HP Network Node Manager
i-series Smart Plug-in for IP Telephony

For the Windows®, HP-UX, Linux, and Solaris operating systems

Software Version: 8.10

Online Help

Document Release Date: February 2009

Software Release Date: November 2008

HP Network Node Manager

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

For information about third-party license agreements, see the license-agreements directory on the product installation media.

Copyright Notices

Trademark Notices

DOM4J® is a registered trademark of MetaStuff, Ltd.

HP-UX Release 10.20 and later and HP-UX Release 11.00 and later (in both 32 and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95 branded products.

Java™ is a U.S. trademark of Sun Microsystems, Inc.

Microsoft® , Windows®, and Windows® XP are U.S. registered trademarks of Microsoft Corporation.

Oracle® is a registered U.S. trademark of Oracle Corporation, Redwood City, California.

UNIX® is a registered trademark of The Open Group.

Oracle Technology — Notice of Restricted Rights

Table of Contents

HP Network Node Manager i-series Smart Plug-in for IP Telephony

The HP Network Node Manager i-series Smart Plug-in for IP Telephony (**iSPI for IP Telephony**) extends the capability of NNM to monitor and manage the IP telephony infrastructure in your network environment. The iSPI for IP Telephony presents additional views to indicate the states of discovered IP telephony devices and display the overall health of the IP telephony infrastructure.

The iSPI for IP Telephony, in conjunction with NNMi, performs the following tasks:

- Automatically discovering of the IP telephony infrastructure
- Displaying the IP telephony devices in the IP telephony views
- Monitoring the status of every discovered component of the IP telephony infrastructure

After you install (and configure) the iSPI for IP Telephony on the NNMi management server, you can monitor and troubleshoot the problems in your IP telephony infrastructure with the additional views provided by the iSPI for IP Telephony.

Managing IP Telephony Networks

The iSPI for IP Telephony provides you with a complete framework to monitor the IP telephony devices available in your network. You can discover all the available IP telephony devices and topologies with the help of the iSPI for IP Telephony. After installing and configuring the iSPI for IP Telephony, you will be able to perform the following tasks:

- **Monitoring the states of the IP telephony environment**

  The inventory views presented by the iSPI for IP Telephony shows detailed states of every discovered device in tables. You can view the following details of a device:

  - IP address and hostname
  - Version, model, or type of the device
  - Status of the device
- **Monitoring the health of the IP telephony network**

  The IP telephony network consists of several IP telephony devices along with several networking devices and elements. The iSPI for IP Telephony can identify the faults related to IP telephony communication in the network topology that is discovered by NNMi. NNMi, in conjunction with the iSPI for IP Telephony, presents the faults identified in the discovered topology in the network inventory views.
- **Investigating problems and troubleshooting**

  NNMi helps you view the discovered network topology in a graphical format, which assists you in diagnosing the defects in your network. You can view the layer 2 or layer 3 path for every device. You can also view the connectivity status between two or more devices. Each device is represented as a node in these graphs, and the color of each node indicates the status of the device.

Discovering IP Telephony Networks

You can start monitoring all the IP telephony infrastructure after a cycle of polling by the iSPI for IP Telephony. You can install the iSPI for IP Telephony for an IP telephony network that is already being managed by NNMi, or you can configure NNMi to monitor an IP telephony network after the installation of the iSPI for IP Telephony.

If you install the iSPI for IP Telephony on an NNMi management server that is already managing an IP telephony network, the subsequent NNMi discovery prompts the iSPI for IP Telephony to discover the IP telephony devices and topologies. Completion of NNMi's discovery cycle always triggers the discovery of the IP telephony network by the iSPI for IP Telephony. By default, NNMi and iSPI for IP Telephony's discovery schedule is set to 24 hours.

After installing the iSPI for IP Telephony to monitor an IP telephony network that was already being managed by NNMi, you can wait for the next discovery cycle of NNMi, or you can run the Configuration Poll action to discover the IP telephony network immediately.

If you install the iSPI for IP Telephony to monitor a network, which is not already managed by NNMi, you must seed all the IP telephony devices from the NNMi console after installation. Seeding enables NNMi to perform Configuration Poll and triggers a cycle of discovery. In effect, the IP telephony network is discovered at the end of the discovery cycle.

Discover IP phones

Since IP phones are not SNMP-enabled devices, a standard discovery by the iSPI for IP Telephony cannot discover them. To discover IP phones available in your network, you must do the following:

- Seed the access switches to which the IP phones are connected
- Set up auto-discovery rules for IP phones
- Disable ping sweep while setting up auto-discovery for IP phones

The auto-discovery rule discovers the IP telephony network including layer 2 connections between IP phones in the network.

Help for Operators

To perform a basic monitoring of the IP telephony network, you can log on to the NNMi console with the operator (level 1 or 2) or guest credentials. After you log on to the NNMi console, you can view the inventory views introduced by the iSPI for IP Telephony. You can access the views to monitor the status and necessary details for every IP telephony device.

Types of views provided by the iSPI for IP Telephony

View	Purpose
Cisco Call Managers	View the discovered Cisco Unified Communication Manager (CallManager) servers available in the network.
Cisco IP Phones	View the discovered Cisco IP phones available in the network.
Cisco IC Trunks	View the discovered Cisco inter-cluster trunks available in the network.
Cisco Gatekeepers	View the discovered Cisco gatekeeper devices available in the network.
Cisco Voice Gateways	View the discovered Cisco voice gateway devices available in the network.
Nortel Call Servers	View the discovered Nortel Call Servers available in the network.
Nortel Signaling Servers	View the discovered Nortel Signaling Servers available in the network.

View	Purpose
Nortel IP Phones	View the discovered Nortel IP phones available in the network.
Nortel Media Gateways	View the discovered Nortel media gateway devices available in the network.
Nortel QOS Zones	View the QoS zones configured with the Nortel Signaling Server.

In this document, the Cisco Unified Communication Manager server is referred to as the Cisco Call-Manager server.

IP Telephony Inventory

The iSPI for IP Telephony adds two new workspaces to the NNMi console—the **Cisco IP Telephony** and **Nortel IP Telephony** workspaces. You can access all the IP telephony related views from these workspaces. The individual views present device details in tables, and you can launch forms from the views to access the connectivity details.

To launch an IP telephony view:

1. In the Workspaces pane, click **Cisco IP Telephony** or **Nortel IP Telephony**. The IP Telephony tab expands and displays the available IP telephony view.
2. Click the view of your interest. The view appears in the right pane.

Monitoring Cisco IP Phones

The Cisco IP Phones view displays a list of available Cisco IP phones in the network. The view arranges the key attributes of all discovered Cisco IP phones in a table.

To launch the Cisco IP Phones view:

From the **Workspaces** navigation pane, click **Cisco IP Telephony > Cisco IP Phones**. The Cisco IP Phones view opens in the right pane.

Basic Attributes of the Cisco IP Phones Table

Attribute	Description
Registration State	The registration status of the Cisco IP phone with its current controller. Possible values are: ● Registered ● Unregistered ● Unknown ● Rejected ● Partially Registered
Extension Number	The extension number of the IP phone.
Model	The model of the IP phone.

Attribute	Description
Protocol	The protocol supported by the IP phone.
IP Address	The IP address of the IP phone.
Controller	The Cisco CallManager server that controls the IP phone.

When the status of a phone changes to *Unregistered*, the iSPI for IP Telephony sends an incident to the NNMi incident browser.

You can view the details of a single IP phone in a form.

To view the Cisco Extension Details form:

In the Cisco IP Phones view, select the node of your interest, and then click . The Cisco Extension Details form opens.

To view the Node Form for the IP phone, click , and then click **Open**. The Node Form opens displaying the details of the IP phone.

Filtering Cisco IP phones

You can filter the listed IP phones in the Cisco IP Phones view with the available filters. You can perform the filtering action only on the Registration State, Extension Number, IP Address, and Controller columns.

To filter the Cisco IP Phones view:

Note: You can use only the *Equals this value* and *Not equal to this value* filters for the Registration State column.

1. Right-click the **Registration State**, **Extension Number**, **IP Address**, or **Controller** attribute of one of the IP phones listed in the Cisco IP Phones view.
2. Select one of the following filters:
   Note: You can use only the *Equals this value* and *Not equal to this value* filters for the Registration State column.
   - Equals this value
   - Contains string
   - Starts with string
   - Matches string
   - Is not empty
   - Is empty
   - Not equal to this value

     The filtered list of Cisco IP phones appears in the view.

Note: After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

Cisco Extension Details form

The Cisco Extension Details form helps you view the node details of the selected Cisco IP phone and the Cisco CallManager servers associated with it. The form presents two different panes.

