



Overview

The Cisco Packet Telephony Center (Cisco PTC) provides an effective management solution for large-scale H.323 networks. Cisco PTC provides network management layer functionality and manages the network through Element Management Systems (EMSs), or through the network element's management interface (for example, SNMP or Command Line Interface (CLI)). Cisco PTC maintains a database of the data, consisting of customer and services information, for the managed network. This database is used to configure the network, provision new services, and to detect network layer configuration inconsistencies.

The chapter is organized into the following sections:

- “Cisco PTC Management Solution”
 - “Provisioning of Virtual Entities”
 - “Detection of Configuration Inconsistencies”
- “Cisco PTC Managed Resources”
 - “NISF Managed Resources”
 - “Discovered Managed Resources”
- “Cisco PTC Indirectly Managed Components”
 - “Signaling Link Termination”
 - “RADIUS Server”
- “Network Discovery”
- “Network Element Configuration Uploading and Parsing”
 - “Signaling Controller Configuration”
 - “Gateway/Gatekeeper/Directory Gatekeeper IOS Configuration”
 - “Virtual Entity Formation”
 - “Inconsistency Flagging”
- “Creating and Deleting Managed Resources”
 - “Creating Managed Resources”
 - “Deleting Managed Resources”
- “Network Synchronization”.

Cisco PTC Management Solution

Cisco PTC provides overall configuration management of the network. A module within Cisco PTC, Cisco Voice Routing Center (VRC), provides for H.323 dial plan management. Cisco PTC allows you to launch other management tools in a context sensitive manner, that is, where it makes sense from a navigation standpoint, for an integrated experience. A pre-integrated application is the VSPT (Virtual Switch Provisioning Tool) which can be used to bulk configure PGW 2200/SC2200 signaling controllers.

To communicate with network devices, Cisco PTC makes use of underlying EMSs (Element Management Systems), such as CMNM (Cisco MGC Node Manager) for the PGW 2200 signaling controller. You can also launch EMSs as auxiliary tools, in case you want to drill down into a device and obtain a graphical device view. In cases where an EMS is not readily available, Cisco PTC can also interface to devices directly, or, as in the case of IOS devices, utilize the Cisco IE 2100 appliance for configuration delivery.

Operating at the network management layer of the Telecommunication Management Network (TMN) hierarchy, Cisco PTC most important function is the realization of a virtual entity view, hiding much of the internal complexity of the network and allowing gateways, gatekeepers, and signaling controllers, to be managed as if the virtual zones, virtual gateways, or virtual switches that they form were single entities. Cisco PTC is architected with high scalability in mind, because it must provide a single, overall management entry point into the network, capable of managing large deployments. Accordingly, it offers flow-through interfaces for OSSs, as well as a graphical user interface (GUI).

Through the Cisco PTC Topology Manager, virtual entities are seamlessly integrated with physical entities and can be navigated across in exactly the same manner, shielding you from their distributed nature.

Provisioning of Virtual Entities

The requirements for coordinated element management are extensive. H.323 gateways and gatekeepers in a zone should be managed as a virtual zone, as if they were one entity. Also, gateways and a signaling controller jointly provide the functionality of a virtual gateway that has SS7 capabilities. A potent management solution should allow for a holistic management of those entities. For example, the concept of a virtual SS7 gateway (that deals with dependencies between an H.323 gateway and a signaling controller that converts SS7 to Q.931 signaling for the gateway), a virtual zone (that deals with dependencies between gateways within a zone, as well as between gateways and gatekeepers), and a zone connection (that deals with dependencies between gatekeepers, or between gatekeepers and directory gatekeepers).

Most voice services and features require coordinated provisioning of the multiple network elements (for instance, in an H.323-based network, setting up signaling backhaul between a signaling controller connected to an SS7 network and an H.323 gateway. Performing these steps manually, and in the right sequence, is inefficient and error prone. Cisco PTC instead provides a set of functions that allow operators to operate in the much more meaningful context of a virtual switch (or other virtual entities). Therefore, instead of requiring tedious individual operations to be performed at each of the network elements, Cisco PTC offers functions such as the following:

- turn up/tear down/modify service for a customer
- associate or disassociate an H.323 gateway from a virtual zone

- associate or disassociate an H.323 gateway from a virtual gateway (signaling controller)
- through its Cisco VRC dial plan management module, Cisco PTC allows for simple management of dial plans that ensures configuration consistency of the affected network elements, without needing to, for instance, manually configure dial peers.

