

Unlocking a RTC System Node

Step	Action
	At the OAMP workstation
1	Open the RTC node window. To do this: a. Click **Configuration>platform>node**. b. Click **Graphical view**. c. Double-click on the icon for the RTC system node you want to unlock to open the Administration view.
2	Click **Unlock** to unlock the RTC system node.

—End—

RTC system node restart operations

You can cycle the card through the lock, load, unlock commands and return it to its current state using the restart command. The links are reactivated automatically by the system when the card returns to its in-service state.

ATTENTION

For SS7 Link system nodes, any in-service links are inhibited and deactivated if appropriate to ensure network stability when the restart command is executing.

Restarting the RTC system node

Step	Action
	At the OAMP workstation
1	Open the RTC node window. To do this:

a. Click **Configuration>platform>node**.

b. Click **Graphical view**.

c. Double-click on the icon for the RTC system node you want to restart to open the Administration view.

2 Click **Restart** to restart the RTC system node.

—End—

Maintenance: Activities on a CC System Node

The following maintenance activities can be performed on a CAM Controller (CC) system node:

- Diagnostic test
- Lock
- Off-line
- Load
- Unlock
- Restart

The following conditions apply to maintenance activities in a dual-shelf system (control CAM shelf and extension CAM shelf):

- Except for loading a disabled CC system node during isolation recovery, you cannot perform any maintenance activities on a CC system node of an extension CAM shelf while the extension CAM shelf is in isolation. For more information about isolation, see *USP Fault Management* (NN10071-911).
- The system prohibits any maintenance activities that would adversely affect communication between the control CAM shelf and the extension CAM shelf. For example, during loss of communication redundancy (LOCR), one inter-shelf communication path is down. During LOCR, off-lining or loading a CC system node on the other path would sever communication between the shelves.
- The system prohibits any maintenance activities that would adversely affect its only network clock source.

CC system node diagnostic tests

You can run diagnostic tests to check for hardware faults on an enabled CC system node. On a CC system node, diagnostic tests run at software initialization to validate hardware sanity.

Running a diagnostic test on a CC system node

Step	Action
	At the OAMP workstation
1	Open the CC node window. To do this: a. Click **Configuration>platform>node**. b. Click **Graphical view**.

c. Double-click on the icon for the CC system node you want to test to open the Administration view.

2 Click **Lock** to lock the CC system node.

3 Click **Load**. The CC system node boot image is downloaded and the CC system node is re-initialized and enabled.

If the test does not pass, replace the mission card for the CC.

—End—

CAUTION
Wear wrist straps and use standard antistatic precautions.

Replacing the mission card and TM for the CC

Step	Action

At the OAMP workstation

1 Open the CC node window. To do this:

a. Click **Configuration>platform>node**.

b. Click **Graphical view**.

c. Double-click on the icon for the CC system node you want to replace to open the Administration view.

2 Click **Lock**.

3 Click **Offline**.

4 Obtain new mission cards or TMs, verify they have the correct PEC labels, and ensure the top and bottom latches are in the outward position.

ATTENTION
If the new mission card and TM have different PECs than the ones you are replacing, you must change the PEC in the administration tab before loading the card.

5 Before you replace a CC mission card, unseat and disconnect its corresponding OC-3 TM.

6 Before you unseat a TM, remove its connector(s) by unscrewing the thumbscrews on the top and bottom of each connector. Gently pull off the TM cable connector(s).

7 Press outward on the top and bottom latches of the mission card or TM to release it from the CAM shelf. Two audible clicks can be heard when the mission card or TM is released completely.

8 Grasp the top and bottom latches of the mission card or TM and gently pull it toward you to remove it from the CAM shelf.

9 Position the top and bottom latches of the new mission card or TM facing you, and gently slide the mission card or TM into the card guide of the one you removed, seating the bottom of the mission card or TM into the card guide and then the top.

10 Apply pressure to the faceplate until you feel resistance.

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

12 After you replace the TM, plug in the TM connector(s) and turn the thumbscrews on the top and bottom of the connector(s) to tighten.