The right pane lists the following details:

- Associated Cisco CallManagers: The Associated Call Managers tab displays the details of the Cisco CallManager server that currently controls the selected Cisco IP phone. The tab displays the details of the Cisco CallManager in the format presented in the Cisco Call Manager view.
- Previous Cisco CallManagers: The Previous Call Managers tab displays the details of the Cisco CallManager server that was previously controlling the selected Cisco IP phone. The tab displays the details of the Cisco CallManager in the format presented in the Cisco Call Manager view.

The left pane lists the following details of the selected Cisco IP phone:

Basic Attributes of the Selected Cisco IP Phone

Attribute	Description
Name	The name of the Cisco IP phone.
Hosted Node	The hostname of the Cisco IP phone.
IP Address	The IP address of the Cisco IP phone.
MAC Address	The MAC address of the Cisco IP phone.
Description	A short description of the phone.
Model	The model of the phone.
Protocol	The protocol used by the phone.

Monitoring Cisco CallManagers

The Cisco Call Managers view displays a list of available Cisco CallManager servers in the network. The view arranges the key attributes of all the discovered Cisco CallManager servers in a table.

To launch the Cisco Call Managers view:

From the **Workspaces** navigation pane, click **Cisco IP Telephony >Cisco Call Managers**. The Cisco Call Managers view opens in the right pane.

Basic Attributes of the Cisco Call Managers Table

Attribute	Description
Status	The Status of the Cisco CallManager server. Possible values are: ● Normal—indicates the server is UP. ● Critical—indicates the server is DOWN. ● No Status—this is indicated before the first polling cycle takes place. ● Unknown—indicates no SNMP, which indicates the state of the server, is available from the node.

Attribute	Description
Name	The hostname of the Cisco CallManager server.
IP Address	The IP address of the Cisco CallManager server.
Version	The version of the server.
Description	A short description of the server.
Cluster	The name of the cluster to which the Cisco CallManager server belongs.

You can view the details of a single CallManager server in a form.

To view the CallManager form:

In the Cisco Call Managers view, select the node of your interest, and then click . The Cisco Call Managers form opens.

To view the Node Form for the CallManager server, click , and then click **Open**. The Node Form opens displaying the details of the CallManager server.

Cisco Call Manager form

The Cisco Call Manager form helps you view the node details of the selected Cisco CallManager server and the gatekeepers and IP phones associated with it. The form presents two different panes.

The right pane lists the following details:

- Associated gatekeepers: The Associated Gatekeepers tab displays the details of all the gatekeepers associated with the selected Cisco CallManager server. The tab displays the details of every associated gatekeeper in the format presented in the Cisco Gatekeepers view.
- Associated IP phones: The Associated Extensions tab displays the details of all the IP phones associated with the selected Cisco CallManager server. The tab displays the details of every associated IP phone in the format presented in the Cisco IP Phones view.

The left pane lists the following details of the selected Cisco CallManager server:

Basic Attributes of the Selected Cisco Call Manager Server

Attribute	Description
Hosted Node	The hostname of the Cisco CallManager node.
Name	The name of the Cisco CallManager server.
IP Address	The IP address of the Cisco CallManager server.
Version	The version of the server.
Description	A short description of the server.
Cluster	The name of the cluster to which the Cisco CallManager server belongs.

Monitoring Call Details Record

The iSPI for IP Telephony can read the Call Details Record (CDR) of the Cisco CallManager CDR Repository server and can collect the values of Quality of Service (QoS) metrics. After you configure the iSPI to read the QoS metrics from CDR, iSPI polls the QoS metric data and compares with threshold values set by you. In the event of threshold violation, the iSPI for IP Telephony sends incidents to the NNMi incident browser.

To configure the iSPI for IP Telephony to monitor QoS metrics from Cisco CallManager CDR, you must log on to the NNMi console with an administrative privileges. See Configuring the iSPI for IP Telephony to Monitor Cisco CallManager Call Detail Records for more information.

Monitoring Cisco IC Trunks

The Cisco IC Trunks view displays a list of available Cisco intercluster trunks in the network. The view arranges the key attributes of all the intercluster trunks in a table.

To launch the Cisco IC Trunks view

From the **Workspaces** navigation pane, click **Cisco IP Telephony > Cisco IC Trunks**. The Cisco IC Trunks view opens in the right pane.

Basic Attributes of the Cisco IC Trunks Table

Attribute	Description
Name	The name of the Cisco intercluster trunk.
Hosted On	The name of the Cisco CallManager server that hosts the intercluster trunk.
Type	Type of the intercluster trunk. This field indicates if the intercluster trunk is gatekeeper-controlled or not.
Remote CM List	The list of Cisco CallManager servers that are connected to the intercluster trunk (for non-gatekeeper-controlled intercluster trunk).
Gatekeeper	The IP address of the gatekeeper device that controls the intercluster trunk. If the intercluster trunk is not controlled by a gatekeeper, the field remains blank.
Registration Status	The registration status of the intercluster trunk. Possible values are: ● Registered ● Unregistered ● Rejected ● Unknown ● Not Applicable (for non-gatekeeper-controlled intercluster trunks)

The iSPI for IP Telephony retrieves the registration state of only gatekeeper-controlled intercluster trunks. When the state of an intercluster trunk becomes *Rejected* or *Unregistered*, the iSPI for IP Telephony sends an incident to the NNMi incident browser.

You can view the details of a single Cisco intercluster trunk within a form.

To view the H323 Trunk form:

In the Cisco IC Trunks view, select the node of your interest, and then click . The H323 Trunk form opens.

To view the Node Form for the intercluster trunk, click , and then click **Open**. The Node Form opens displaying the details of the IC trunk.

H323 Trunk form

The H323 Trunk form helps you view the node details of the selected Cisco IC trunk and the gatekeepers associated with the trunk. The form presents two different panes.

The right pane lists the following details:

Controlling gatekeepers: The Controlling Gatekeepers tab displays the details of the gatekeeper device that controls the intercluster trunk. The tab displays the details of the gatekeeper in the format presented in the Cisco Gatekeepers view.

The left pane lists the following details of the selected Cisco intercluster trunk:

Basic Attributes of the Selected Cisco IC Trunk

Attribute	Description
Hosted Node	The name of the Cisco CallManager server that hosts the intercluster trunk.
Name	The name of the Cisco intercluster trunk.
Type	Type of the Cisco intercluster trunk.
Remote CM List	The list of Cisco CallManager servers that are connected to the intercluster trunk.
Gatekeeper	The IP address of the gatekeeper device that controls the intercluster trunk.

Monitoring Cisco Gatekeepers

The Cisco Gatekeepers view displays a list of available Cisco gatekeeper devices in the network. The view arranges the key attributes of all gatekeepers in a table.

To launch the Cisco Gatekeepers view

From the **Workspaces** navigation pane, click **Cisco IP Telephony > Cisco Gatekeepers**. The Cisco Gatekeepers view opens in the right pane.

Basic Attributes of the Cisco Gatekeepers Table

Attribute	Description
Hosted Node	The hostname of the Cisco gatekeeper device.
IP Address	The IP address of the interface on the gatekeeper that communicates with other endpoints and gateways in the network.
H323Endpoints	The number of endpoints associated with the gatekeeper.

You can view the details of a single Cisco gatekeeper in a form, which you can launch from the Cisco Gatekeepers view.

To view the Cisco Gatekeepers form:

In the Cisco Gatekeepers view, select the node of your interest, and then click . The Cisco Gatekeepers form opens. The Cisco Gatekeepers form displays details of the selected gatekeeper in the left pane, and details of all the associated Cisco CallManagers in the right pane.

To view the Node Form for the gatekeeper, click , and then click **Open**. The Node Form opens displaying the details of the gatekeeper.

Cisco GateKeeper form

The Cisco GateKeeper form helps you view the node details of the selected Cisco gatekeeper device and the Cisco CallManager servers associated with it. The form presents two different panes.

The right pane lists the following details:

Associated Cisco CallManagers: The Associated Call Managers tab displays the details of all the Cisco CallManager servers associated with the selected gatekeeper device. The tab displays the details of every associated CallManager in the format presented in the Cisco Call Manager view.

The left pane lists the following details of the selected Cisco gatekeeper device:

Basic Attributes of the Selected Cisco Gatekeeper Device

Attribute	Description
Hosted Node	The hostname of the gatekeeper.
IP Address	The IP address of the gatekeeper interface.
Description	A short description of the device.
Model	Model of the device.
H323 Endpoints	Number of H323 endpoints associated with the gatekeeper.

Monitoring Cisco Voice Gateways

The Cisco Voice Gateways view displays a list of available Cisco voice gateway devices in the network. The view arranges the key attributes of all discovered Cisco voice gateway devices in a table.

To launch the Cisco Voice Gateways view

From the **Workspaces** navigation pane, click **Cisco IP Telephony > Cisco Voice Gateways**. The Cisco Voice Gateways view opens in the right pane.