All of the above functions are provided as if they were single operations, hiding the underlying operational complexity of having to deal with multiple operations across multiple network elements, thus greatly improving operations efficiency and accuracy and making provisioning less error prone.

In addition to virtual entities requiring configuration of multiple network devices in a consistent manner, Cisco PTC supports configuration operations that can be scoped across the network and its virtual entity. For example, Cisco PTC allows you to apply the same configuration of certain gateway parameters across all gateways within a zone or a region. Although simpler than operations on virtual entities because they lack their stringent transactional requirements, this results, nonetheless, in a significant gain in operational efficiency.

Provisioning of a virtual entity occurs through the Cisco PTC Provisioning Manager. To increase productivity, basic parameters that must be supplied are treated separately from the rest of the parameters whose configuration is optional and for which the system provides defaults. Many of the Cisco PTC provisioning operations lead to multiple management requests issued to various EMSs and network elements, resulting internally in network management transactions, or provisioning jobs. Monitoring of job progress is available, allowing for the display of details of a particular job. This display allows operators to know the actual job status at any point in time and to infer what went wrong in cases of failures.

Detection of Configuration Inconsistencies

The notion of virtual entities provides Cisco PTC the ability to detect and flag network-level configuration inconsistencies that are otherwise very hard to troubleshoot. This is one aspect in which it goes significantly beyond a system that would be content doing only provisioning.

Cisco PTC provides comprehensive configuration management capabilities. It not only supports provisioning, that is, the generation and delivery of device configurations, but also configuration retrieval to provide an accurate image of the actual network configuration. By validating the current configuration of individual components against the expected virtual entities, you can be alerted of violations of such integrity rules, which might be introduced by operating personnel working outside Cisco PTC by configuring network devices directly using CLI, or in cases where Cisco PTC resides, added to an already existing deployment. Such inconsistent configurations can be very hard to detect, as typically, they are not trapped from an element view (such as the one displayed by an EMS) and everything seems perfectly legal. For example, a gateway and a signaling controller should be configured so they point to one another. However, if an erroneous configuration is performed manually at the devices, and the gateway does not point to the signaling controller and vice-versa, the configuration of each network element, in isolation, is perfectly legal, however, a network level configuration integrity is violated, resulting in dysfunctional service at both gateways.

Cisco PTC Managed Resources

A managed resource can be a managed element, an Element Management System (EMS), a network appliance, or a management domain. Some of these managed resources are *introduced* to the Cisco PTC system by a network administrator manually editing an initial seed file called the Network Information Seed File (NISF). See section “[NISF Managed Resources](#)” for a description of these managed resources.

Other managed resources are *discovered* by Cisco PTC through inventory upload from the underlying EMSs. See section “[Discovered Managed Resources](#)” for a description of these managed resources.

NISF Managed Resources

This section describes the managed resources that are *introduced* to the Cisco PTC system through the Network Information Seed File (NISF). A network administrator must manually edit this file, thus providing a list of the managed resources and their properties to the Cisco PTC system. See [Appendix A, “Cisco PTC Network Information Seed File,”](#) for a detailed description of the NISF and the Seed File Editor which you can use to edit the NISF. Following are the types of managed resources available through the NISF:

- regions
- Cisco MGC Node Managers
- Cisco IE2100 appliances
- gateways (GWs)
- gatekeepers (GKs)
- directory gatekeepers (DGKs).

Regions

A region is a management domain that partitions the Global Long Distance voice network. It may contain zero or one directory gatekeeper group and one or more virtual zones. A region that contains a directory gatekeeper group is configured as a hierarchical region, for which the directory gatekeeper is the only address resolution authority. Those regions that do not contain a directory gatekeeper group are configured as a meshed region, where every gatekeeper is an authority.

For each region defined in the NISF, Cisco PTC creates a region object in the Cisco PTC database. Each region is created with a unique name in the NISF and contains a list of its properties.

Cisco MGC Node Manager

A CMNM is the Element Management System for signaling controllers. The NISF contains a list of CMNMs and their properties.

