



## Cisco LNP Mediation Device

---

In Hungary and some other European countries, service providers are responsible for downloading Local Number Portability (LNP) data from a Central Reference Database (CRD) for their switches. To enable the LNP functions on Cisco BTS 10200 Softswitches in these locales, the Cisco LNP Mediation Device provides LNP data retrieval services for the Cisco BTS 10200 Softswitch by downloading the LNP data from the CRD and mapping the data into the softswitches' internal data format.



**Note**

---

This release is applicable only to Hungarian LNP.

---

The Cisco LNP Mediation Device runs on the Sun Microsystems Netra V120 with a minimum of 2GB of memory. This hardware configuration enables the Cisco LNP Mediation Device to support up to ten Cisco BTS 10200 Softswitches.

The Cisco LNP Mediation Device supports the following:

- Web-based GUI end-user interface.
- Populate up to 2 million records.
- Scheduling of automatic synchronization time windows.
- Synchronization updates initiated from a defined past point in time.
- Full synchronization update can also be initiated on demand.
- Throttle watermarks can be defined for the number of records being synchronized.
- SOAP/HTTPS management interface to the Hungarian CRD.
- HTTPS interface for downloading data from CRD.
- CORBA/XML interface for downloading data to the Cisco BTS 10200 EMS.
- Scheduler that performs a delta update from the CRD at provisioned time windows.
- Mapping of CRD data to the Cisco BTS 10200 LNP schema.
- Cisco LNP Mediation Device runs only in Simplex mode (does not support Duplex mode).
- Data resiliency when losing connectivity to the Cisco BTS 10200 EMS.
- Periodically purges expired LNP data from the Cisco BTS 10200 EMS.
- Backup and restore of configuration data.
- Uses IP-aliasing on the EMS to communicate with the active EMS in case of a failover.
- Logs failures and event reports through SNMP traps.
- Standard SNMP MIBS supported by CIAgent from SNMP Research International.

# Network Management

A UNIX command level login is required only for installing, starting, or stopping the Cisco LNP Mediation Device. The web-based graphical user interface (GUI) supports all other day-to-day operations.

**Note**

---

Microsoft Internet Explorer 6.0 is the only web browser supported by the Cisco LNP Mediation Device.

---

The Sun Solaris 10 operating system uses the Cisco BTS 10200 Element Management System (EMS) jumpstart image for Release 4.5. The Cisco LNP Mediation Device hardware and operating system installation time is approximately the same as for the Cisco BTS 10200 EMS. The software installation time is approximately 15 minutes.

## Database Synchronization

Automatic synchronization time windows can be defined to include a start time, a duration, and day(s) of the week. The Cisco LNP Mediation Device has a Scheduler that wakes up at the provisioned start times and performs an incremental update from the CRD. Only incremental updates are normally supported for automatic synchronization; however, if the last successful update was more than 30 days previous, or if this is the first time the Cisco LNP Mediation Device attempts an automatic update, a full update is performed.

If an update is already in progress, the Cisco LNP Mediation Device rejects the scheduled update. If the data cannot be downloaded from the CRD by the stop time (as determined by the duration setting), the Cisco LNP Mediation Device terminates the update. If the data has been downloaded from the CRD, but has not been transferred to the Cisco BTS 10200 when the stop time arrives, the Cisco LNP Mediation Device continues transferring data.

The Cisco LNP Mediation Device also validates that schedules do not overlap. If a schedule entered or modified on the GUI overlaps an existing schedule, an error message is displayed and the changes are rejected.