Basic Attributes of the Cisco Voice Gateway Table

Attribute	Description
Hosted Node	The hostname of the router on which the Cisco voice gateway device runs.
IP Address	The IP address of the Cisco voice gateway device.

Attribute	Description
Protocol	The protocol used by the gateway device.
Call Server	The fully-qualified domain name of the Cisco CallManager device to which the voice gateway device is configured.
Operational State	The status of the Cisco voice gateway device. Possible values are: ● No Status—the first polling cycle to collect the operational state has not taken place. ● Normal—states of all associated circuit-switched interfaces with the voice gateway device are normal. ● Unknown—states of all associated circuit-switched interfaces with the voice gateway device are unknown. ● Warning—state of at least one associated circuit-switched interface is unknown; no associated circuit-switched interface is in the critical condition. ● Minor—state of at least one (but not every) associated circuit-switched interface is critical. ● Critical—state of every associated circuit-switched interface is critical. ● Node Down—state of the voice gateway device is critical.
Description	A description of the voice gateway device.

Viewing Cisco Voice Gateway Endpoints

You can launch the Node form from the Cisco Voice Gateway view to view the endpoint details of a Cisco Voice Gateway device. The node form for a Cisco Voice Gateway device includes an additional tab—the **Circuit Switched Interfaces** tab. The Circuit Switched Interfaces tab arranges all the key attributes of all the endpoints of the Cisco Gateway device in a table.

To launch the Node form for a Cisco Voice Gateways device

1. From the **Workspaces** navigation pane, click **IP Telephony > Cisco Voice Gateways**. The Cisco Voice Gateways view opens in the right pane.
2. In the right pane, click within the row representing the Voice Gateway device of your interest. The Node form for the Cisco Voice Gateway device opens.

Alternatively, follow these steps:

1. From the **Workspaces** navigation pane, click **Inventory > Nodes**. The Nodes view opens in the right pane. The Nodes view represents all the Cisco Voice Gateway devices (discovered by the iSPI for IP Telephony) as nodes.
2. In the right pane, click within the row representing the Voice Gateway device of your interest. The Node form for the Cisco Voice Gateway device opens.

After you launch the Node form for the Cisco Voice Gateway device, view the details of all the endpoints from the Circuit Switched Interfaces tab.

Node Form: Circuit Switched Interfaces Tab

The Circuit Switched Interfaces tab lists the key attributes of the endpoints of the Cisco Voice Gateway device.

Basic Attributes of the Circuit Switched Interfaces Tab

Attribute	Description
Name	The hostname of the endpoint.
Interface	Details of the interface detected by NNMi.
Type	The type of the endpoint. Possible values are:
Operational State	This field indicates the operational state of the endpoint. Possible values are: ● Up ● Down ● Testing ● Unknown ● Dormant ● Not Present ● Lower Layer Down
Usage State	The usage status of the endpoint. This state is not applicable for non-DS1 interfaces. Possible values are: ● Idle— if all channels associated with the interface are idle. ● In-use—if all channels associated with the interface are in use. ● Partially in-use—if at least one interface is in use (not all the interfaces are in use).
Registration State	Indicates if the endpoint is registered with a Cisco CallManager. This state is applicable only for interfaces with the Media Gateway Control Protocol (MGCP). Possible values are: ● Unknown ● Registered ● Unregistered ● Rejected ● Partially Registered

Viewing Cisco Voice Gateway Endpoint Channels

You can launch a Node form from the Circuit Switched Interfaces tab to view the channel details of an endpoint of a Cisco Voice Gateway device. This node form includes an additional tab—the **Circuit Switched Channels** tab. The Circuit Switched Channels tab arranges all the key attributes of all the channels of the Cisco Gateway device endpoint in a table.

To launch the Node form to view endpoint channel details of a Cisco Voice Gateway device

1. From the **Workspaces** navigation pane, click **IP Telephony > Cisco Voice Gateways**. The Cisco Voice Gateways view opens in the right pane.

2. In the right pane, click within the row representing the Voice Gateway device of your interest. The Node form for the Cisco Voice Gateway device opens.
3. In this form, go to the Circuit Switched Interfaces tab. You can view a list of discovered endpoints.
4. Click within the row representing the endpoint of your interest. The Node form opens. To view the channel details, click the **Circuit Switched Channels** tab.

Alternatively, follow these steps:

1. From the **Workspaces** navigation pane, click **Inventory > Nodes**. The Nodes view opens in the right pane. The Nodes view represents all the Cisco Voice Gateway devices (discovered by the iSPI for IP Telephony) as nodes along with the other general nodes.
2. In the right pane, click within the row representing the Voice Gateway device of your interest. The Node form for the Cisco Voice Gateway device opens.
3. In this form, go to the Circuit Switched Interfaces tab. You can view a list of discovered endpoints.
4. Click within the row representing the endpoint of your interest. The Node form opens. To view the channel details, click the **Circuit Switched Channels** tab.

Node Form: Circuit Switched Channels Tab

The Circuit Switched Channels tab lists the key attributes of the channels (DS0) associated with the endpoints of the Cisco Voice Gateway device.

Basic Attributes of the Circuit Switched Channels Tab

Attribute	Description
Name	The name of the channel.
Interface	The name of the associated interface.
Type	The type of the channel.
Operational Status	The operational status of the channel. Possible values are: ● Up ● Down ● Testing ● Unknown ● Dormant ● Not present ● Lower layer down
Usage Status	The usage status of the channel. Possible values are: ● In-use ● Idle ● Unknown ● Not-polled
In Use	Indicates if the channel was in use during the configured hold time. The hold time is the period for which the iSPI for IP Telephony waits before changing the *usage status* of the circuit-switched channel to *Idle*. Possible values are: ● Yes ● No

Monitoring Nortel Call Servers

The Nortel Call Servers view displays a list of available Nortel Call Servers in the network. The view arranges the key attributes of all discovered Nortel Call Servers in a table.

To launch the Nortel Call Servers view

From the **Workspaces** navigation pane, click **Nortel IP Telephony > Nortel Call Servers**. The Nortel Call Servers view opens in the right pane.

Basic Attributes of the Nortel Call Servers Table

Attribute	Description
Node Status	The status of the Nortel Call Server. Possible values are: ● No Status ● Normal ● Disabled

Attribute	Description
	● Warning ● Minor ● Major ● Critical ● Unknown
Name	The system name of the Nortel Call Server.
IP Address	The IP address of the Nortel Call Server.
Model	The model of the Nortel Call Server.
Version	Version of the Nortel Call Server.
Description	A description of the Nortel Call Server.

View the Nortel Call Server form

You can view the details of a single Nortel Call Server in a form, which you can launch from the Nortel Call Servers view.

To view the Nortel Call Server form:

In the Nortel Call Servers view, select the node of your interest, and then click . The Nortel Call Server form opens. The Nortel Call Server form displays details of the selected server in the left pane, and details of all the associated Nortel Signaling Servers in the right pane.

To view the Node Form for the Nortel Call Server, click , and then click **Open**. The Node Form opens displaying the details of the server.

Nortel Call Server form

The Nortel Call Server form helps you view the node details of the selected Nortel Call Server and the Signaling Servers and IP phones associated with it. The form presents two different panes.

The right pane lists the following details:

- Associated Signaling Servers: The Associated Signaling Servers tab displays the details of all the Signaling Servers associated with the selected server. The tab displays the details of every associated Signaling Servers in the format presented in the Nortel Signal Servers view.
- Associated IP phones: The Associated Extensions tab displays the details of all the IP phones associated with the selected Nortel Call Server. The tab displays the details of every associated IP phone in the format presented in the Nortel IP Phones view.

The left pane lists the following details of the selected Nortel Call Server:

Basic Attributes of the Selected Nortel Call Server

Attribute	Description
Hosted Node	The hostname of the Nortel Call Server node.
Name	The name of the Nortel Call Server.
IP Address	The IP address of the Nortel Call Server.

Attribute	Description
Description	A short description of the server.
Version	The version of the server.
ELAN IP	IP address of the interface that is connected to the ELAN where the Nortel Call Server belongs.
Model	Model of the Nortel Call Server.

Monitor Nortel Signaling Servers

The Nortel Signaling Servers view displays a list of available Nortel Signaling Servers in the network. The view arranges the key attributes of all discovered Nortel Signaling Servers in a table.

To launch the Nortel Signaling Servers view

From the **Workspaces** navigation pane, click **Nortel IP Telephony > Nortel Signaling Servers**. The Nortel Signaling Servers view opens in the right pane.

