CHAPTER 32

Logical Partitioning

The Logical Partitioning feature specifies the capability of a telephony system to control calls and features on the basis of specific allowed or forbidden configurations. A common telephony system can provide access to Voice over Internet Protocol (VoIP) and Public Switched Telephone Networks (PSTN), and configuration can control access.

This chapter contains information on the following topics:

- Configuration Checklist for Logical Partitioning, page 32-1
- Introducing Logical Partitioning, page 32-4
- Overview of Logical Partitioning Architecture, page 32-8
- Enterprise Parameters for Logical Partitioning, page 32-10
- System Requirements for Logical Partitioning, page 32-22
- Interactions and Limitations, page 32-22
- Configuring Logical Partitioning, page 32-39
- Logical Partitioning Configuration Upon Upgrade From Previous Releases, page 32-47
- Troubleshooting Logical Partitioning, page 32-47
- Related Topics, page 32-47

Configuration Checklist for Logical Partitioning

Logical partitioning allows configuration of Cisco Unified Communications Manager systems, so single-line phones, multiline phones, and analog phones can get configured to prevent restricted calls that mix VoIP and PSTN resources when calls occur between different geolocations. Only geolocations (in the Phone Configuration window) and geolocation filters (in the Device Pool Configuration window) can get configured for phones.

Table 32-1 provides a checklist for configuring logical partitioning. For more information on logical partitioning, see the "Related Topics" section on page 32-47.

Table 32-1 Logical Partitioning Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Enable logical partitioning by setting the value of the Enable Logical Partitioning enterprise parameter to *True*.	Enterprise Parameter Configuration, *Cisco Unified Communications Manager Administration Guide* Enterprise Parameters for Logical Partitioning, page 32-10
Step 2	Define a set of geolocations on a new Geolocation Configuration window.	Geolocation Configuration, page 24-10
Step 3	Assign geolocations to device pools, devices, trunks, gateways, or MGCP ports.	Device Pool Configuration Settings, *Cisco Unified Communications Manager Administration Guide* Gateway Configuration Settings, *Cisco Unified Communications Manager Administration Guide* Displaying the MAC Address of a Phone, *Cisco Unified Communications Manager Administration Guide* Trunk Configuration Settings, *Cisco Unified Communications Manager Administration Guide*
Step 4	Assign geolocations to the default geolocation that the Default Geolocation enterprise parameter specifies.	Geolocation Configuration, page 24-10 Enterprise Parameter Configuration, *Cisco Unified Communications Manager Administration Guide* Enterprise Parameters for Logical Partitioning, page 32-10
Step 5	Define the Logical Partitioning Default Policy, which determines whether to allow or deny PSTN calls between devices that associate with valid geolocations and geolocation filters when no explicit Allow/Deny policy is configured in the Logical Partitioning Policy Configuration window for the related geolocation policy records. Use the Enterprise Parameters Configuration window to set the value for the Logical Partitioning Default Policy enterprise parameter.	Enterprise Parameter Configuration, *Cisco Unified Communications Manager Administration Guide* Enterprise Parameters for Logical Partitioning, page 32-10

Table 32-1 Logical Partitioning Configuration Checklist (continued)

Configuration Steps		Procedures and Related Topics
Step 6	For devices that do not participate in logical partitioning policy checks, define the geolocation as *Unspecified* or leave undefined. **Note** Devices that do not associate with a geolocation or geolocation filter do not participate in logical partitioning policy checks. This lack of association can get defined at the individual-device level, the device-pool level, or the enterprise-parameter level.	Device Pool Configuration Settings, *Cisco Unified Communications Manager Administration Guide* Gateway Configuration Settings, *Cisco Unified Communications Manager Administration Guide* Displaying the MAC Address of a Phone, *Cisco Unified Communications Manager Administration Guide* Trunk Configuration Settings, *Cisco Unified Communications Manager Administration Guide* Enterprise Parameter Configuration, *Cisco Unified Communications Manager Administration Guide* Enterprise Parameters for Logical Partitioning, page 32-10
Step 7	Define a set of filter rules in a new Geolocation Filter Configuration window.	Geolocation Filter Configuration, page 24-17
Step 8	Assign geolocation filters to device pools, trunks, intercluster trunks, gateways, or MGCP ports.	Device Pool Configuration Settings, *Cisco Unified Communications Manager Administration Guide* Gateway Configuration Settings, *Cisco Unified Communications Manager Administration Guide* Trunk Configuration Settings, *Cisco Unified Communications Manager Administration Guide*
Step 9	Assign geolocation filter to the default filter that the Logical Partitioning Default Filter enterprise parameter specifies.	Enterprise Parameter Configuration, *Cisco Unified Communications Manager Administration Guide* Enterprise Parameters for Logical Partitioning, page 32-10
Step 10	Define a set of logical partitioning policy records in a new Logical Partitioning Policy Configuration window.	Logical Partitioning Policy Configuration, page 32-40

Table 32-1 Logical Partitioning Configuration Checklist (continued)