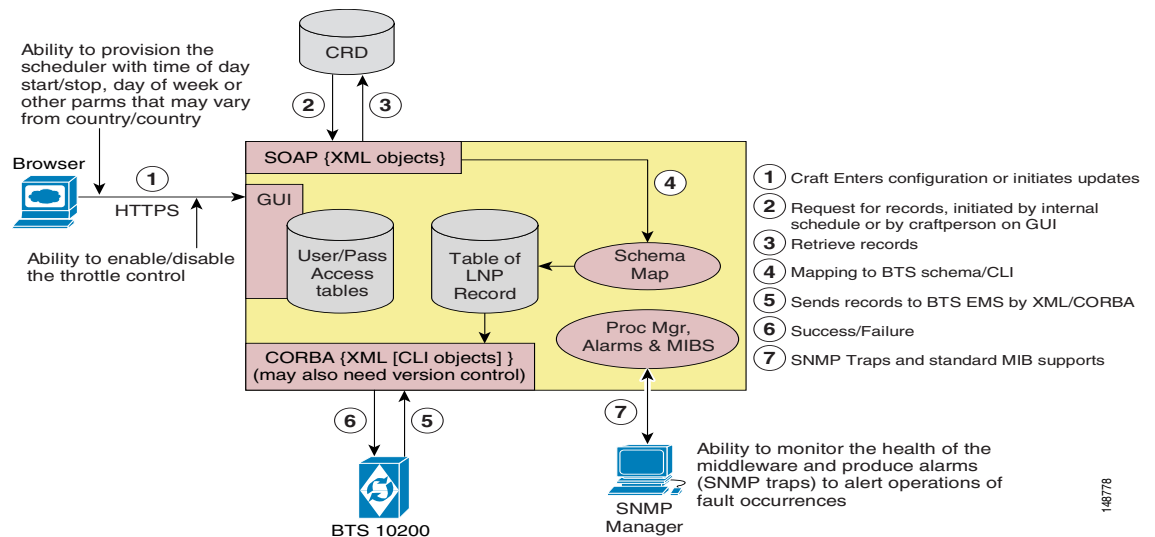
## Full Synchronization Update

A full synchronization update can be initiated on demand through the web-based GUI interface. You must provide a duration for the update. If the full synchronization data cannot be retrieved from the CRD within the duration specified, the update is terminated. If an update is already in progress, the request is rejected.

## Partial Synchronization Update

A partial synchronization update can also be initiated from any past point in time or from the occurrence of the last successful update through the web-based GUI. You must provide a duration for the update. If the requested synchronization data cannot be retrieved from the CRD within the duration specified, the update is terminated. If an update is already in progress, the request is rejected.

[Figure 1](#) illustrates the LNP synchronization process.

**Figure 1** LNP Synchronization

## Error Recovery

The web-based GUI provides the current status for CRD data downloads and the past history for each scheduled and manual update for up to 30 days. The Cisco LNP Mediation Device also stores transaction history for data sent to each Cisco BTS 10200 Softswitch for at least the last 7 days. The Cisco LNP Mediation Device may trim the history periodically to reduce the database size; however, the local database can store up to 2 million LNP records per Cisco BTS 10200 Softswitch, plus all the transaction history data.

The following data is stored for each transaction history entry:

- date-time of the transaction (DD/MM/YYYY HH:MM:SS)
- status (success/fail)
- start phone number (DN)
- stop phone number (DN)
- routing number
- valid-from timestamp
- valid-to timestamp

The transaction history can also be displayed on the GUI by the user to troubleshoot problems.

After each successful update, the Cisco LNP Mediation Device stores the successful data timestamp and uses it for the next update. If there is a system failure during an update, or a failure that results in missing one or more updates, the next time window either does a full update or an update from the last known time.

The Cisco LNP Mediation Device connects to the active Cisco BTS 10200 EMS on start up. If the connected EMS fails, the Cisco LNP Mediation Device uses IP aliasing to find the new active EMS and reconnects automatically. If the connection to a Cisco BTS 10200 EMS is lost, data stored in the local database is transferred to the EMS when the connection is restored.

## Configuration Data Backup and Restore

A UNIX command line utility, `dbBackup.sh`, is provided to backup configuration data to a file. A file name for this backup is generated automatically using the current date and time. The default directory used to store the backup files is the directory from which the script is executed. The user can schedule automatic configuration data backups with the UNIX cron jobs.

The `dbRestore.sh` utility can be used to restore configuration data from a backup file. After data restore, the last successful CRD update timestamp is reset on the application server so the next update is a full update.

## Health Status

A UNIX command line tool, `lnpStatus.sh`, indicates whether the web server and database applications are running.

## Throttle Control

The throttling mechanism is a way to control the frequency of transactions sent to the Cisco BTS 10200 Softswitch. The throttle control applies only to the add, edit, and delete commands. The show command is not affected by the throttle control because it does not affect call processing.