Basic Attributes of the Nortel Signaling Servers Table

Attribute	Description
Node Status	The status of the Nortel Signaling Server. Possible values are: ● No Status ● Normal ● Disabled ● Warning ● Minor ● Major ● Critical ● Unknown
Name	The fully-qualified domain name of the Nortel Signaling Server.
IP Address	The IP address of the Nortel Signaling Server.
Description	Description of the Nortel Signaling Server.
Model	The model of the Nortel Signaling Server.
Version	Version of the Nortel Signaling Server.
Call Server	The associated Nortel Call Servers.

View the Nortel Signaling Server form

You can view the details of a single Nortel Signaling Server in a form, which you can launch from the Nortel Signaling Servers view.

To view the Nortel Signaling Server form:

In the Nortel Signaling Servers view, select the node of your interest, and then click . The Nortel Signaling Server form opens. The Nortel Signaling Server form displays details of the selected signaling server in the left pane, and details of all the associated Nortel Call Servers in the right pane.

To view the Node Form for the Nortel Signaling Server, click , and then click **Open**. The Node Form opens displaying the details of the server.

Nortel Signaling Server form

The Nortel Signaling Server form helps you view the node details of the selected Nortel Signaling Server and the Nortel Call Servers and QOS Zones associated with it. The form presents two different panes.

The right pane lists the following details:

- Associated CallServers: The Associated CallServers tab displays the details of all the Nortel Call Servers associated with the selected server. The tab displays the details of every associated Nortel Call Servers in the format presented in the Nortel Call Servers view.
- Associated QOS Zones: The Associated QOS Zones tab displays the details of all the QoS zones configured with the selected Nortel Signal Server. The tab displays the details of every associated QoS zone in the format presented in the Nortel QOS Zone Table view.

The left pane lists the following details of the selected Nortel Signaling Server:

Basic Attributes of the Selected Nortel Signaling Server

Attribute	Description
Hosted Node	The hostname of the Nortel Signaling Server node.
Name	The name of the Nortel Signaling Server.
IP Address	The IP address of the Nortel Signaling Server detected by NNMi.
Version	The version of the server.
Description	A short description of the server.
Model	Model of the Nortel Signaling Server.
ELANIpAddress	IP address of the interface that is connected to the ELAN where the Nortel Signaling Server belongs.
HostIpAddress	All the IP addresses of the Nortel Signaling Server.

Nortel IP Phones View

The Nortel IP Phones view displays a list of available Nortel IP phones in the network. The view arranges the key attributes of all discovered Nortel IP phones in a table.

To launch the Nortel IP Phones view

From the **Workspaces** navigation pane, click **Nortel IP Telephony > Nortel IP Phones**. The Nortel IP Phones view opens in the right pane.

Basic Attributes of the Nortel IP Phones Table

Attribute	Description
Extension Number	The extension number of the IP phone.
Name	The name of the IP phone.
Model	The model of the IP phone.
Controller	The fully-qualified domain name or IP address of the Nortel Call Server to which the IP phone belongs.
Description	A description of the IP phone.

View the Nortel Phone Detailed form

You can view the details of a single Nortel IP phone in a form, which you can launch from the Nortel IP Phones view.

To view the Nortel Phone Detailed form:

In the Nortel IP Phones view, select the node of your interest, and then click . The Nortel Phone Detailed form opens. The Nortel Phone Detailed form displays details of the selected phone in the left pane, and details of the associated Nortel Call Server in the right pane.

To view the Node Form for the Nortel IP phone, click , and then click **Open**. The Node Form opens displaying the details of the phone.

Nortel Phone Detailed form

The Nortel Phone Detailed form helps you view the node details of the selected IP phone and the Nortel Call servers associated with it. The form presents two different panes.

The right pane lists the following details:

Associated CallServers: The Associated CallServers tab displays the details of the Nortel Call server associated with the selected IP phone. The tab displays the details of the associated Nortel Call Server in the format presented in the Nortel Call Server view.

The left pane lists the following details of the selected Nortel IP phone:

Basic Attributes of the Selected Nortel IP Phone

Attribute	Description
Name	The name of the Nortel IP phone.
Extension Number	Extension number of the phone.
Description	A short description of the phone.
Model	The model of the phone.
Vendor	Nortel
Controller	The IP address of the Nortel Call Server that controls the phone.

Monitoring Nortel media gateways

The Nortel Media Gateways view displays a list of available Nortel media gateway devices in the network. The view arranges the key attributes of all discovered Nortel media gateway devices in a table.

To launch the Nortel Media Gateways view

From the **Workspaces** navigation pane, click **Nortel IP Telephony > Nortel Media Gateways**. The Nortel Media Gateways view opens in the right pane.

Basic Attributes of the Nortel Media Gateways Table

Attribute	Description
IP Address	The IP address of the Nortel media gateway device.
Type	The type of the Nortel media gateway device. Possible types are: Voice Gateway Media Card (**VGMC**) and Media Gateway Controller (**MGC**).
Call Server	The fully-qualified domain name of the CS1000 server to which the gateway device is configured.
Protocol	The protocol used by the gateway device.
Description	A description of the media gateway device.

View the Nortel Media Gateway form

You can view the details of a single Nortel media gateway in a form, which you can launch from the Nortel Media Gateways view.

To view the Nortel Media Gateway form:

In the Nortel Media Gateways view, select the node of your interest, and then click . The Nortel Media Gateway form opens. The Nortel Media Gateway form displays details of the selected gateway in the left pane, and details of all the associated Nortel Call Servers in the right pane.

To view the Node Form for the media gateway, click , and then click **Open**. The Node Form opens displaying the details of the gateway.

View the Nortel Media Gateway form

The Nortel Media Gateway form helps you view the node details of the selected Nortel media gateway and the Nortel Call servers associated with it. The form presents two different panes.

The right pane lists the following details:

Associated CallServers: The Associated CallServers tab displays the details of all the Nortel Call servers associated with the selected media gateway. The tab displays the details of every associated Call Server in the format presented in the Nortel Call Server view.

The left pane lists the following details of the selected Nortel media gateway:

Basic Attributes of the Selected Nortel Media Gateway

Attribute	Description
Hosted Node	Hostname of the media gateway.
Name	The name of the media gateway.
Model	The model of the media gateway.
Description	A short description of the media gateway.
Model	The model of the phone.
Vendor	Nortel
ELAN IP	IP address of the interface that is connected to the ELAN where the gateway belongs.
TLAN IP	IP address of the interface that is connected to the TLAN where the gateway belongs.

Nortel QOS Zones Table View

The Nortel QOS Zones table view displays the QoS metrics of all the configured QoS zones on a Nortel Signaling Server. The view arranges the QoS metrics in a table.

To launch the Nortel QOS Zones table view

From the **Workspaces** navigation pane, click **Nortel IP Telephony > Nortel QOS Zones**. The Nortel QOS Zones table view opens in the right pane.

Basic Attributes of the Nortel QOS Zones Table

Attribute	Description
QOS Zone ID	The ID of a QoS zone.
Name	The name of the QoS zone. The name is formed using the IP address of the Nortel Signaling Server and the QoS Zone number.
Signaling Server IP Address	The IP address of the Signaling Server on which the QOS zone was configured.

View the Nortel QOS Zone Details form

You can view the details of QOS zones in a form, which you can launch from the Nortel QOS Zones Table view.

To view the Nortel QOS Zone Details form:

In the Nortel QOS Zones table view, select the node of your interest, and then click . The Nortel QOS Zone Details form opens. The Nortel QOS Zone Details form displays details of the QoS zone in the left pane, and details of set parameters in the right pane.

View the Nortel QOS Zone Details form

The Nortel QOS Zone Details form includes the details of a particular QoS zone that was configured on a Nortel Signaling Server.

The left pane lists the following details:

- QOS Zone ID
- Name of the QoS zone
- IP address of the Signaling Server where the QoS zone was configured.

The right pane introduces two tabs—**Intra Zone QOS Parameters** and **Inter Zone QOS Parameters**.

The Intra Zone QOS parameter tab presents you the following metrics:

Basic Attributes of the Intra Zone QOS Parameters tab

Attribute	Description
CallsMadeIn	The number of calls made successfully within the selected zone.
CallsBlockedIn	The number of calls blocked within the selected zone.
PeakIn	The percentage peak bandwidth within the selected zone.
AvgIn	The percentage average bandwidth within the selected zone.
InThrViol	Violation of bandwidth-usage threshold within the selected zone.
IntervalIn	The number of measuring-interval samples within the selected zone.
UnacpLatencyIn	The number of unacceptable latency samples within the selected zone.
UnacpPacketLossIn	The number of unacceptable packet loss within the selected zone.
UnacpJitterIn	The number of unacceptable jitter samples within the selected zone.
UnacpRFactorIn	The number of unacceptable R-factor samples within the selected zone.
UnacpEchoRLossIn	The number of unacceptable Echo Return Loss within the selected zone.
WarnLatencyIn	The number of warning latency samples within the selected zone.
WarnJitterIn	The number of warning jitter samples within the selected zone.
WarnPacketLossIn	The number of warning packet-loss samples within the selected zone.
WarnRFactorIn	The number of warning R-factor samples within the selected zone.
WarnEchoRLossIn	The number of warning Echo Return Loss within the selected zone.