Cisco IE2100

The Cisco IE2100 is a network appliance used to download and upload IOS configuration files to/from IOS devices. The NISF contains a list of Cisco IE2100 devices and their properties.

Gateways

The NISF contains a list of the gateways within each region, with each gateway identified by its:

- Name—name assigned to the network element
- Role—gateway
- IP Address—Ipv4 network address
- Region Name—name of the region the network element belongs.

A gateway is a Network Access Server (NAS) acting as an interface between a circuit-switched Public Switched Telephone Network (PSTN) and a packetized voice network. In the Wholesale voice solution, the gateway serves an H.323 terminal that interfaces from the PSTN to an H.323 VoIP network.

A gateway is the point at which a circuit-switched Fax or voice call is encoded (using a CODEC) and repackaged into IP packets (or vice versa). A gateway initiates a call set-up with an H.323 gateway through H.225 RAS.

The originating gateway terminates the VoIP call to an appropriate destination gateway with the gateway's assistance. The terminating gateway then retranslates the packetized voice into a format acceptable to the adjacent PSTN network. gateways provide accounting and Interactive Voice Response (IVR) services, while most voice routing intelligence resides on the gateway. Examples of Cisco gateways are: AS5300, AS3640 and AS3660 that can act as H.323 gateways for SS7 and non-SS7 based POPs; AS5400 can act as H.323 gateway only for a non-SS7 based POP.

Gatekeepers and Directory Gatekeepers

The NISF contains a list of the gateways and directory gatekeeper within each region, with each gatekeeper and directory gatekeeper specified by its:

- Name—name assigned to the network element
- Role—gateway or directory gatekeeper
- IP Address—Ipv4 network address
- Region Name—name of the region the gatekeeper or directory gatekeeper belongs.

Gatekeepers

An H.323 gatekeeper provides E.164 address resolution and controls access for all types of H.323 endpoints. It can provide other services to the endpoints such as bandwidth shaping and gatekeeper location. The gatekeeper maintains a registry of H.323 endpoints in a multimedia network. The endpoints register with the gatekeeper at start-up, and they request admission from the gatekeeper to set up a call. Examples of Cisco gatekeepers are: 3600 series routers (3620, 3640, 3660) and 7206 routers.

Cisco gatekeepers perform the following tasks:

- Resource Management—gatekeepers determine the health of H.323 gateways by monitoring registration and unregistration messages and resource availability indicators.
- Call Routing—gatekeepers provide call routing based on destination E.164 addresses. They may use their knowledge of local gateway health levels to make routing decisions in order to increase network availability of the gateways.
- Security—gatekeepers in conjunction with an external server (for example, RADIUS) may be used for secure call admission.
- CDR Generation—gatekeepers have limited abilities to generate CDR records for calls either in addition to or instead of from the gateway.

Gatekeeper Group

A gatekeeper group is an address resolution authority in a virtual zone. The gatekeeper group must contain a primary gatekeeper and may also contain an HSRP gatekeeper and/or one or more alternate gatekeepers.

Multiple directory gatekeepers may be assigned to a region. However, it is necessarily true that all directory gatekeepers contained within a given region will be configured solely for the purpose of redundancy through HSRP and/or serving as alternate directory gatekeepers. Such a configuration of directory gatekeepers is defined as a directory gatekeeper group. The directory gatekeeper group in a region serves as the *hub* for the zone prefix routing tables.

Directory Gatekeepers

A directory gatekeeper is a gatekeeper that is configured to accept LRQ forwarding. With a directory gatekeeper, individual gatekeepers do not need to know about other gatekeepers. Instead, a gatekeeper consults its routing table, which provides a default route to a directory gatekeeper. This directory gatekeeper is more knowledgeable about the topology of the network and can forward messages over to the proper egress gatekeeper. The egress gatekeeper can then contact the originating gatekeeper to complete the call set up.

Directory Gatekeeper Group

Multiple directory gatekeepers may be assigned to a region. However, it is necessarily true that all directory gatekeepers contained within a given region will be configured solely for the purpose of redundancy through HSRP and/or serving as alternate directory gatekeepers. Such a configuration of directory gatekeepers is defined as a directory gatekeeper group. The directory gatekeeper group in a region serves as the *hub* for the zone prefix routing tables.