13 If you replaced a CC mission card, remember to reseat and reconnect its OC-3 TM.

14 On the front and rear of the CAM shelf, press the Lamp Test buttons. If the LEDs do not light for the system node you just replaced, ensure the mission card and TM are seated properly by performing step 9 to step 14 again.

15 On the associated system node administration tab, click **Load** and wait for the system node to enable, click **Unlock** to ensure the system node returns to full service, and click **Graphical View**.

16 On the shelf_name window, ensure that the LED indicator is lit for the system node and click **Close**.

17 Check Alarms. If this alarm is still displayed for the same system node, contact your next-level support.

—End—

CC system node lock operations

You must lock a CC system node before performing CC system node maintenance operations, except for diagnostics. To be able to lock a CC system node, the following conditions apply:

- The mate CC system node in the shelf must be unlocked and enabled, or all of the application system nodes in the shelf must be locked.
- In a dual-shelf system, both CC system nodes and all of the application system nodes on the extension CAM shelf must be locked before you can lock the last enabled, unlocked CC system node on the control CAM shelf.

For more information on locking CC system nodes, refer to the table of Locking and Unlocking Rules.

To lock a CC system node, perform the following steps:

Locking a CC system node

Step	Action
	At the OAMP workstation
1	Open the CC node window. To do this: a. Click **Configuration>platform>node**. b. Click **Graphical view**. c. Double-click on the icon for the CC system node you want to lock to open the Administration view.
2	Click **Lock** to lock the CC system node.

—End—

CC system node offline operations

A locked CC system node can be taken offline. You must take a CC system node offline before replacing any of its hardware.

Taking a CC system node offline

Step	Action
	At the OAMP workstation
1	Open the CC node window. To do this: a. Click **Configuration>platform>node**. b. Click **Graphical view**.

c. Double-click on the icon for the CC system node you want to take offline to open the Administration view.

2 If the CC system node is locked, proceed to the next step. If the CC system node is unlocked, click Lock in the Maintenance portion of the window and proceed to the next step.

3 Click **Offline** to take the CC system node offline.

—End—

CC system node load operations

You can perform a load operation to download the boot image and re-initialize a CC system node. You must lock the CC system node before you can load it.

If an automatic or manual SWACT operation is performed on the RTC system nodes while you are loading a CC system node, the load operation is unsuccessful and the CC system node remains disabled. You have to load the CC system node again.

Loading a CC system node

Step	Action

At the OAMP workstation

1 Open the CC node window. To do this:

a. Click **Configuration>platform>node**.

b. Click **Graphical view**.

c. Double-click on the icon for the CC system node you want to load to open the Administration view.

2 If the CC system node is locked, proceed to the next step. If the CC system node is unlocked, click **Lock** in the Maintenance portion of the window.

3 In the Maintenance portion of the window, click **Load**. The CC system node boot image is downloaded and the CC system node is re-initialized and enabled.

—End—

CC system node unlock operations

To be able to unlock a CC system node, the following conditions apply:

- At least one of the RTC system nodes in the control CAM shelf must be unlocked and enabled.
- In a dual-shelf system, at least one CC system node on the control CAM shelf must be unlocked before you can unlock a CC system node on the extension CAM shelf.

Unlocking a CC system node

Step	Action
	At the OAMP workstation
1	Open the CC node window. To do this: a. Click **Configuration>platform>node**. b. Click **Graphical view**. c. Double-click on the icon for the CC system node you want to unlock to open the Administration view.
2	Click **Unlock**.
	—End—

CC system node restart operations

You can cycle the card through the lock, load, and unlock commands and return it to its current state using the restart command. The links are reactivated automatically by the system when the card returns to its in-service state.

ATTENTION

For SS7 Link system nodes, any in-service links are inhibited and deactivated if appropriate to ensure network stability when the restart command is executing.

Restarting the CC system node

Step	Action
	At the OAMP workstation
1	Open the CC node window. To do this: a. Click **Configuration>platform>node**. b. Click **Graphical view**.

c. Double-click on the icon for the CC system node you want to restart to open the Administration view.