The Inter Zone QOS parameter tab presents you the following metrics:

Basic Attributes of the Inter Zone QOS Parameters tab

Attribute	Description
CallsMadeOut	The number of calls made successfully within different zones.
CallsBlockedOut	The number of calls blocked within different zones.

Attribute	Description
PeakOut	The percentage peak bandwidth within different zones.
AvgOut	The percentage average bandwidth within different zones.
OutThrViol	Violation of bandwidth-usage threshold within different zones.
IntervalOut	The number of measuring-interval samples within different zones.
UnacpLatencyOut	The number of unacceptable latency samples within different zones.
UnacpPacketLossOut	The number of unacceptable packet loss within different zones.
UnacpJitterOut	The number of unacceptable jitter samples within different zones.
UnacpRFactorOut	The number of unacceptable R-factor samples within different zones.
UnacpEchoRLossOut	The number of unacceptable Echo Return Loss within different zones.
WarnLatencyOut	The number of warning latency samples within different zones.
WarnJitterOut	The number of warning jitter samples within different zones.
WarnPacketLossOut	The number of warning packet-loss samples within different zones.
WarnRFactorOut	The number of warning R-factor samples within different zones.
WarnEchoRLossOut	The number of warning Echo Return Loss within different zones.

In this form, you can view the following details:

- Value of a QoS metric
- The threshold set for the metric
- If the metric value has violated the set threshold

If you want to set the thresholds for these metrics, you must log on to the NNMi console with an administrative or operator level 2 privileges.

For more information to set thresholds for Nortel QoS zone metrics, see Set thresholds for Nortel QoS metrics.

Incidents generated by the iSPI for IP Telephony

When specific events occur in the IP telephony environment, the iSPI for IP Telephony sends incidents with appropriate messages to the NNMi incident view.

Incidents Generated by the iSPI for IP Telephony

Incident	Message	Severity	Description
LowQOSCall	Low QOS Call: SRC Phone IP:$origMediaIPAddress Extn:$getCallingPartyNumber DEST Phone IP:$d-	Critical	This incident indicates a low voice quality call between two given phones, along with their extension and IP address details, cluster-Id of

Incident	Message	Severity	Description
	estIPAddress Extn:$-finalCalledPartyNumber Cluster:$getGlobalCallId_ClusterId Jitter:$jitter Latency:$latency MOS:$avgMLQK		the source phone, and QoS details (such as Jitter, Latency, and average MOS).
CiscoCktSwitchedIFStatusIdle	Cisco Ckt Switched interface changed usage status to idle. Gateway ipaddress : $gwIPAddress	Warning	This incident indicates that the usage state of a circuit switched interface i.e. the endpoint hosted on a voice gateway has changed to idle. The usage state of an endpoint is computed by considering the usage state of the bearer channels for the endpoint.
CiscoCktSwitchedIFOperStatusDown	The operational state of a Cisco Ckt Switched interface has changed to critical. Gateway ipaddress : $gwIPAddress	Critical	This incident indicates that the operational state of a circuit switched interface (endpoint) hosted on a voice gateway has changed from up to down. The operational state of an endpoint is computed by considering the operational states of the endpoint and bearer channels for the endpoint.
CiscoCktSwitchedChannelStatusIdle	Cisco Circuit Switched Channel changed usage status to Idle.	Critical	This incident indicates that a Cisco circuit switched channel has reported that its usage status is now idle.
CiscoCktSwitchedChannelOperStatusDown	The operation state of a Cisco Ckt Switched channel has changed to critical.	Critical	This incident indicates that the operational state of a circuit switched channel has changed to down.
CiscoCallManagerStatusDown	Call Manager Down. IP: $ip Cluster: $cluster	Critical	Call Manager Down.

Incident	Message	Severity	Description
CiscoCktSwitchedIFRegnStatusUnReg	The registration state of a Cisco Ckt Switched interface has changed to critical. Gateway ipaddress : $gwIPAddress	Critical	This incident indicates that the registration state of a circuit switched interface (endpoint) hosted on a voice gateway has changed from registered to unregistered.
CiscoCktSwitchedIFRegnStatusRejected	The registration state of a Cisco Ckt Switched interface has changed to critical. Gateway ipaddress : $gwIPAddress	Critical	This incident indicates that the registration state of a circuit switched interface (endpoint) hosted on a voice gateway has changed to rejected. It happens when a call manager rejects an interface register request.
CiscoPhoneUnRegistered	Cisco Phone Unregistered from CallManager.	Minor	Cisco Phone Unregistered from a Cisco CallManager.
CiscoPhoneUnknown	Cisco Phone registration status is not known	Minor	Cisco Phone registration status is not known.
CiscoPhonePartiallyRegistered	Cisco Phone has some extensions unregistered.	Warning	Cisco Phone has some extensions unregistered.
CiscoGkControlledICTStatusRejected	The Gatekeeper-Controlled Inter-Cluster Trunk has changed its registration state to Rejected. Call Manager IP: $cmIPAddress	Critical	This incident is generated whenever a Gatekeeper-Controlled Inter-Cluster Trunk's registration request is rejected by a Cisco CallManager.
CiscoGkControlledICTStatusUnRegd	The Gatekeeper-Controlled Inter-Cluster Trunk has changed its registration state to UnRegistered.	Critical	This incident is generated when ever a Gatekeeper-Controlled Inter-Cluster Trunk un registers with a call manager.
CiscoVgwStatusCritical	Cisco Voice Gateway Status is Critical. Gateway IP Address: $ipAddress	Critical	Cisco Voice Gateway Status is Critical.

Incident	Message	Severity	Description
CiscoVgwStatusWarning	Cisco Voice Gateway Status is Warning. Gateway IP Address: $ipAddress	Warning	Cisco Voice Gateway Status is Warning.
CiscoVgwStatusMinor	Cisco Voice Gateway Status is Minor. Gateway IP Address: $ipAddress	Minor	Cisco Voice Gateway Status is Minor.
callsMadeInViolation	The Intra QOS Zone callsMadeIn parameter has violated set threshold value.	Critical	The Intra QOS Zone callsMadeIn parameter has violated set threshold value.
callsMadeOutViolation	The Inter QOS Zone callsMadeOut parameter has violated set threshold value.	Critical	The Inter QOS Zone callsMadeOut parameter has violated set threshold value.
callsBlockedOutViolated	The Inter QOS Zone callsBlockedOut parameter has violated set threshold value.	Critical	The Inter QOS Zone callsBlockedOut parameter has violated set threshold value.
callsPeakInViolated	The Intra QOS Zone peakIn parameter has violated set threshold value.	Critical	The Intra QOS Zone peakIn parameter has violated set threshold value.
callsBlockedInViolated	The Intra QOS Zone callsBlockedIn parameter has violated set threshold value.	Critical	The Intra QOS Zone callsBlockedIn parameter has violated set threshold value.
callsPeakOutViolated	The Inter QOS Zone peackOut parameter has violated set threshold value.	Critical	The Inter QOS Zone peackOut parameter has violated set threshold value.
inThrViolViolated	The Intra QOS Zone inThrViol parameter has violated set threshold value	Critical	The Intra QOS Zone inThrViol parameter has violated set threshold value.
outThrViolViolated	The Inter QOS Zone outThrViol parameter has violated set threshold value.	Critical	The Inter QOS Zone outThrViol parameter has violated set threshold value.
avgInViolated	The Intra QOS Zone avgIn parameter has violated set threshold value.	Critical	The Intra QOS Zone avgIn parameter has violated set threshold value.

Incident	Message	Severity	Description
avgOutViolated	The Inter QOS Zone avgOut parameter has violated set threshold value.	Critical	The Inter QOS Zone avgOut parameter has violated set threshold value.
unacpLatencyInViolated	The Intra QOS Zone unacpLatencyIn parameter has violated set threshold value.	Critical	The Intra QOS Zone unacpLatencyIn parameter has violated set threshold value.
intervalOutViolated	The Inter QOS Zone intervalOut parameter has violated set threshold value.	Critical	The Inter QOS Zone intervalOut parameter has violated set threshold value.
intervalInViolated	The Intra QOS Zone intervalIn parameter has violated set threshold value.	Critical	The Intra QOS Zone intervalIn parameter has violated set threshold value.
unacpLatencyOutViolated	The Inter QOS Zone unacpLatencyOut parameter has violated set threshold value.	Critical	The Inter QOS Zone unacpLatencyOut parameter has violated set threshold value.
unacpPacketLossInViolated	The Intra QOS Zone unacpPacketLossIn parameter has violated set threshold value.	Critical	The Intra QOS Zone unacpPacketLossIn parameter has violated set threshold value.
unacpPacketLossOutViolated	The Inter QOS Zone unacpPacketLossOut parameter has violated set threshold value.	Critical	The Inter QOS Zone unacpPacketLossOut parameter has violated set threshold value.
unacpRFactorInViolated	The Intra QOS Zone unacpRFactorIn parameter has violated set threshold value.	Critical	The Intra QOS Zone unacpRFactorIn parameter has violated set threshold value.
unacpJitterOutViolated	The Inter QOS Zone unacpJitterOut parameter has violated set threshold value.	Critical	The Inter QOS Zone unacpJitterOut parameter has violated set threshold value.
unacpJitterInViolated	The Intra QOS Zone unacpJitterIn parameter has violated set threshold value.	Critical	The Intra QOS Zone unacpJitterIn parameter has violated set threshold value.