Discovered Managed Resources

This sections describes the signaling controller managed resources that are auto discovered by Cisco PTC through inventory upload from the underlying EMSs.

Signaling Controller Discovery

CMNMs have mechanisms to discover all of the network elements that are in their management domains. By polling or other means, CMNMs populate their object models with information about the network elements (including SC2200 controller complexes and their constituting network elements, SC2200 hosts, Signaling Link Terminations (SLTs), and LAN switches) in their domain. CMNM, in turn, uploads this information to Cisco PTC through its Northbound Application Programming Interface (NBAPI).



Note

A signaling controller (SC) complex itself is a distributed network element that consists of multiple components (SC2200, 5500, SLT 2600), however, it is considered to be one network element. This is supported by the fact that the SC complex as a whole is managed by the CMNM SC Element Management System.

The SC2200 provides an SS7 (ISUP or TCAP) to Q.931-over-IP signaling conversion function. The SC2200 terminates the Message Transfer Part (MTP) Layer 3, converts the messages to Q.931 protocol and sends them to the gateway over an IP-based NFAS D channel. Thus, the SC2200 is a signaling controller that provides SS7 connectivity to the PSTN for Cisco H.323 voice-enabled gateways.

The SC2200 converts RUDP-based MTP3 messages from the SLT to Q.931 messages and sends them to the voice-enabled gateway. The SC2200 must also maintain the Circuit Identification Code (CIC) state for all trunks under its control within all media gateways. The SC2200 responds to all Q.931 messages from the media gateway and interfaces with the SS7 network. In so doing, the SC2200 must maintain the CIC state as it relates to both sides (the time-division multiplexing (TDM) network and the packet network). On the packet side, the SC2200 uses the Redundant Link Manager (RLM) to provide a virtual link management function between itself and the media gateway or NAS.

**Note**

The SC does not provide call routing functionality in the packet network. The call processing and routing functions are handled by the gateways and gatekeepers.

Media Gateway

A media gateway is a type of Network Access Server (NAS) that acts as an interface between a circuit-switched PSTN network and a packetized voice network. A Gateway is the point at which a circuit-switched fax or voice call is encoded (using a CODEC) and repackaged into IP packets (or vice versa).

In the Global Long Distance voice context, the Cisco AS5300s, AS3640s, AS5400s, and AS3660s are considered media gateways. In this context, a gateway initiates a call set up with a H.323 gatekeeper through H.225 RAS. The originating gateway terminates the VoIP call to an appropriate destination gateway with a gatekeeper's assistance. The terminating gateway then retranslates the packetized voice packet into a format acceptable to the adjacent PSTN network.

**Note**

A media gateway actually constitutes a role that a physical device plays in the voice network; the same device can be configured for another role (such as an MGCP gateway) in another setting.

Media Gateway Controller

A media gateway controller (MGC) is a network element that contains call control logic and terminates signaling. In the Global Long Distance voice context, the signaling controller complex constitutes a media gateway controller. See the "[Signaling Controller Discovery](#)" section for a description of the role played by signaling controllers.

Cisco PTC Indirectly Managed Components

This section describes the major network components indirectly managed by Cisco PTC.

Signaling Link Termination

The Signaling System 7 (SS7) signaling link termination is performed with the use of a Cisco Signaling Link Termination (SLT). Cisco SLT enables service providers to reliably transport SS7 protocols across an IP network. The Cisco SLT uses the Cisco Internetworking (IOS) Operation System SS7 Cisco SLT feature set, providing reliable interoperability with the signaling controller. The Cisco SLT uses the Cisco Reliable User Datagram protocol (RUDP) to backhaul, or transport, upper-layer SS7 protocols

across an IP network. The Cisco SLT terminates the MTP layer 2 of the SS7 ISUP message and inserts the remaining MTP layer 3 message into a Cisco-proprietary RUDP message in an IP datagram, and transports it across the IP network to the signaling controller.

The SLT can be broken down into the following functional components:

- SS7 signaling link
- SS7 MSU processing
- IP/packet connection between the SLT and the signaling controller.