Configuration Steps		Procedures and Related Topics
Step 11	Define a set of policies between geolocation policy record device-type pairs: `{{Geolocation Policy1, devType1}, {Geolocation Policy2, devType2}, policyValue}`	Logical Partitioning Policy Configuration, page 32-40
Step 12	To allow devices in different clusters to participate in logical partitioning policy checks, turn on location conveyance as follows: • Check the Send Geolocation Information check box in the intercluster trunk (ICT) or SIP trunk of the local cluster. • Check the Send Geolocation Information check box in the ICT or SIP trunk of the remote cluster.	Trunk Configuration Settings, *Cisco Unified Communications Manager Administration Guide* Configuration Checklist for Location Conveyance, page 24-4

Introducing Logical Partitioning

Logical partitioning specifies a call control feature in Cisco Unified Communications Manager that provides functionality, so communication between the following pairs of VoIP entities can be controlled:

1. A VoIP phone and a VoIP gateway
2. A VoIP gateway and another VoIP gateway
3. An intercluster trunk and a VoIP phone
4. An intercluster trunk and a VoIP gateway

Options exist to configure Cisco Unified Communications Manager, so any such set of VoIP devices may be allowed communication with each other and any device can be restricted to one device or to a group of devices. No logical partitioning policy logic exists on endpoints.

Be aware that logical partitioning is required to control such communication not only during basic call establishment but also during mid-call as a result of midcall features.

The Cisco Unified Communications Manager basic routing policy constructs of calling search spaces and partitions suffice to prevent forbidden basic calls from being established but are not sufficient to prevent forbidden calls from being created as a result of midcall features. In Cisco Unified Communications Manager, such midcall features are often termed Join and Redirect features, because these primitives often get used internally to affect these features.

Logical partitioning enhances Cisco Unified Communications Manager to handle such midcall scenarios. Configuration for logical partitioning remains independent of supplementary features, where the policy checking gets performed based on devices being joined or redirected to a supplementary feature.

Note Logical partitioning policy checks get performed later than digit analysis/calling search space/partition logic during call processing.

The logical partitioning solution comprises the following elements:

- Identifiers—A framework to associate a unique identifier with every device.
- Policies—Allow administrator the ability to define rules or policies that determine the interconnection between any two devices (a VoIP phone and a gateway) in the Cisco Unified Communications Manager system. The configured policies work bidirectionally between the pair of devices.
- Policy Checking—Call processing and features such as transfer, pickup, and ad hoc conference check the defined policies before allowing the calls or features between participants.

Identifiers

Identifiers specify a device type for every device (element) in a Cisco Unified Communications Manager logical partitioning solution. Device types classify all elements into two types: interior and border. Table 32-2 specifies the Cisco Unified Communications Manager devices that associate with each device type:

Table 32-2 Device Types and Associated Cisco Unified Communications Manager Devices

Device Type	Cisco Unified Communications Manager Device
Border	Gateway (for example, H.323 Gateway)
	Intercluster trunk (ICT), both gatekeeper-controlled and non-gatekeeper-controlled
	H.225 trunk
	SIP trunk
	MGCP port (E1, T1, PRI, BRI, FXO)
Interior	Phones (SCCP, SIP, third party)
	CTI route points
	VG224 analog phones
	MGCP port (FXS)
	Cisco Unity Voice Mail (SCCP)

Note For MGCP PRI Q.SIG devices, the internal Cisco Unified Communications Manager device type in Geolocation Info will be “QsigDevice,” which is mapped to “Interior.” “Interior” is used for onnet devices.

Note For Q.SIG ICT trunk, Q.SIG H225 trunk & Q.SIG H323 gateways, the internal Cisco Unified Communications Manager device type in Geolocation Info is “AccessDevice,” which is mapped to “Border.” “Border” is used for offnet devices.

Note You cannot edit the classification of Cisco Unified Communications Manager elements: only border and interior designations are allowed, and a particular device can be classified only according to the scheme that Table 32-2 provides. For example, a SIP trunk can be classified only as a border element.

See the "Geolocation Identifiers" section on page 24-8 for further information. See "Geolocation Examples" section on page 24-8 for examples of geolocation identifiers.

Allow and Deny Policies

Based on the system requirements for VoIP network topology, you can configure Cisco Unified Communications Manager to provide the following default system policy for logical partitioning:

- Deny—Calls or features get blocked between VoIP device participants of types 1 to 4 (previously enumerated).

  To allow VoIP communication, ensure the Allow policy is configured through logical partitioning configuration.

- Allow—Be aware that calls or features are allowed between VoIP device participants of types 1 to 4 (previously enumerated).

  To deny VoIP communication, ensure the Deny policy is configured through logical partitioning configuration.

Additional Information

See the "Related Topics" section on page 32-47.

Applicability to Requirements From Indian Telecom Regulations

Regulations of the Telecom Regulatory Authority of India (TRAI) require that voice traffic over the enterprise data network and the Public Switched Telephone Network (PSTN) must be strictly separated and no mixing of calls between the two networks can occur for the purpose of toll bypass.

The following list shows basic scenarios that are restricted (that is, not allowed):

- The call that passes through a PSTN gateway connects directly by using WAN to a VoIP phone or VoIP PSTN gateway in a different geographic location.
  - If PSTN gateway is located in India, this remains strictly restricted. If the PSTN is in another country and a VoIP phone is in India and if connection results in revenue loss to Indian telecom service providers, the connection gets considered restricted.