2 Click **Restart** to restart the CC system node.

—End—

Maintenance: Activities on an Link System Node

The following maintenance activities can be performed on an Link system node:

- Lock
- Off-line
- Load
- Unlock
- Restart
- Remote loopback
- BERT
- SS7 link administration

Link system node lock operations

You must lock an Link system node when you are going to perform Link system node maintenance operations, except for diagnostics. Locking the Link system node makes the paths unavailable.

Locking a Link system node

Step	Action
	At the OAMP workstation
1	Open the node window. To do this: a. Click **Configuration>platform>node**. b. Click **Graphical view**. c. Double-click the icon for the system node you want to lock to open the Administration view.
2	Click **Lock**.
	—End—

Link system node offline operations

You can take a locked Link system node offline. You must take a Link system node offline before replacing any of its hardware.

Taking a Link system node offline

Step	Action
	At the OAMP workstation
1	Open the node window. To do this: a. Click **Configuration>platform>node**. b. Click **Graphical view**. c. Double-click the icon for the system node you want to take offline to open the Administration view.
2	If the Link system node is locked, proceed to the next step. If the Link system node is Unlocked, click **Lock** and proceed to the next step.
3	Click **Offline**.
	—End—

Link system node load operations

You can perform a load operation to download the boot images and re-initialize the Link system node. Only a locked and enabled or a disabled Link system node can be loaded.

ATTENTION

If an automatic or manual SWACT operation is performed on the RTC system nodes while you are loading a Link system node, the load operation is unsuccessful and the Link system node remains disabled. You have to perform the load operation again after the SWACT operation is complete.

Loading a Link system node

Step	Action
	At the OAMP workstation
1	Open the node window. To do this: a. Click **Configuration>platform>node**. b. Click **Graphical view**. c. Double-click the icon for the system node you want to load to open the Administration view.
2	If the Link system node is locked, proceed to the next step. If the Link system node is Unlocked, click **Lock** and proceed to the next step.
3	Click **Load**.

—End—

Link system node unlock operations

To be able to unlock a Link system node, at least one CC system node must be unlocked and enabled.

Unlocking a Link system node

Step	Action
	At the OAMP workstation
1	Open the node window. To do this: a. Click **Configuration>platform>node**. b. Click **Graphical view**. c. Double-click the icon for the system node you want to unlock to open the Administration view.
2	Click **Unlock**.

—End—

Link system node restart operations

You can cycle the card through the lock, load, and unlock commands and return it to its current state using the restart command. The links are reactivated automatically by the system when the card returns to its in-service state.

ATTENTION

For SS7 Link system nodes, any in-service links are inhibited and deactivated if appropriate to ensure network stability when the restart command is executing.

Restarting a Link system node

Step	Action
	At the OAMP workstation
1	Open the RTC node window. To do this: a. Click **Configuration>platform>node**. b. Click **Graphical view**.

c. Double-click the icon for the RTC system node you want to restart to open the Administration view.

2 Click **Restart** to restart the RTC system node.

—End—

Remote loopback

To verify the communication path between the two ends of a SS7 link, run BERT (bit error rate test) on the link. To return BERT generated from the far end of the link, you must configure the port associated with the SS7 link for remote loopback. Remote loopback testing can only be performed on an enabled Link system node that does not have SS7 traffic associated with it.

Remote loopback cannot be set on IP Link or SS7 IP Link node types.

To set up a remote loopback on one of the port/channel on a Link system node, perform the following steps:

Setting up a remote loopback

Step	Action
	At the OAMP workstation
1	Open the node window. To do this: a. Click **Configuration>platform>node**. b. Click **Graphical view**. c. Double-click the icon for the system node you want to set for loopback to open the Administration view.
2	Confirm that there is either no link associated to the port/channel in question or that the link is deactivated. a. Click **Retrieve** (located in the command bar to the immediate left of the **Help** button). b. Select **mtp link** from the table relation list. c. If this is a channelized link card, select **platform channel** from the table relation list. Otherwise, select **platform port**. d. Click **OK**. e. In the **mtp-link** window, ensure that all links are deactivated. If active links are present, Post and Deactivate them.
3	In the Port or Channel window, double-click on the port or channel to be tested.