The Cisco SLT uses a Session Manager to manage the communication sessions with the signaling controller. When the SLT is used with a redundant pair of signaling controllers, the Session Manager maintains a separate communication session with each controller in the pair. The session between the Cisco SLT and the active controller transports the SS7 traffic, while the session between the SLT and the standby controller provides backup. The Session Manager uses RUDP to communicate between the Cisco SLT and the controller. RUDP is a simple, connection-oriented, packet-based transport protocol that is Cisco-proprietary and is based upon RFC 908 (Reliable Data Protocol) and RFC 1151 (version 2 of the Reliable Data Protocol).

RADIUS Server

The RADIUS Server interfaces with gateway and gatekeeper components to provide the following functions:

- Call Detail Record (CRD) Collection and Billing System Front-Ending—gateways send call start/stop records to a RADIUS server by means of AAA. The billing application can extract these records to generate CDRs. CDRs may be shared between carriers as a method of settlement through billing system mediation applications.
- User Authentication and Authorization—for card services, a AAA RADIUS server may validate end users on the basis of Automatic Number Identification (ANI) or username and password combinations.
- Application Hosting—a gateway may run a call script that interacts with an application mounted on the RADIUS server. The server is capable of manipulating call information by means of VSAs (vendor-specific attributes) in AAA.
- Security—gatekeepers can administer H.235 security options to perform secure endpoint registrations.
- Settlement—some billing system vendors support interdomain settlement based on CDRs that are collected from each local domain. This offers a viable alternative to Open Settlement Protocol (OSP) in some cases.

Network Discovery

Initial network discovery is the process through which Cisco PTC discovers the current device configurations on the voice network and uses that information to populate its baseline Management Information Tree (MIT). Cisco PTC determines the network elements in the Global Long Distance voice network, the physical and logical device configurations on each network element, the network connectivity relationships between these network elements, and the other network layer concepts.

Network Element Configuration Uploading and Parsing

This section describes how the various managed resources have their configuration files uploaded and parsed by Cisco PTC.

Signaling Controller Configuration

Cisco PTC uploads the discovered signaling controller configurations from the CMNMs through their Northbound Application Programming Interface (API). The configuration information that is uploaded includes the SC nodes, SC hosts, signaling components, and trunking components. Cisco PTC parses these configuration files and extracts the physical and logical information from the devices. The corresponding SC managed objects are then populated in the Cisco PTC database.

Gateway/Gatekeeper/Directory Gatekeeper IOS Configuration

Cisco PTC reads the list of gateways, gatekeepers, and directory gatekeepers specified by the network administrator in the NISF, and uploads their running IOS configurations, from the devices, through the Cisco IE2100 appliance. Cisco PTC then parses the IOS configuration files and extracts the voice related physical and logical information from them. The device type (such as, AS5300, AS5300, 7200) is then extracted from the configuration files (the system administrator is not required to provide the device type information). The corresponding Cisco PTC related gateway, gatekeeper, and directory gatekeeper managed objects are then populated in the Cisco PTC database.

Virtual Entity Formation

Based upon the device configurations uploaded from the network elements, and the region, gateway, gatekeeper, and directory gatekeeper information provided in the NISF, Cisco PTC creates the following virtual entities that represent network layer concepts:

- region
- directory gatekeeper group
- gatekeeper group
- virtual gateway
- virtual zone.

Region

A region is a logical container that partitions the Global Long Distance voice network. It may contain zero or one directory gatekeeper group and one or more virtual zones. A region that contains a directory gatekeeper group is configured as a hierarchical region, for which the directory gatekeeper is the only address resolution authority. Those that do not are configured as a meshed region, where every gatekeeper is an authority.

For each region defined in the NISF, Cisco PTC creates a region object in the Cisco PTC database. Each region is created with a unique name in the NISF.

Directory Gatekeeper Group

Multiple directory gatekeepers can be assigned to a region. However, all directory gatekeepers contained within a given region are configured solely for the purpose of redundancy through HSRP, and/or serve as alternate directory gatekeepers. Such a configuration of directory gatekeepers is defined as a directory gatekeeper group. The directory gatekeeper group in a region serves as the hub for the zone prefix routing tables.

Based upon the directory gatekeepers information provided in the NISF, Cisco PTC groups together the directory gatekeepers that are assigned to the same region to form a directory gatekeeper group.

Gatekeeper Group

A gatekeeper group is an address resolution authority in a virtual zone. The gatekeeper group must contain a primary gatekeeper and may also contain an HSRP gatekeeper and/or one or more alternate gatekeepers.