Incident	Message	Severity	Description
unacpRFactorOutViolated	The Inter QOS Zone unacpRFactorOut parameter has violated set threshold value.	Critical	The Inter QOS Zone unacpRFactorOut parameter has violated set threshold value.
unacpEchoRLossOutViolated	The Inter QOS Zone unacpEchoRLossOut parameter has violated set threshold value	Critical	The Inter QOS Zone unacpEchoRLossOut parameter has violated set threshold value.
unacpEchoRLossInViolated	The Intra QOS Zone unacpEchoRLossIn parameter has violated set threshold value.	Critical	The Intra QOS Zone unacpEchoRLossIn parameter has violated set threshold value.
warnPacketLossInViolated	The Intra QOS Zone warnPacketLossIn parameter has violated set threshold value.	Critical	The Intra QOS Zone warnPacketLossIn parameter has violated set threshold value.
warnLatencyOutViolated	The Inter QOS Zone warnLatencyOut parameter has violated set threshold value.	Critical	The Inter QOS Zone warnLatencyOut parameter has violated set threshold value.
warnLatencyInViolated	The Intra QOS Zone warnLatencyIn parameter has violated set threshold value.	Critical	The Intra QOS Zone warnLatencyIn parameter has violated set threshold value.
warnRFactorInViolated	The Intra QOS Zone warnRFactorIn parameter has violated set threshold value.	Critical	The Intra QOS Zone warnRFactorIn parameter has violated set threshold value.
warnJitterOutViolated	The Inter QOS Zone warnJitterOut parameter has violated set threshold value.	Critical	The Inter QOS Zone warnJitterOut parameter has violated set threshold value.
warnEchoRLossInViolated	The Intra QOS Zone warnEchoRLossIn parameter has violated set threshold value.	Critical	The Intra QOS Zone warnEchoRLossIn parameter has violated set threshold value.
warnEchoRLossOutViolated	The Inter QOS Zone war-	Critical	The Inter QOS Zone warnEchoRLossOut

Incident	Message	Severity	Description
	nEchoRLossOut parameter has violated set threshold value.		parameter has violated set threshold value.
warnRFactorOutViolated	The Inter QOS Zone warnRFactorOut parameter has violated set threshold value.	Critical	The Inter QOS Zone warnRFactorOut parameter has violated set threshold value.
warnJitterInViolated	The Intra QOS Zone warnJitterIn parameter has violated set threshold value.	Critical	The Intra QOS Zone warnJitterIn parameter has violated set threshold value.
warnPacketLossOutViolated	The Inter QOS Zone warnPacketLossOut parameter has violated set threshold value.	Critical	The Inter QOS Zone warnPacketLossOut parameter has violated set threshold value.
commonMIBAlarmMinor	Minor alarm condition on Nortel device $6. Err Code $7. Alarm Type $8. Probable Cause $9. Alarm Data $10.	Critical	This trap is used to provide a real time indication of a minor alarm condition. The variables listed in VARIABLES clause are defined in `mgmt-info' group and are present in all info alarms.

Viewing the Network Connectivity

With the iSPI for IP Telephony, you can view the complete connectivity of the IP telephony network that you want to monitor. NNMi enables you to monitor the complete topology of the discovered network. If you log on to the NNMi console with an operator (level 1 or level 2) or guest credential, you can use the following tools to view the complete overview of your IP telephony network:

- **Topology Maps**

  The Topology Maps workspace of NNMi will help you view the complete topology of the IP telephony network. With the help of the following maps, you can perform a diagnosis of the connectivity between the devices in the IP telephony network.

  - Network Overview
  - Networking Infrastructure Devices
  - Routers
  - Switches

- **Troubleshooting**

  The Troubleshooting workspace helps you launch the path view, layer 2 neighbor view, or layer 3 neighbor view . These views help you identify the devices (layer 2 or 3) that reside between two different IP telephony devices

Refer to the *NNMi Online Help for Operators* for more information on these views.

The iSPI for IP Telephony presents two additional views—**Voice Path** and **Control Path**—that help you construct the connecting path between two different Cisco IP phones or between a Cisco IP phone and the controlling Cisco CallManager server respectively.

Launch a Voice Path

For Cisco networks only. With the iSPI for IP Telephony, you can launch the voice path between two Cisco IP phones. The voice path graph displays all the layer 2 and 3 devices between two IP phones with all the associated interfaces. The graphs presents an easy way to view the states of the connecting IP phones, all the intermediate layer 2/3 devices, and associated interfaces.

To launch a voice path view:

1. From the **Workspaces** navigation pane, click **Cisco IP Telephony > Cisco IP Phones**. The Cisco IP Phones view opens in the right pane.
2. In the Cisco IP Phones view, select two different Cisco IP phones.
3. Click **Actions > Voice Path**. The voice path graph opens in a new window.

Launch a Control Path

For Cisco networks only. A control path displays the connectivity between a Cisco IP phone and the controlling Cisco CallManager. With the iSPI for IP Telephony, you can launch the control path between a Cisco IP phones and the Cisco CallManager that controls the IP phone. The control path graph displays all the layer 2 and 3 devices between the IP phone and the Cisco CallManager with all the associated interfaces. The graphs presents an easy way to view the states of all the intermediate layer 2/3 devices and associated interfaces.

To launch a control path view:

1. From the **Workspaces** navigation pane, click **Cisco IP Telephony > Cisco IP Phones**. The Cisco IP Phones view opens in the right pane.
2. In the Cisco IP Phones view, select a Cisco IP phone.
3. Click **Actions > Control Path**. The control path graph opens in a new window.

Help for Administrators

With the administrative privilege, you can configure the polling and monitoring mechanism of the iSPI for IP Telephony. You can gain access to the configuration forms presented by the iSPI for IP Telephony, which enables you to change the settings like:

- Polling interval of a monitored device
- Access credentials to connect to a Cisco CDR
- Thresholds to generate incidents against specific QOS parameters

You can access all the views and forms that are accessible by an operator's profile. With the access to the two configuration forms—**IPT Polling Configuration** and **IPT QOS Configuration**—you can modify the polling schedules and control the mechanism to generate IP telephony-related incidents.

Configuration Workspace for Administrators

With the administrative privileges to the NNMi console, you can access the Configuration workspace. Along with the configuration forms presented by NNMi, the iSPI for IP Telephony introduces the IPT Polling Configuration and IPT QOS Configuration forms in this workspace.

To launch the IPT Polling Configuration form:

From the **Workspaces** navigation pane, click **Configuration > IPT Polling Configuration**. The IPT Polling Configuration form opens.

To launch the IPT QOS Configuration form:

From the **Workspaces** navigation pane, click **Configuration > IPT QOS Configuration**. The IPT QOS Configuration form opens.

iSPI for IP Telephony Configuration Workspaces

Name	Description
IPT Polling Configuration	Used to configure the polling schedules for collecting the states of Cisco CallManagers, Cisco IP phones, Nortel QOS Zone objects, and so on.
IPT QOS Configuration	Used to specify the details to access Cisco CallManager CDR repository server.

Configuring the iSPI for IP Telephony to Monitor Cisco CallManager Call Detail Records

The iSPI for IP Telephony can read the Cisco CallManager Call Detail Records (CDR) and can send incidents to the NNMi console's incident browser in the events of violations of QoS threshold parameters.

Configure the access details of Cisco CallManager CDR:

1. In the Workspaces pane, click **Configuration > IPT QOS Configuration**. The IPT QOS Configuration form opens.
2. In the IPT QOS Configuration form, specify the following details:
    a. In the **Configuration for accessing Cisco IPT CDR/CMR** section, specify the following details:
        - **CDR Repository Server IP**: Type the IP address of the Cisco CallManager CDR Repository Server
        - **SOAP Username**: Type the username for the Cisco SOAP-CDROnDemand service
        - **SOAP Password**: Type the password for the above user
        - **Port**: Type the port number for the Cisco SOAP-CDROnDemand service

- ○ **CM TimeZone**: Type the time zone that was set on the Cisco CallManager server. For Cisco CallManager version 5.1 and higher, leave this field empty, or type GMT. For other Cisco CallManager 5.x versions, type the time zone in the Java-acceptable format. For example, <*continent*>/<*city*>.

b. Click **Add**.