The following list gives basic scenarios that are permitted:

- Call directly between two VoIP phones in different geographic locations
- Call from a VoIP phone to a PSTN gateway in the same geographic location

A call that passes through a PSTN gateway must never connect directly to a VoIP phone or VoIP PSTN gateway in a different site or geographic location (geolocation) through use of IP telephony.

Requirement for Deployments

While following TRAI regulations and avoiding toll bypass, a single-line phone should be able to reach outside VoIP (closed user group [CUG]) or PSTN networks, provided that the suggested configuration guidelines are met.

Note Ensure logical partitioning is enabled to avoid any toll bypass.

Available Cisco Unified Communications Manager Support

Cisco Unified Communications Manager prior to implementation of the logical partitioning feature provides the following support:

- Phones can use the same line to reach the VoIP or PSTN networks.
- The existing calling search space (CSS) and partitions mechanism allows partitioning of the network for basic calls only.

Limitations With a Single Line

The following limitations exist when a single line is used without (or prior to) configuration of the logical partitioning feature:

- Possible midcall Join—A call that connects to a VoIP network on WAN and another call that is made to a PSTN network may get joined upon invocation of a supplementary feature such as Transfer.
- Possible redirects—A call that comes from a VoIP network on WAN may get redirected to a PSTN network upon invocation of a supplementary feature such as Forwarding.

Without the logical partitioning feature, you cannot configure supplementary features to prevent invocation of the restricted scenarios.

Existing Deployments Prior to Use of Logical Partitioning

In India and other countries, separate lines on phones get used to separate the VoIP (CUG) and PSTN networks. This implementation previously prevented use of low-cost analog phones and single-line VoIP phones.

In deployments that use two-line phones, invocation of supplementary features like Join Across Lines (JAL) or Direct Transfer Across Line (DTAL) can result in scenarios that are restricted by TRAI regulations. For such deployments to conform to the regulations, you need the logical partitioning feature.

Additional Information

See the "Related Topics" section on page 32-47.

History

Originally, Indian regulations required that Voice over IP (VoIP) systems be physically separate from PSTN interconnect systems. Users used phones on a VoIP system strictly for interoffice phone calls, but any calls that needed to go to or come from the PSTN had to be made by using the PSTN system. Telecom Regulatory Authority of India (TRAI) regulations as of 2008 permit a single system to support both types of calls, as long as the system can be configured so that forbidden calls cannot complete. In a Cisco Unified Communications Manager system, the term *logical partitioning* specifies this capability.

The Enterprise VoIP implementations that use releases of Cisco Unified Communications Manager prior to Release 7.1(x) in India use the same Cisco Unified IP Phone for both the VoIP and PSTN connectivity. Cisco Unified Communications Manager does not support specific configurations for controlling the mixing of VoIP and PSTN traffic when supplementary features are invoked from a single line with participants in VoIP or PSTN domains. To comply with regulations, previous VoIP implementations in India used separate lines on VoIP phones for PSTN and VoIP calls.

Cisco Unified Communications Manager uses the concept of partitions and calling search spaces (CSS) for configuration of the respective lines. Thus, control remains separate for the VoIP and PSTN domains, and features like Transfer cannot be performed on single-line phones, because invoking such features could result in joining the VoIP with the PSTN network.

With this limitation, enterprise VoIP deployments in India that use Cisco equipment remained limited to using phones with minimum of two lines, which is not a cost-effective solution for most customers. This limitation also prevented solutions that use low-cost analog phones that are single line by design and use VG224/VG248 gateways.

To overcome the limitations, a Cisco Unified Communications Manager solution now allows logical partitioning of a single line on Cisco Unified IP Phones through administrator policies. Be aware that control of call joining or call redirection is required, based on an attribute tag or the geolocation of the parties.

Additional Information

See the "Related Topics" section on page 32-47.

Overview of Logical Partitioning Architecture

The logical partitioning solution entails provisioning the following elements:

- Configure geolocation identifiers
  - Administrator can define sets of geolocations (civic addresses).
  - Administrator can assign these geolocations to VoIP phones, VoIP gateways, IP trunks, device pools, and enterprise parameters.
  - Administrator can define filters that select a subset of fields from geolocation and associate with VoIP gateways, IP trunks, device pools, and enterprise parameters.
- Configure policies
  - Allow administrator to define geolocation policy records and define matrices of geolocation policy records that contain a policy that indicates whether a connection is permitted or denied. The configured policies work bidirectionally between the pair of devices.
- Communicate geolocation information across clusters
  - Allow communication of geolocation information from one cluster to another, both at call establishment as well as midcall joins and redirects.

Additional Information

See the "Related Topics" section on page 32-47.

Logical Partitioning Use of Geolocations and Geolocation Filters

Cisco Unified Communications Manager administrators must define the following items:

- A *geolocation* for every device that uses logical partitioning. See the "Geolocation Characteristics" section on page 24-6 for details.
- A *geolocation filter* for every device that uses logical partitioning. See the "Introducing Geolocation Filters" section on page 24-16 for details.

Cisco Unified Communications Manager administrators then assign geolocations and geolocation filters to devices.