For each gatekeeper specified in the NISF, Cisco PTC uploads its HSRP and cluster IOS configurations. Redundant gatekeepers in a region, that are configured as HSRP and/or alternate gatekeepers, are grouped together to form a gatekeeper group.

Virtual Gateway

A virtual gateway consists of a voice gateway and an SS7 signaling controller, if the gateway is configured for SS7 signaling. The SS7 SC functions as an SS7 to Q.931-over-IP signaling converter to the gateway.

For each gateway specified in the NISF, a virtual gateway object is created in the Cisco PTC database. When the gateway is configured for SS7 signaling, Cisco PTC includes the corresponding signaling controller as part of the virtual gateway. Cisco PTC also forms a Q.931 signal path object under the virtual gateway to represent the signal link between the gateway and the signaling controller.

Virtual Zone

A virtual zone groups together gatekeepers and virtual gateways according to the same criteria as would be found for a canonical H.323 zone. A virtual zone is composed of a gatekeeper group and a list of virtual gateways. The gatekeeper group functions as the sole gatekeeper address resolution authority for all of the gateways within the virtual zone. An address resolution authority is used as the destination for egress routes.

Corresponding to each gatekeeper group in a region, a virtual zone object is created. Cisco PTC uploads the dial-peer IOS configurations for each gateway in the same region, as specified in the NISF. gateways that are configured to talk to the same gatekeeper group collectively form a virtual zone.

Inconsistency Flagging

While discovering the virtual entities, Cisco PTC detects any misconfiguration and flags them, as described in the following sections.

Region Validation

Cisco PTC detects inconsistent inter-region configurations. Any inconsistency detected is marked in the respective region and directory gatekeeper/gatekeeper objects.

- **Hierarchy Region to Hierarchy Region**—Cisco PTC detects misconfigurations amongst the directory gatekeepers between the two regions. The directory gatekeepers in two different hierarchical regions must be configured to point to each other as the remote directory gatekeepers for one another.
- **Hierarchy Region to Meshed Region**—Cisco PTC detects mis-configurations between the directory gatekeepers in the hierarchy region and the gatekeepers in the meshed region. The directory gatekeeper in the hierarchy region must point to each gatekeeper in the meshed region as a remote gatekeeper. The gatekeepers in each zone of the meshed region must point to the directory gatekeeper as a remote gatekeeper.
- **Meshed Region to Meshed Region**—Cisco PTC detects mis-configurations amongst the gatekeepers between the two regions. The gatekeepers in each zone of a region must point to gatekeepers in each zone of the other region as the remote gatekeeper, and vice versa.

Cisco PTC detects inconsistent intra-region configurations. Any inconsistency detected is marked in the respective region and the directory gatekeeper/gatekeepers objects.

- **Hierarchy Region**—Cisco PTC detects misconfiguration between the directory gatekeeper group and the zones. Each directory gatekeeper must be configured to point to each gatekeeper in each zone as a remote gatekeeper, and vice versa.
- **Meshed Region**—Cisco PTC detects misconfiguration between zones. Each gatekeeper in each zone must be configured to point to each gatekeeper in the other zones as a remote gatekeeper.

Directory Gatekeeper Group Validation

Cisco PTC validates that all directory gatekeepers contained in the directory gatekeeper group are configured solely for the purpose of redundancy through HSRP and/or serving as alternate directory gatekeepers. The validation is done by cross-referencing the HSRP and cluster IOS configurations amongst the directory gatekeepers. Any inconsistency detected is flagged in the respective directory gatekeeper group object.

Gatekeeper Group Validation

Cisco PTC validates that all gatekeepers contained in the gatekeeper group are configured solely for the purpose of redundancy through HSRP, clustering, and/or serving as alternate gatekeepers. The validation is done by cross-referencing the HSRP and cluster IOS configurations amongst the gatekeepers. Any inconsistency detected is flagged in the respective gatekeepers group object.