Configure the thresholds for Cisco IP telephony QoS metrics:

The iSPI for IP Telephony sends incidents to the NNMi incident browser based on the thresholds set for the Cisco IP telephony QoS metrics. To set the threshold values in the IPT QOS Configuration form, specify appropriate values for the following metrics in the **Cisco IPT QOS/MOS Thresholds Configuration** section:

- **Jitter:** The threshold jitter in milliseconds
- **PPL:** The threshold percentage packet loss
- **Latency:** The threshold latency in milliseconds
- **MOS:** The threshold Mean Opinion Score in the hundred's measure. For example, type 3.6 for 360.
- **RTT:** The threshold round trip time in milliseconds.

Note: Changes will take effect only after you click **Apply**.

Configure the FTP-communication mode:

To enable the iSPI for IP Telephony to send the data collected from CDR of the monitored Cisco CallManager CDR Repository server to the NNMi console, you must specify the following details in the **IPTSPI Server FTP Configuration to be used by Cisco IPT QOS/MOS monitor** section:

- **FTP Username:** Type a valid FTP user name with the write privileges on the NNMi server. See the *Preinstallation Tasks* section in the *Installation Guide* for more information on creating this user.
- **FTP Password:** Password for the above user.

Note: Changes will take effect only after you click **Apply**.

Configure the Polling of Cisco IP Phones

After the iSPI for IP Telephony discovers the available Cisco IP phones in the network, the polling of the phones occur with the default polling interval. You can modify the default polling interval and other polling parameters with the help of the IPT Polling Configuration form.

To configure the polling for Cisco IP phones:

1. From the **Workspaces** navigation pane, click **Configuration > IPT Polling Configuration**. The IPT Polling Configuration form opens.
2. In the IPT Polling Configuration form, go to the section **Configuration for polling Registration State & Controller-Association of Cisco IP Phones**.
3. In the **Configuration for polling Registration State & Controller-Association of Cisco IP Phones** section, specify the following details:
   - ■ **Poll Phone Table Objects:** Set this option to **True** if you want to poll the registration states of Cisco IP phones.
   - ■ **Poll Phone Update Table Objects:** Set this option to **True** if you want to poll the details of Cisco CallManagers associated with a Cisco IP phone.

- **Phone Table polling Interval:** Specify the interval (in milliseconds) to poll the registration states of Cisco IP phones.
- **Phone Update Table polling interval:** Specify the interval (in milliseconds) to poll the details of the associated Cisco CallManagers.

4. Click **Apply Changes**.

Configure the Polling of Cisco CallManagers

After the iSPI for IP Telephony discovers the available Cisco CallManagers in the network, the polling of the Cisco CallManager servers occur with the default polling interval. You can modify the default polling interval with the help of the IPT Polling Configuration form.

To configure the polling for Cisco CallManagers:

1. From the **Workspaces** navigation pane, click **Configuration > IPT Polling Configuration**. The IPT Polling Configuration form opens.
2. In the IPT Polling Configuration form, go to the section **Cisco Call Manager State Polling Configuration**.
3. In the **Cisco Call Manager State Polling Configuration** section, specify the following details:
   - **Poll Call Managers:** Set this option to **True** to poll the states of Cisco CallManagers.
   - **Call Manager polling Interval:** Specify the interval (in milliseconds) to poll the states of Cisco CallManagers.
4. Click **Apply Changes**.

Configure the Polling of Cisco Circuit Switch Channels

With the IPT Polling Configurations form, you can set the polling interval to poll the *usage* and *operational* states of discovered Cisco circuit-switched channels.

To configure the polling for the usage state of Cisco circuit-switched channels:

1. From the **Workspaces** navigation pane, click **Configuration > IPT Polling Configuration**. The IPT Polling Configuration form opens.
2. In the IPT Polling Configuration form, go to the section **Cisco Circuit Switched Channel Usage State Poller Configuration**.
3. In the **Cisco Circuit Switched Channel Usage State Poller Configuration** section, specify the following details:
   - **Poll usage state of Circuit Switched channel objects:** Set this option to **True** to poll the usage states of Cisco circuit-switched channels.
   - **Channel Usage state polling interval:** Specify the interval (in milliseconds) to poll the usage states of Cisco circuit-switched channels.
4. Click **Apply Changes**.

To configure the polling for the operational state of Cisco circuit-switched channels:

1. From the **Workspaces** navigation pane, click **Configuration > IPT Polling Configuration**. The IPT Polling Configuration form opens.
2. In the IPT Polling Configuration form, go to the section **Cisco Circuit Switched Channel Operational State Poller Configuration**.
3. In the **Cisco Circuit Switched Channel Operational State Poller Configuration** section, specify the following details:
   - **Poll oper state of Cisco Circuit Switched channel:** Set this option to **True** to poll the operational states of Cisco circuit-switched channels.
   - **Channel Operational state polling interval:** Specify the interval (in milliseconds) to poll the operational states of Cisco circuit-switched channels.
4. Click **Apply Changes**.

Configure the Hold Time of Cisco Circuit-Switched Channels

The usage states of Cisco circuit-switched channels are likely to undergo rapid changes. Frequent transitions to the *Idle* state for available channels may lead to the generation of unnecessary alarms in the incident browser. To prevent this, you can program the iSPI for IP Telephony to hold for a period of time before changing the state of a channel to *Idle*.

To configure the hold time of Cisco circuit-switched channels:

1. From the **Workspaces** navigation pane, click **Configuration > IPT Polling Configuration**. The IPT Polling Configuration form opens.
2. In the IPT Polling Configuration form, go to the section **Configuration of Cisco Circuit Switched Channel Idle time threshold**.
3. In the **Configuration of Cisco Circuit Switched Channel Idle time threshold** section, specify the following details:
   - **Poll Channel Usage state objects:** Set this option to **True** to poll the usage states of Cisco circuit -switched channels.
   - **Channel Usage State Hold Time:** Specify the interval (in milliseconds) for which the iSPI must wait before changing the state of a channel from *Active* to *Idle*. You can set this parameter to a multiple of the *Channel Usage state polling interval* parameter (see here).
4. Click **Apply Changes**.

Configure the Polling of Cisco Circuit Switch Interfaces

With the IPT Polling Configurations form, you can set the polling interval to poll the states of discovered Cisco circuit-switched interfaces. In addition, this form helps you set the options to monitor the registration state of a circuit-switched interface.

To configure the polling for the operational state of Cisco circuit-switched interfaces:

1. From the **Workspaces** navigation pane, click **Configuration > IPT Polling Configuration**. The IPT Polling Configuration form opens.
2. In the IPT Polling Configuration form, go to the section **Circuit Switched Interface Operational State Poller Configuration**.
3. In the **Circuit Switched Interface Operational State Poller Configuration** section, specify the following details:

- **Poll oper state of Circuit Switched IF objects:** Set this option to **True** to poll the operational states of Cisco circuit-switched interfaces.
- **Circuit Switched Interface oper state polling interval:** Specify the interval (in milliseconds) to poll the operational states of Cisco circuit-switched interfaces.

4. Click **Apply Changes**.

To configure the polling for the registration state and controller association of Cisco circuit-switched interfaces:

1. From the **Workspaces** navigation pane, click **Configuration > IPT Polling Configuration**. The IPT Polling Configuration form opens.
2. In the IPT Polling Configuration form, go to the section **Configuration for polling Registration State & Controller-association of Cisco Circuit Switched Interfaces**.
3. In the **Configuration for polling Registration State & Controller-association of Cisco Circuit Switched Interfaces** section, specify the following details:
   - **Poll Registration State and Controller-association:** Set this option to **True** to poll the registration state and controller association of Cisco circuit-switched interfaces.
   - **Startup Delay:** This parameter introduces a delay before the initial polling.
   - **Registration State and Controller-association polling interval:** Specify the interval (in milliseconds) to poll the registration states and controller association of Cisco circuit-switched interfaces.
4. Click **Apply Changes**.

Configure the Polling of Cisco Gatekeepers

In the Cisco Gatekeepers view, the iSPI for IP Telephony lists all the discovered Cisco gatekeeper devices with the number of endpoints associated with every gatekeeper device. You can configure the default interval to poll the discovered Cisco gatekeepers to read the number of associated endpoints.