The following entities in a Cisco Unified Communications Manager cluster can have geolocation and geolocation filter values that are assigned:

- Device pools
- CTI route points
- Phones (optional)
- CTI ports

Note Phones do not specify a drop-down list box for associating a phone with a geolocation filter.

- SIP trunks
- Intercluster trunks (ICT)
- H.323 gateways
- MGCP ports of the following types: T1, E1, PRI, FXO

Media devices, such as media termination points (MTP), conference bridges (CFB), annunciators, and music on hold (MOH) servers, do not need to be associated with geolocations and geolocation filters.

Internally, the device layer of Cisco Unified Communications Manager associates with geolocation values that call processing uses. The following sequence takes place:

1. Devices read the GeolocationPkid and GeolocationFilterPkid for its configuration at device or device-pool level.
2. The devices communicate this Pkid and deviceType information in CC (for example, CcRegisterPartyA) and PolicyAndRSVPRegisterReq messages during call signaling.
3. The call processing and feature layer uses this information for logical partitioning policy checking.

The standard record for a geolocation specifies *Unspecified*. Use this value when no geolocation needs to associate with a device. For a device, if the geolocation specifies *Unspecified* or the geolocation filter specifies *None*, no identifier gets created, and the device does not participate in logical partitioning policy checks.

Be aware that the Default Geolocation enterprise parameter and the Logical Partitioning Default Filter enterprise parameter can be configured from drop-down list boxes on the Enterprise Parameters Configuration window.

Examples of Geolocations and Geolocation Filters

See Table 24-4 in the "Geolocations and Location Conveyance" chapter for examples of geolocations.

See Table 24-6 in the "Geolocations and Location Conveyance" chapter for examples of geolocation filters.

Additional Information

See the "Related Topics" section on page 32-47.

Logical Partitioning Geolocation Usage for Shared Lines and Route Lists

When the called party specifies a group device, a different geolocation can apply for each device in a group. For the early attended scenarios, the actual connected device is not known until the device gets answered. Thus, the Geolocation information gets aggregated until the device answers.

- The Call Control and Feature layer receives temporary geolocation information (“MixedDevice”) until the device answers.
- The logical partitioning policy checks in the feature layer or LPSession process get ignored until the device answers and the actual geolocation information for the device becomes available.
- This behavior impacts the Early attended Transfer and Early attended Conference features by delaying the logical partitioning policy check until answer time.

Additional Information

See the “Related Topics” section on page 32-47.

Logical Partitioning Usage of Geolocation Identifiers

Geolocation identifiers get constructed from a combination of geolocations, geolocation filters, and device types of Cisco Unified Communications Manager devices.

See the “Geolocation Identifiers” section on page 24-8 of the “Geolocations and Location Conveyance” for details.

Additional Information

See the “Related Topics” section on page 32-47.

Enterprise Parameters for Logical Partitioning

You can use the following enterprise parameters to configure logical partitioning:

- Enable Logical Partitioning—This parameter determines whether the logical partitioning feature is enabled. Logical partitioning policies get used for restricting calls and other supplementary features such as transfer, forward, conferences including Meet-Me, and so on. Valid values specify True (enable logical partitioning) or False (do not enable logical partitioning). When this parameter is set to False, calls do not get validated against any logical partitioning policy. This represents a required field. The default value specifies *False*.
- Default Geolocation—This parameter determines the default geolocation setting for all devices and device pools that do not have a specified geolocation in Cisco Unified Communications Manager Administration. Valid values include the names of all the geolocations that have been configured in the Geolocation Configuration window in Cisco Unified Communications Manager Administration. The default geolocation can get overridden on a per-device and per-device-pool basis in the Device Configuration window or the Device Pool Configuration window in Cisco Unified Communications Manager Administration. This represents a required field. The default value specifies *Unspecified*.
- Logical Partitioning Default Policy—This parameter determines the default policy for allowing or denying calls between geolocations. Before calls between geolocations are allowed to proceed, Cisco Unified Communications Manager checks to be sure that calls are allowed between the specified geolocations based on the setting in the Logical Partitioning Policy Configuration window in Cisco Unified Communications Manager Administration. If Use System Default is specified in

the Logical Partitioning Policy Configuration window, the value in this parameter determines whether calls are allowed or denied. Valid values specify Allow (allow calls to proceed) or Deny (do not allow calls to proceed). This represents a required field. The default value specifies *Deny*.

- Logical Partitioning Default Filter—This parameter determines the default filter for geolocations in the logical partitioning feature. Applying a filter to geolocations allows you to reduce the number of fields on the Geolocation Configuration window that apply to devices and device pools that belong to that geolocation. To choose a filter in this parameter, you must ensure that the filter is already configured in the Geolocation Filter Configuration window in Cisco Unified Communications Manager Administration. Valid values include None (do not include any geolocation fields) and the names of all the filters that are configured in the Geolocation Filter Configuration window in Cisco Unified Communications Manager Administration. The default value specifies *None*.

Additional Information

See the "Related Topics" section on page 32-47.

Logical Partitioning Policies

Ensure logical partitioning policies are configured for the required interconnection behavior between the following entities:

- Between PSTN gateways and VoIP phones
- Between PSTN gateway and PSTN gateway
- Between an intercluster trunk (ICT) and a VoIP phone
- Between an ICT and a VoIP gateway

The System Default Policy enterprise parameter (Default value=DENY) represents the default policy when no configured policy is found.