4 Click the **Loopback Set** command.

5 When the test is complete, clear the remote loopback by clicking the **Loopback Clear** command

6 If any links were deactivated previously in this procedure, return them to service by selecting them, clicking **Post** in the mtp-link window, then clicking the **Activate** command.

—End—

BERT

Run BERT (Bit Error Rate Test) to verify the communication path between the two ends of an SS7 link. BERT is run from a port/channel on a Link system node to the far end of the link.

For a BERT to be successful, the transmitted test pattern must be returned to the transmitting node for comparison. To do this, a loopback is required, either at the far end of the link or somewhere in the intermediate transmission media.

Each link is identified by a unique combination of node, port and channel (channel is applicable only to channelized link nodes). You can run only one BERT session per Link system node at one time. BERT can be run only on an enabled Link system node in which the port/channel is idle.

The maximum duration for a BERT is 24 hours. If BERT is still running when the duration reaches 24 hours, the system automatically stops the test and generate a log with the results.

ATTENTION

BERT cannot be run on IP Link or SS7 IP Link node types.

A resolution for HSLs in which the BERT maximum duration is 12 hours will be featured in a future release.

To run BERT from a port/channel on a Link system node, perform the following steps:

Running BERT on a Link system node

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

3 Double-click the system node you want to set for loopback to open the Administration view.

4 Confirm that there is either no link associated to the port or channel in question or that the link is deactivated.

a. Click **Retrieve** (located in the command bar to the immediate left of the **Help** button).

b. Select **mtp link** from the table relation list.

c. If this is a channelized link card, select **platform channel** from the table relation list. Otherwise, select **platform port**.

d. Click **OK**.

e. In the mtp-link window, ensure that all links are deactivated. If active links are present, Post and Deactivate them.

5 Ensure a loopback is set, either at the far end of the link or somewhere in the intermediate transmission media.

6 In the Port or Channel window, double-click on the port or channel to be tested. The window changes to the Administration panel.

7 Click the **`Bert Start`** command to begin testing. The BERT fields change to indicate the test is running. The system updates the results boxes approximately every 20 seconds.

An Out of sync message displayed in the bert-bit-error-rate the first time that the box is updated could be a result of normal network delays. If the Out of sync message continues to be displayed during subsequent updates, investigate and correct the cause before continuing with the BERT.

8 Click the **`Bert Stop`** command to conclude testing. The final test statistics are generated in a log and the bert fields change to indicate the port/channel is idle.

9 If you ran the BERT on a V.35 port configured as DTE, check to ensure that the clock signal for the V.35 TM was present during the entire test. If you ran the BERT on any other link type/configuration, proceed to step 10.

a. Calculate the approximate duration of the BERT using the BERT start and stop time stamps. The start time stamp is available from the BERT Start Requested log and the stop time stamp is available from the BERT Stop Requested log.

b. Compare the calculated duration of the BERT to the test duration value reported in the BERT Test Statistics log. If the two values differ by more than five percent, the V.35 TM probably lost its clock source for some portion of the BERT. The difference

between the calculated and reported BERT duration values is the amount of time that the V.35 TM lost its clock signal.

c. If your check indicates that the V.35 TM lost its clock signal for some portion of the BERT test, correct the clock problem and run the BERT again.

10 If any links were deactivated previously in this procedure, return them to service by selecting them, clicking **Post** in the mto-link window, then clicking the **`Activate`** command.

—End—

SS7 link administration

The SS7 links provide the physical connection between two adjacent signaling nodes in a network. You can administer the SS7 links associated with the ports on the Link system nodes. For more information on the administration of SS7 links, see *USP Configuration Management* (NN10093-511).

Accessing the link administration function

Step	Action
	At the OAMP workstation
1	Click **Configuration>mtp>link**.