The user can enable or disable the throttle control. If it is enabled, the Cisco LNP Mediation Device “sleeps” for 250 milliseconds after each reply from the Cisco BTS 10200 EMS, then sends the next command. The Cisco BTS 10200 EMS also has to populate the IDX database on the Call Agent (CA), so, if the update is a synchronous operation, transactions may take longer and data may need to be buffered.

## SNMP Configuration

The SNMP configuration file can be changed with a UNIX editor such as `vi`; however, you must be logged in as the UNIX super-user to perform this task, and the SNMP daemon must be restarted for changes to take effect.

Standard MIBs are supported by `CIAGENT` from SNMP Research. `CIAGENT` is also used to monitor the web server process. If the web server process terminates, an SNMP trap is raised. Alarms and SNMP traps are also raised for Cisco LNP Mediation Device failures. The Cisco LNP Mediation Device logs all failures to a file.

The following alarms are set:

- Web server failure.
- Failure to connect to the database.
- Failure to connect to CRD.
- Failure to connect to the Cisco BTS 10200 EMS.
- Cisco LNP Mediation Device running with low memory.
- Cisco LNP Mediation Device running out of memory.

A clear alarm and trap is issued when a fault condition is resolved.

## Performance

The Cisco LNP Mediation Device responds within 10 seconds to all web page queries that require access to the local database. The Cisco LNP Mediation Device responds within 60 seconds to operational type queries, such as starting or stopping synchronization updates.

## Major External Interfaces

This section provides additional information on the major external interfaces between the Cisco LNP Mediation Device and other network components. UNIX administrators can login via UNIX shell to install, start, or stop the Cisco LNP Mediation Device. Only SSH access to the system is provided.

### XML/Corba Interface to the Cisco BTS 10200 EMS

All communication between the Cisco LNP Mediation Device and the Cisco BTS 10200 EMS uses XML/CORBA. The Cisco LNP Mediation Device can handle up to 10 Cisco BTS 10200 Softswitches.

### SOAP/HTTPS Interface to the CRD

All interactive communication between the Cisco LNP Mediation Device and the CRD is done through a SOAP/HTTPS interface as defined by the Hungarian CRD. Response messages from the CRD contain a URL referencing a XML file to download. This XML file is parsed to populate the local database.

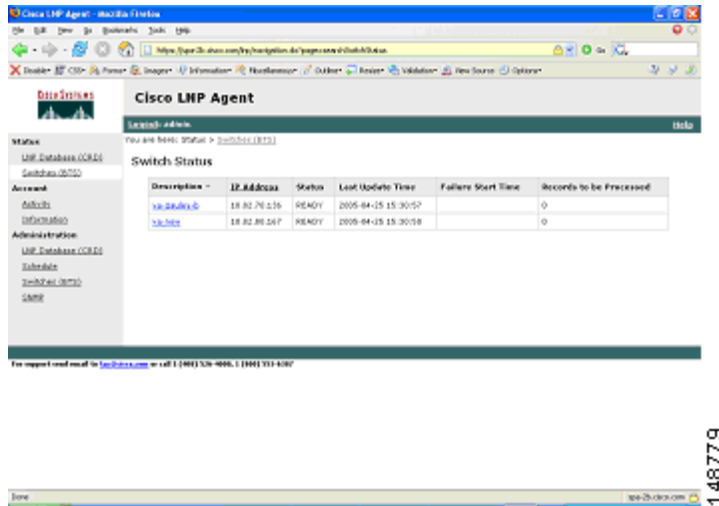
### Cisco LNP Mediation Device GUI

The Cisco LNP Mediation Device graphical user interface (GUI), [Figure 2](#), is a web-based application that users of the system work with to view and update information.

The web-based GUI provides the user tools to:

- Manage system configurations, including BTS connections, CRD connections, and scheduling.
- Monitor system health on status pages.
- Troubleshoot problems on log and history pages.

**Figure 2** Cisco LNP Mediation Device Page



This screen consists of several areas:

- **Title Area** – this contains the logo and application name.
- **Menu Bar** – this contains the logout and help links.
- **Path** – this is the area under the menu bar indicating where the user is within the Cisco LNP Mediation Device.
- **Contents** – this is the area on the left of the page that contains the navigation.
- **Content Area** – this is the area under the breadcrumbs and to the right of the navigation. The content area is driven by what navigation item is currently selected.
- **Footer** – this is the area at the bottom of the page containing a support email and phone number.