Ensure Allow and Deny policies are configured. See the "Allow and Deny Policies" section on page 32-6 for configuration details.

In the Logical Partitioning Policy Configuration window (**Call Routing > Logical Partitioning Policy Configuration** menu option in Cisco Unified Communications Manager Administration), the administrator must create geolocation policy records from a subset of the fields that are configured for geolocations. See the "Logical Partitioning Policy Configuration" section on page 32-40 for details of using Cisco Unified Communications Manager Administration to create logical partitioning policy records.

Configure logical partitioning policies between pairs of geolocation policy records and device types.

Example of Logical Partitioning Policy

({geolocpolicy1, devType1}, {geolocpolicy2, devType2}, Allow)

The following tables show the construction of a logical partitioning policy among geolocations, device types, and policy types.

First, assume the following geolocation policy records:

Geolocation Policy	Record Data
BLRBLD1GeolocPolicy	(country=IN, A1=KA, A3=Bangalore, LOC=BLD1)
BLRBLD2GeolocPolicy	(country=IN, A1=KA, A3=Bangalore, LOC=BLD2)

Geolocation Policy	Record Data
MUMBLD1GeolocPolicy	(country=IN, A1=MH, A3=Mumbai, LOC=BLD1)
blankGeolocPolicy	() – All fields blank

From these records, you can configure the following sample logical partitioning policies. The system default policy specifies DENY.

Source		Target		
DevType1	GeolocationPolicy1	DevType2	GeolocationPolicy2	Policy
Border	BLRBLD1GeolocPolicy	Interior	BLRBLD1GeolocPolicy	ALLOW
Border	BLRBLD1GeolocPolicy	Border	BLRBLD1GeolocPolicy	ALLOW
Border	BLRBLD2GeolocPolicy	Interior	BLRBLD2GeolocPolicy	ALLOW
Border	BLRBLD2GeolocPolicy	Border	BLRBLD2GeolocPolicy	ALLOW
Border	MUMBLD1GeolocPolicy	Interior	MUMBLD1GeolocPolicy	ALLOW
Border	MUMBLD1GeolocPolicy	Border	MUMBLD1GeolocPolicy	ALLOW

The first logical partitioning policy,

Border	BLRBLD1GeolocPolicy	Interior	BLRBLD1GeolocPolicy	ALLOW

allows all the traffic to and from gateways that match BLRBLD1GeolocPolicy to and from VoIP phones that match BLRBLD1GeolocPolicy.

If more granular policies are required, the geolocation NAM field allows naming the devices within a building.

Example

- Between desktop phones and gateway1 in BLD1 of Bangalore

  Interior:(country=IN, A1=KA, A3=Bangalore, LOC=BLD1, NAM=deskphone)

  Border:(country=IN, A1=KA, A3=Bangalore, LOC=BLD1, NAM=gateway1) = Allow
- Between Cisco IP Softphones and ICT1 in BLD1 of Bangalore

  Interior:(country=IN, A1=KA, A3=Bangalore, LOC=BLD1, NAM=softphone)

  Border:(country=IN, A1=KA, A3=Bangalore, LOC=BLD1, NAM=ICT1) = Allow

Devices that have geolocation fields that match the preceding policies can communicate as per policy.

See the "Logical Partitioning Policy Configuration" section on page 32-40 for details of how to use Cisco Unified Communications Manager Administration to configure logical partitioning policies.

Additional Information

See the "Related Topics" section on page 32-47.

LPPolicyManager and Policy Tree

LPPolicyManager specifies a singleton process that interfaces with database and maintains policies in call processing as logical partitioning policy tree. During Cisco Unified Communications Manager service startup, the LPPolicyManager reads the policies from database tables and constructs the logical partitioning policy tree.

The add/delete/update of a policy in the database results in change notification to LPPolicyManager, and the change takes place in the logical partitioning policy tree.

Call processing interfaces with LPPolicyManager to read the logical partitioning policies that correspond to the geolocation policy records for the devices.

The LPPolicyManager provides utility functions for these search types:

- Geolocation information for a pair of devices
- Geolocation information for existing devices versus a new participant
- Geolocation information for existing devices versus list of new participants

Policy Tree Example

This section presents examples of a policy tree.

Figure 32-1 provides an example of a policy tree for logical partitioning policies for India cluster between geolocation policy records for gateways in Bangalore (BLD1, BLD2) and VoIP phones in Bangalore (BLD1, BLD2).

Note Normally, only one pair of policies gets configured between a particular source geolocation policy record and a particular target geolocation policy record.

The policy tree gets constructed so that a paired policy is represented as a source and target portions on the tree.