—End—

Maintenance: Activities on an IPS7 Link System Node

The following maintenance activities can be performed on an IPS7 Link system node:

- Lock
- Off-line
- Load
- Unlock
- Restart

IPS7 Link system node lock operations

You must lock an IPS7 Link system node when you are going to perform IPS7 Link system node maintenance operations, except for diagnostics. Locking the IPS7 Link system node makes the IPS7 paths unavailable.

Locking a IPS7 Link system node

Step	Action
	At the OAMP workstation
1	Open the node window. To do this: a. Click **Configuration>platform>node**. b. Click **Graphical view**. c. Double-click the icon for the system node you want to lock to open the Administration view.
2	Click **Lock**.
	—End—

IPS7 Link system node offline operations

You can take a locked IPS7 Link system node offline. You must take a IPS7 Link system node offline before replacing any of its hardware.

Taking a IPS7 Link system node offline

Step	Action
	At the OAMP workstation

1 Open the node window. To do this:

a. Click **Configuration>platform>node**.

b. Click **Graphical view**.

c. Double-click the icon for the system node you want to take offline to open the Administration view.

2 If the Link system node is locked, proceed to the next step. If the Link system node is Unlocked, click **Lock** and proceed to the next step.

3 Click **Offline**.

—End—

IPS7 Link system node load operations

You can perform a load operation to download the boot images and re-initialize the IPS7 Link system node. Only a locked and enabled or a disabled IPS7 Link system node can be loaded.

ATTENTION

If an automatic or manual SWACT operation is performed on the RTC system nodes while you are loading a IPS7 Link system node, the load operation is unsuccessful and the IPS7 Link system node remains disabled. You have to perform the load operation again after the SWACT operation is complete.

Loading a IPS7 Link system node

Step	Action

At the OAMP workstation

1 Open the node window. To do this:

a. Click **Configuration>platform>node**.

b. Click **Graphical view**.

c. Double-click the icon for the system node you want to load to open the Administration view.

2 If the Link system node is locked, proceed to the next step. If the Link system node is Unlocked, click **Lock** and proceed to the next step.

3 Click **Load**.

—End—

IPS7 Link system node unlock operations

To be able to unlock a IPS7 Link system node, at least one CC system node must be unlocked and enabled.

Unlocking a IPS7 Link system node

Step	Action
	At the OAMP workstation
1	Open the node window. To do this: a. Click **Configuration>platform>node**. b. Click **Graphical view**. c. Double-click the icon for the system node you want to unlock to open the Administration view.
2	Click **Unlock**.

—End—

IPS7 Link system node restart operations

You can cycle the card through the lock, load, and unlock commands and return it to its current state using the restart command. The links are reactivated automatically by the system when the card returns to its in-service state.

ATTENTION

For SS7 Link system nodes, any in-service links are inhibited and deactivated if appropriate to ensure network stability when the restart command is executing.

Restarting the IPS7 Link system node

Step	Action
	At the OAMP workstation
1	Open the RTC node window. To do this: a. Click **Configuration>platform>node**. b. Click **Graphical view**. c. Double-click the icon for the system node you want to restart to open the Administration view.
2	Click **Restart** to restart the RTC system node.

—End—

Maintenance: Fan Filter

Perform the following steps monthly to clean the fan filter:

Cleaning the fan filter

Step	Action
	At the USP
1	Turn the two screws on the front of the shelf counter-clockwise (3/4 turn) to loosen the front air grill.
2	Remove the front grill.
3	Slide the metal fan filter tab to one side to free the fan filter for removal.
4	Pull the fan filter forward and completely remove it from the shelf.
5	Clean the fan filter using a mild detergent and a constant stream of warm water.
6	Allow the fan filter to air dry.
7	Return the fan filter to the shelf.
8	Slide the metal fan filter tab to its original position to secure the fan filter.
9	Replace the front grill.
10	Turn the two screws on the front of the shelf clockwise (3/4 turn) to secure the front grill.
	—End—

Carrier VoIP

USP Security and Administration

Publication: NN10159-611
Document status: Standard
Document version: 07.04
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.