To configure the polling for Cisco gatekeepers:

1. From the **Workspaces** navigation pane, click **Configuration > IPT Polling Configuration**. The IPT Polling Configuration form opens.
2. In the IPT Polling Configuration form, go to the section **Configuration for polling Cisco Gatekeepers' count of registered endpoints** .
3. In the **Configuration for polling Cisco Gatekeepers' count of registered endpoints** section, specify the following details:
   - **Poll count of registered endpoint objects:** Set this option to **True** if you want to collect the number of endpoints registered with every Cisco gatekeeper.
   - **Registered endpoint count polling interval:** Specify the interval (in millisecond) to poll the number of endpoints registered with every Cisco gatekeeper.
4. Click **Apply Changes**.

Configure the Polling of Cisco Gatekeeper-Controlled Intercluster Trunks

You can configure the mechanism to poll the registration states of all discovered Cisco gatekeeper-controlled intercluster trunks.

To configure the polling for Cisco gatekeeper-controlled intercluster trunks:

1. From the **Workspaces** navigation pane, click **Configuration > IPT Polling Configuration**. The IPT Polling Configuration form opens.
2. In the IPT Polling Configuration form, go to the section **Configuration for polling Registration State of Cisco GK controlled ICTs**.
3. In the **Configuration for polling Registration State of Cisco GK controlled ICTs** section, specify the following details:
   - **Poll Registration State of Cisco GK controlled ICTs:** Set this option to **True** to poll the registration states of Cisco gatekeeper-controlled intercluster trunks.
   - **Registration state polling interval:** Specify the interval (in milliseconds) to poll the registration states of Cisco gatekeeper-controlled intercluster trunks.
4. Click **Apply Changes**.

Configure the Polling of Nortel QoS Zones

In the Nortel QOS Zones table view, the iSPI for IP Telephony lists QoS metrics of all the configured QoS zones on discovered Nortel Signaling Servers. With the IPT Polling Configuration form, you can modify the mechanism to collect this data.

To configure the polling for Nortel QoS Zones:

1. From the **Workspaces** navigation pane, click **Configuration > IPT Polling Configuration**. The IPT Polling Configuration form opens.
2. In the IPT Polling Configuration form, go to the section **Nortel QOS Zone Threshold Polling Configuration**.
3. In the **Nortel QOS Zone Threshold Polling Configuration** section, specify the following details:
   - **Poll QOS Zone objects:** Set this option to **True** if you want to generate incidents based on the values of QoS metrics that are configured with the Nortel Signaling Server.
   - **QOS Zone polling interval:** Specify the interval (in millisecond) to poll the Nortel Signaling Sever to collect the details of QoS metrics.
4. Click **Apply Changes**.

Set thresholds for Nortel QoS metrics

In the Nortel QOS Zones table view, when you open the Nortel QOS Zone Details form, you can view the values of QoS metrics of all the configured QoS zones on discovered Nortel Signaling Servers. With this form, you can set threshold values for these metrics. In the event of threshold violation, the iSPI for IP Telephony sends incidents to the NNMi incident browser.

To set the threshold values for Nortel QoS metrics:

Note: You must log on with an administrative or operator level 2 privileges.

1. From the **Workspaces** navigation pane, click **Nortel IP Telephony > Nortel QOS Zones**. The Nortel QOS Zones view opens.
2. In the Nortel QOS Zones view, click to open the form for a particular Nortel QoS zone.
3. In the Nortel QOS Zone Details form, go to the Intra Zone QOS Parameters and Inter Zone QOS Parameters tabs and set threshold values for different metrics listed in the form. By default, all thresholds are set to **0**, which indicates no threshold has been set. You must set the threshold values to non-zero positive integers.
4. Click **Save and Close**.

Enable Log File Tracing

To perform the monitoring task, the iSPI for IP Telephony uses different processes. The iSPI for IP Telephony provides you with log files that capture the states of these processes.

These log files are stored into the following directory:

On the UNIX management server: /var/opt/OV/log/ipt

On the Windows management server: %NnmDataDir%\log\ipt

You can set the level of details that can be captured in these log files by setting the trace level appropriately.

To set the trace level:

1. Open the logging.properties file with a text editor from the following location on the management server:
   - On UNIX: /var/opt/OV/shared/ipt/conf
   - On Windows: %NnmDataDir%\shared\ipt\conf
2. Set the following properties to **INFO**, **FINE**, or **FINEST** (by default, all properties are set to INFO):
   - level
   - java.util.logging.FileHandler.level
   - com.hp.ov.nms.spi.ipt.statepoller.level
   - com.hp.ov.nms.spi.ipt.services.level
   - com.hp.ov.nms.spi.ipt.content.level
   - com.hp.ov.nms.spi.ipt.level
   - com.hp.ov.nms.apa.level
   - com.hp.ov.nms.analysis.level
   - com.hp.ov.nms.statepoller.level
   - com.hp.ov.nms.disco.level

The FINEST option gives you the most comprehensive level of details.

Reference Information

This section includes reference information on the processes and commands presented by the iSPI for IP Telephony. The iSPI for IP Telephony introduces the **encryptiptpasswd.ovpl** command and the **iptjboss** process.

This section includes the following topics:

- iptjboss
- encryptiptpasswd.ovpl

Name

iptjboss—This is a customized version of the jboss application server for the HP NNM i-series Smart Plug-in for IP Telephony (iSPI for IP Telephony).

Synopsis

iptjboss

DESCRIPTION

iptjboss is managed by ovspmd. It uses the $NNM_DATA/shared/ipt/conf/nms-ipt.jvm.properties file to pass arguments to the iSPI for IP Telephony jboss application server.

You can start it by running **ovstart** or **ovstart -c iptjboss**. To stop it, run **ovstop** or **ovstop -c iptjboss**. To see the status of it, run **ovstatus -c iptjboss** or **ovstatus -v iptjboss**.

The **iptjboss** process starts and stops along with NNMi processes. The **iptjboss** process hosts all the iSPI for IP Telephony services including discovery, polling, GUI server, and so on.

If there are problems starting iptjboss, see the $NNM_DATA/log/ipt/jbossServer.log file and other log files present in the $NNM_DATA/log/ipt directory for more information. The iptjboss process determines the trace level from the $NNM_DATA/shared/ipt/conf/logging.properties file for logging data in the log files present in the $NNM_DATA/log/ipt directory. For more information, see the online help.

EXAMPLES

To start the **iptjboss** processes along with other NNMi processes, run the following command:

$InstallDir/bin/ovstart

To start only the **iptjboss** process, run the following command:

$InstallDir/bin/ovstart -c iptjboss

To find the status of the **iptjboss** process, run the following command:

$InstallDir/bin/ovstatus -c iptjboss

AUTHOR

iptjboss was developed by Hewlett-Packard Company.

FILES

The **iptjboss** process process uses the following parameter files:

$NNM_DATA/shared/ipt/conf/nms-ipt.jvm.properties	This file contains the parameters that are passed to the JVM where iptjboss runs.
$NNM_DATA/shared/ipt/conf/nms-ipt.ports.properties	This file contains the lists of ports used by iptjboss.
$NNM_DATA/log/ipt/jboss-Server.log	This file contains the exceptions generated by iptjboss.

Name

encryptiptpasswd.ovpl—This command updates the HP NNM i-series Smart Plug-in for IP Telephony (iSPI for IP Telephony) jboss application server with the modified NNMi system account password and modifies the Web Server Client password (used during the iSPI for IP Telephony installation).

Synopsis

encryptiptpasswd.ovpl -c ipt

encryptiptpasswd.ovpl -e ipt <new-password>

DESCRIPTION

If you change the NNMi system account password after installing the iSPI for IP Telephony, you must update the iSPI for IP Telephony jboss application server with the changed password using this command. The password is stored in an encrypted format.

You can use this command to modify the password of the Web Service Client user, which was used during the iSPI for IP Telephony installation. The password is stored in an encrypted format. You must be logged on as root/administrator to run this command.

PARAMETERS

encryptiptpasswd.ovpl -c ipt

encryptiptpasswd.ovpl -e ipt <new-password>

-c ipt	This option helps you update the iSPI for IP Telephony jboss application server with the changed NNMi system account password.
-e ipt <new-password>	This option helps you modify the password of the Web Service Client user (used during the iSPI for IP Telephony installation).

EXAMPLES

To update the iSPI for IP Telephony jboss application server with the changed NNMi system account password, run the following command:

$InstallDir/bin/encryptiptpasswd.ovpl -c ipt

To modify the password of the Web Service Client user, run the following command:

$InstallDir/bin/encryptiptpasswd.ovpl -e ipt password123

password123 is the new password.

AUTHOR

encryptiptpasswd.ovpl was developed by Hewlett-Packard Company.

FILES

The **encryptiptpasswd.ovpl** uses the following files:

$NnmInstallDir/nonOV/ipt/jboss/server/nms/conf/props/nms-users.properties: NNMi system account's credentials are stored in this file.

$NNM_DATA//shared/ipt/conf/nnm.extended.properties: This file stores the credentials of the Web Service Client user.

Appendix B: Index