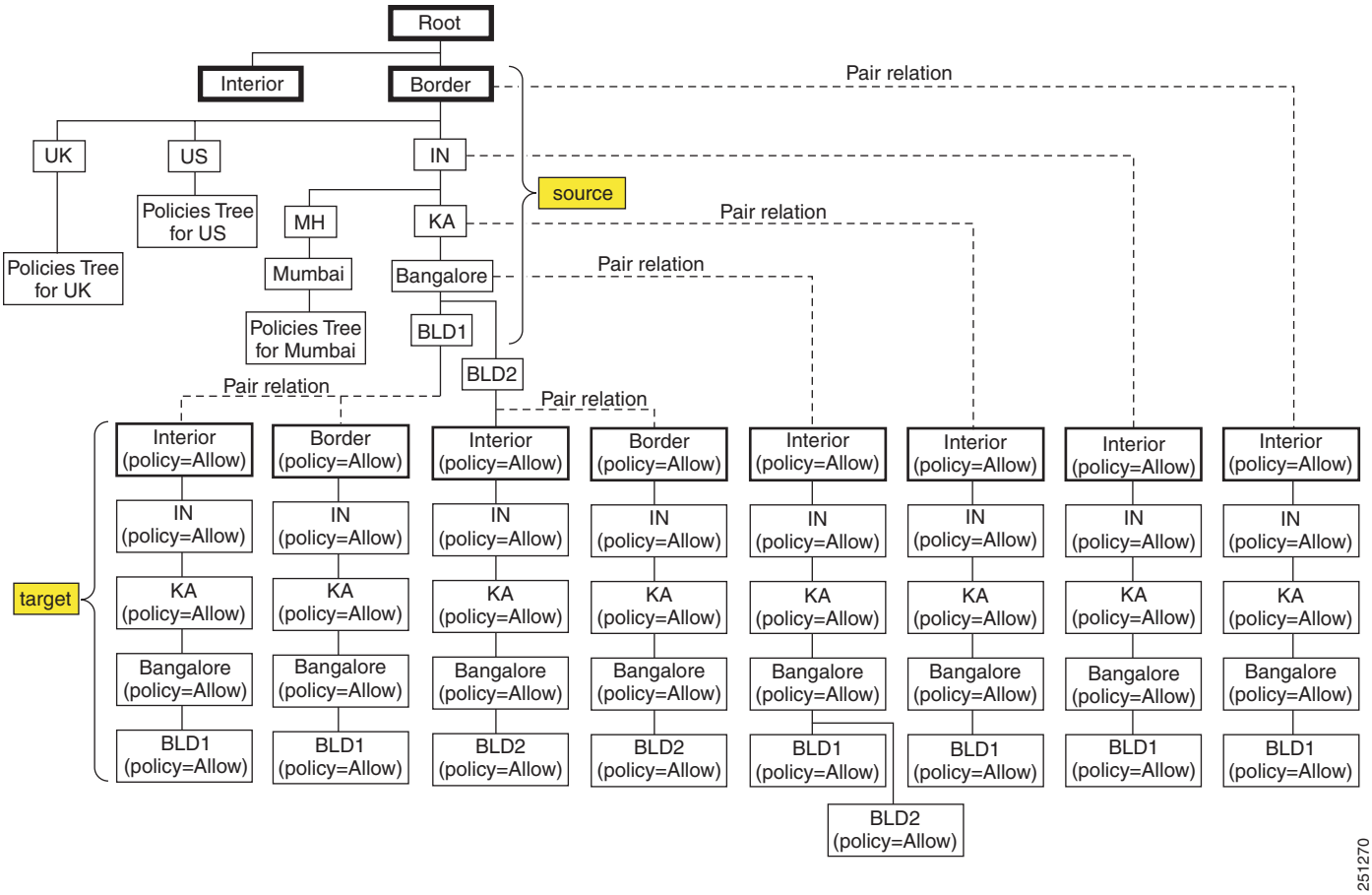
For example, the policy records with data Src=Border:IN:KA:Bangalore:BLD1 and Target=Interior:IN:KA:Bangalore:BLD1 with policy *Allow* associate with the following nodes:

- Border, IN, KA, Bangalore, BLD1 in the source portion
- Interior, IN, KA, Bangalore, BLD1 in the target portion

For this example, the Allow policy gets configured in the leaf node of the target portion.

The figure shows that the target portion of the tree can have a possible policy at each level. That is, each node (Interior, IN, KA, Bangalore, and BLD1) can have a policy.

Figure 32-1 Example Policy Tree for Logical Partitioning Policies for India Cluster



See the "Logical Partitioning Policy Search Algorithm" section on page 32-15 for a discussion of the logical partitioning policy search algorithm for searching through a policy tree. Table 32-3 on page 32-16 provides a listing that shows all permutations of possible policies that are found in this example policy tree.

Policy Tree Construction

The policy tree construction follows a fixed algorithm. The policy tree includes a source portion and a target portion.

1. [GLP_X Border GLP_Y Interior] policy gets added. The construction takes the source portion from GLP_X Border and the target portion from GLP_Y Interior.
2. [GLP_Y Interior GLP_X Border] policy gets added. The construction takes the source portion from GLP_X Border and the target portion from GLP_Y Interior.

Thus, the Border-to-Interior policy specifies that the Border part always originates in the source portion of the tree. The policy gets added in a leaf node.

3. [GLP_X Border GLP_Y Border] policy gets added.

First, a determination decides whether to add GLP_X in the source portion or GLP_Y in the source portion.

If no existing policy matches any tokens of GLP_X or GLP_Y (due to other GLP policy), the tree construction takes the source portion from GLP_X Border and the target portion from GLP_Y Border.

If an existing policy matches some tokens in the source portion, the source portion gets taken from that GLP.