The Cisco LNP Mediation Device help file describes the data provided by the Cisco LNP Mediation Device GUI.

## Alarms and SNMP Traps

The following events generate alarms. A clear is generated when the corresponding fault condition is resolved. Alarms and clears are logged in the alarm log file `/opt/SPA/data/logs/alarm.log`.

The SNMP Research Institute **logagt** application is used to monitor the alarm log file. A trap **siLogMatchTrap** is generated for each alarm and clear.

**Table 1** Events and Alarms

Alarm Condition/Value	Alarm Set/Clear Text
Failure to connect to Database	Failed to connect to Database
WEB Server failure	WEB Server is down
Failure to connect to CRD	Failed to connect to CRD
Failure to connect to BTS EMS	Failed to connect to BTS EMS, 10.82.80.167

**Table 1** Events and Alarms (continued)

Alarm Condition/Value	Alarm Set/Clear Text
Application Running Out of Memory	Free memory in web server is exhausted
Application Running with Low Memory	Free memory in web server is running low

In addition to these alarms and traps, **critagt** of CIAgent will generate **critAppDown** and **critAppUp** traps, with **critAppName = jsvc** and **critAppName = mysqld** for the web server process and database process, respectively.

## Mapping Data

Hungarian CRD data is mapped to the Cisco BTS 10200 Softswitch DN2RN table using the mapping in [Table 2](#).

**Table 2** CRD to DN2RN Field Mapping

Hungarian CRD Data Field Name	LNP Mediation Device LNP_DATA Table Field Name	BTS CLI Field Name
Phone_numberStartr	Start_dn and End_dn	DN
Active_provider + equipment	Route_num	RN
valid_from	Valid_from	VALID_FROM
valid_until	Vaid_to	VALID_TO
Startr <sup>1</sup>	Start_dn	FROM_DN
Stopr	End_dn	TO_DN

1. Startr and Stopr fields always come in pairs; they are mutually exclusive with the phone\_number field.

## Purge Expired Data from BTS

Any Cisco BTS 10200 Softswitch DN2RN table entries with a timestamp in the **valid-to** field that is prior to the current time are deleted. The Cisco LNP Mediation Device can delete all expired DN2RN entries on the Cisco BTS 10200 Softswitch with the following command,

```
Delete DN2RN start-time=2000-01-01 00:00:00 end-time=<current-time>
```

This command is sent to the Cisco BTS 10200 Softswitch before each update and every hour when an update is not in progress.

## Installation Procedures

Before installing the Cisco LNP Mediation Device software, do the following:

- Obtain two certificate files from CRD, one for digital signing of SOAP messages and the other for HTTPS communication to the CRD.
- Verify that Solaris 10 is installed and running on your server.

## Cisco LNP Mediation Device Installation

To install and configure the Cisco LNP Mediation Device software, complete the following steps:

- 
- Step 1** Copy the file LNP\_1\_0\_x\_V00.tar.gz (where x is the maintenance release number) to your local machine.
  - Step 2** On your local machine, login as root and enter **gunzip** LNP\_1\_0\_x\_V00.tar.gz
  - Step 3** Then enter **tar xvf** LNP\_1\_0\_x\_V00.tar
  - Step 4** Enter **./install.sh**
  - Step 5** Change the password for spausr to a new password.
  - Step 6** Login as spausr, change the directory to /opt/SPA/data/cert (this step is optional, just to make the next step easier)
  - Step 7** Enter **copy\_certs.sh**
  - Step 8** Enter file name and password for both certificates.  
(Customer will enter his certificate file name and password).
  - Step 9** Start the Cisco LNP Mediation Device application by entering **lnp.sh start**  
You can stop the Cisco LNP Mediation Device application with **lnp.sh stop**
  - Step 10** From your Windows PC, launch your Internet Explorer 6.0 browser and login to <https://your-middleware-host-name/>.

**Note**

Use the Help link in the menu bar of the Cisco LNP Mediation Device for explanations of the GUI screens, the data you must enter, and the information that is displayed.

---