Virtual Gateway Validation

Cisco PTC validates the configuration between the gateway and the signaling controller on an SS7 virtual gateway. Any inconsistency detected is flagged in the respective virtual gateway and gateway/signaling controller objects. The validation includes:

- **Consistent Redundant Link Manager (RLM)**— the gateway RLM group configurations must be consistent with the signaling controller NAS path IP links

- Consistent Q.931 Signal Path—the gateway SS7 serial interface configurations must be consistent with the signaling controller NAS path configurations
- Consistent Trunk Termination—the signaling controller nailed trunk configurations must be consistent with the gateway PRI group configurations.

Virtual Zone Validation

Cisco PTC validates consistency between the gateway dial peer configurations and the gatekeeper zone configurations. Any inconsistency detected is marked in the respective virtual zone and gatekeepers/gateway objects. Cisco PTC validates that the gatekeeper ID configured on the gateway exactly matches the gatekeeper ID in the gatekeeper configuration.

Creating and Deleting Managed Resources

This section provides an overview about creating and deleting Cisco PTC managed resources.

Creating Managed Resources

Cisco PTC supports the creation of newly managed resources. These include:

- adding a new region—the unique name of the region must be specified
- adding a new signaling controller—the signaling controller complex name and the managing CMNM must be specified. Cisco PTC uploads the device configurations through the respective CMNM.
- adding a new gateway/gatekeeper/directory gatekeeper—the network element's name, role (gateway/gatekeeper/directory gatekeeper), IP address, assigned region, and Cisco IE2100 must be specified. Cisco PTC uploads the device configurations through the respective Cisco IE2100 appliance.

Cisco PTC supports on-demand creation of new Element Management Systems (EMSs). These include:

- adding a new CMNM—the CMNM IP address must be specified. No immediate attempt to upload device configurations from the newly created CMNM will be made. Uploads are triggered through periodic or on-demand synchronization.
- adding a new Cisco IE2100—the Cisco IE2100 IP address must be specified.



Note

Prior to introducing EMSs, Cisco IE2100 appliances, or network elements to the Cisco PTC system, it is assumed they have been deployed in the network (meaning they have been preconfigured through CLI or other means, and have established IP connectivity to the network).

Cisco PTC supports bulk introduction of managed resources to the system in a single request.

See the [“Adding a Device” section on page 3-22](#) for a detailed description on how to add a managed resource to the Cisco PTC system.

Deleting Managed Resources

Cisco PTC supports on-demand removal of a managed resource from the system. These include:

- region removal—a region can only be removed from the Cisco PTC system when it contains no network elements
- signaling controller removal—a signaling controller can only be removed from the Cisco PTC system when it is in the inactive state (that is, it has been removed from the underlying CMNM, or is unreachable from the CMNM, or it has been removed from the network)
- gateway/gatekeeper/directory gatekeeper removal—a gateway/gatekeeper/directory gatekeeper can only be removed from the Cisco PTC system when it is in the inactive state (that is, it is unreachable from the Cisco IE2100 or it has been removed from the network).

Cisco PTC supports on-demand removal of EMSs. These include:

- CMNM—a CMNM can be removed only if it is not managing any SCs or it is in an inactive state (that is, it is unreachable or has been removed from the network)
- Cisco IE2100—a Cisco IE2100 can be removed only if it is not managing any IOS devices or if it is in an inactive state (that is, it is unreachable or removed from the network).

See the [“Removing a Device” section on page 3-26](#) for a detailed description on how to remove a managed resource from the Cisco PTC system.

Network Synchronization

Network synchronization is the process through which Cisco PTC reconciles its management information with the current device configurations on the voice network.

Cisco PTC supports the following mechanisms to synchronize the objects in its model with the network elements:

1. Notification based—when configuration or state changes occur on network elements, they emit real time notifications which are processed and passed to Cisco PTC as events. Therefore, Cisco PTC receives the real time update of the objects.
2. Interval based—periodically, preferably nightly, Cisco PTC forces a synchronization of the object model with the network elements on the entire H.323 voice network. Depending upon the number of objects in the system, this could be an expensive operation and is performed during non-peak times.
3. On demand (forced)—synchronization of the entire network or on specific regions may be requested, on demand, by an operator. This mechanism could be requested when there is reason to believe that Cisco PTC and the underlying network elements have gotten out of sync (for example, after a previous bulk configuration). This is an expensive operation and a scope should be applied.

See the [“Resync Topology” section on page 3-11](#) for a detailed description of the events that occur when you choose the **Resync Topology** option in the Topology Management window.