Example 1: GLP_Y Border GLP_X Interior is already configured.

Because GLP_Y is already used in the source portion, to add the [GLP_X Border GLP_Y Border] policy, the GLP_Y gets added in the source portion.

Example 2: If the two policies, [GLP_X Border GLP_Y Interior] and [GLP_Y Border GLP_X Interior] exist, two source branches exist that both start with Border.

Assume that GLP_B overlaps more tokens with GLP_X (as compared to GLP_Y) and GLP_A does not match any Border branches.

To add the [GLP_A Border GLP_B Border] policy, the policy gets searched as to whether GLP_A or GLP_B can fit in the existing source branches.

As GLP_B matches some tokens from GLP_X, the portion of the tree gets shared with GLP_X.

Assume that Border:IN:KA:BLR:BLD1 to Border:IN:MH:MUM:BLD1 exists.

Adding Border:IN:MH:Pune:BLD1 to Border:IN:KA:BLR:BLD2 policy uses the source portion of Border:IN:KA:BLR and adds BLD2 in the leaf of the source tree and adds a target portion of Border:IN:MH:Pune:BLD1.

Thus, for Border-to-Border policies, the policy tree gets constructed to fit best in the existing source and target branches. Consider sharing as many nodes as possible as preferable.

Additional Information

See the "Related Topics" section on page 32-47.

Logical Partitioning Policy Search Algorithm

This section explains the logical partitioning policy search algorithm.

The logical partitioning policy search algorithm functions as follows:

- Policies get searched during call control or feature interactions.
- The configured tree of policies gets used for run-time searching of the configured policy by using tree traversal.
- The policy gets searched between a pair of devices by using geolocation information (that is, geolocation, geolocation filter, and device type) of both the source (A) device and target (B) device.

Basic Operation

Construct a list of name/value pairs from the geolocation and geolocation filter information (that is, pairList1 and pairList2).

Example: pairList ="Country=IN:A1=KA:A3=Bangalore:LOC=BLD1"

Input for the search specifies {pairList1, devType1}, {pairList2, devType2}.

The following steps take place during the policy search:

Step 1 If devType1=Border and devType2=Interior, set {devTypeA=devType1, pairListA= pairList1} and {devTypeB=devType2, pairListB= pairList2}.

Step 2 If devType1=Interior and devType2=Border, set {devTypeA=devType2, pairListA= pairList2} and {devTypeB=devType1, pairListB= pairList1}.

Step 3 Match the exact pair by searching the nodes of a policy tree. Use values from {devTypeA, pairListA} and find the source branch of the tree.

Step 4 Use values from {devTypeB, pairListB} and find the target (paired) branch of the tree.

Step 5 If an exact match is found in the tree and the policy is configured, use the policy data that is configured in the leaf node and return the policy value.

Step 6 If exact match is not found, find a match by stripping one column from pairListB input (that is, go one level up on target [paired] branch of policy tree and check whether policy data is configured in the corresponding node).

Step 7 If a match is found, return the policy value; otherwise, continue going up the paired branch of the policy tree and check whether policy data is configured.

Step 8 If a policy is not found, go one level (node) up on the source branch that corresponds to pairListA.

Step 9 Repeat Step 4 through Step 8 until a policy is found or the root node is reached.

Step 10 If devType1=Border and devType2=Border, search for exact match by traversing. Use {devTypeA=devType1, pairListA= pairList1}, and {devTypeB=devType2, pairListB= pairList2}. If not found, traverse and use {devTypeA=devType2, pairListA= pairList2} and {devTypeB=devType1, pairListB= pairList1}.

Note The tree layout can specify any order, based on how the administrator added policies, so you need to use both combinations to search the tree.

Assume that the policy is searched with the following data:

(devTypeA = “Border”, pairListA = “Country=IN:A1=KA:A3=Bangalore:LOC=BLD1”, devTypeB = “Interior”, pairListB = “Country=IN:A1=KA:A3=Bangalore:LOC=BLD1”).

In Table 32-3 that shows all permutations of possible policies, any value specifies a match. The search algorithm proceeds in the order that the table specifies for finding the configured policy.

The first found match specifies an entry from which the configured policy gets used.

Table 32-3 Example of Policy Variations in Policy Configuration and Order of Policy Search

GeolocationValueA	GeolocationValueB	Policy
Border:IN:KA:Bangalore:BLD1	Interior:IN:KA:Bangalore:BLD1	Allow/Deny
Border:IN:KA:Bangalore:BLD1	Interior:IN:KA:Bangalore	Allow/Deny
Border:IN:KA:Bangalore:BLD1	Interior:IN:KA	Allow/Deny
Border:IN:KA:Bangalore:BLD1	Interior:IN	Allow/Deny
Border:IN:KA:Bangalore:BLD1	Interior	Allow/Deny
Border:IN:KA:Bangalore	Interior:IN:KA:Bangalore:BLD1	Allow/Deny
Border:IN:KA:Bangalore	Interior:IN:KA:Bangalore	Allow/Deny
Border:IN:KA:Bangalore	Interior:IN:KA	Allow/Deny
Border:IN:KA:Bangalore	Interior:IN	Allow/Deny
Border:IN:KA:Bangalore	Interior	Allow/Deny

Table 32-3 Example of Policy Variations in Policy Configuration and Order of Policy Search (continued)

GeolocationValueA	GeolocationValueB	Policy
Border:IN:KA	Interior:IN:KA:Bangalore:BLD1	Allow/Deny
Border:IN:KA	Interior:IN:KA:Bangalore	Allow/Deny
Border:IN:KA	Interior:IN:KA	Allow/Deny
Border:IN:KA	Interior:IN	Allow/Deny
Border:IN:KA	Interior	Allow/Deny
Border:IN	Interior:IN:KA:Bangalore:BLD1	Allow/Deny
Border:IN	Interior:IN:KA:Bangalore	Allow/Deny
Border:IN	Interior:IN:KA	Allow/Deny
Border:IN	Interior:IN	Allow/Deny
Border:IN	Interior	Allow/Deny
Border	Interior:IN:KA:Bangalore:BLD1	Allow/Deny
Border	Interior:IN:KA:Bangalore	Allow/Deny
Border	Interior:IN:KA	Allow/Deny
Border	Interior:IN	Allow/Deny
Border	Interior	Allow/Deny

For a given pair of geolocation identifiers, if no configured policy is found, the Logical Partition Default System Policy gets used.

Additional Information

See the "Related Topics" section on page 32-47.

Policy Matching

Policy checking takes place in the following situations:

- Policy checking occurs for all calls that connect a PSTN gateway and a VoIP phone.
- Policy checking occurs for all calls that invoke supplementary services, such as Transfer and Conference, that connect a PSTN gateway and VoIP phones.
- All restricted calls and connections based on policies get denied.

Additional Information

See the "Related Topics" section on page 32-47.

Deny Policy Handling

When calls are denied because of logical partitioning policy, the following handling occurs:

- Basic calls get cleared with a reorder tone that Cisco Unified Communications Manager sends.
  - Q.850-compliant devices (SCCP, H323. MGCP) get cleared by using cause code=63 “Service or option not available.”
  - SIP line or trunk gets cleared by using SIP status code=503 “Service unavailable.”
- Features get handled based on the individual feature
  - If call clearing is involved, the cause code=63 or SIP status code=503 gets used.
  - Feature=based message gets sent to VoIP phones for display on the status line.
  - For analog phones that invoke a feature, Transfer results in both calls getting cleared. Conference clears the secondary call to play reorder tone to the analog phone.

Additional Information

See the “Related Topics” section on page 32-47.

LPSession Infrastructure and Policy Checking

LPSession specifies an infrastructure that enhances the Cisco Unified Communications Manager Resource Reservation Protocol (RSVP) infrastructure to provide a centralized policy-checking infrastructure.

Note The enhancement of the RSVP infrastructure is based on similar paired policy checking behavior for logical partitioning. Logical partitioning has no impact on RSVP policy checking and vice-versa.

The following operations use LPSession infrastructure for policy checking:

- Basic calls
- Redirections (for example, Forwarding, Redirecting features, and Park reversion)
- Split/Join primitive

The commonly used features perform logical partitioning policy checks in the feature layer before Split/Join or Redirection:

- Transfer
- Ad Hoc Conference
- Meet-me Conference
- Pickup
- Call Park and Directed Call Park

Other existing Split/Join features and similar features depend on LPSession infrastructure for Split/Join primitive-level policy checking (for example, MKI for Cisco Unified Mobility).

Additional Information

See the “Related Topics” section on page 32-47.

Logical Partitioning Handling for a Basic Call

This section describes logical partitioning handling with a basic call.

Operation

The logical partitioning policy gets checked between the geolocation policy records of the calling device and the called device.

Configuration

The calling device and the called device both associate with a geolocation and geolocation filter.

When

Logical partitioning handling takes place in the following circumstances:

- During a basic call between a VoIP phone and a PSTN gateway, a PSTN gateway and another PSTN gateway, an ICT and a PSTN gateway, or an ICT and another ICT.
- During Post Digit Analysis, which uses configured calling search spaces and partitions for routing the calls.
- Cisco Unified Communications Manager uses the geolocation identifier information that associates with the incoming and outgoing Cisco Unified Communications Manager device to perform logical partitioning policy checking.
- The configured logical partitioning policy returns to an outgoing Cisco Unified Communications Manager device layer, which takes action accordingly.

When Not

Logical partitioning handling does not take place in the following circumstances:

- When both the calling and called devices specify VoIP phones (DevType=Interior).
- When geolocation or geolocation filter is not associated with any device.

Deny Handling

Logical partitioning handles a denied call as follows:

- The call gets denied/rejected with a reorder tone.
- The call does not get extended to a phone, gateway, or intercluster trunk.
- The Number of Basic Call Failures perfmon counter gets incremented.

Additional Information

See the "Related Topics" section on page 32-47.

Logical Partitioning Interaction with Geolocation Conveyance Across SIP Trunks and Intercluster Trunks

If logical partitioning applies to a multicluster environment, ensure location conveyance is configured.

Location conveyance configuration entails the same configuration as logical partitioning configuration for a single-cluster environment, but additional configuration must take place for devices that belong to remote clusters.

For the details of configuring logical partitioning for systems that do not require location conveyance, see the "Configuration Checklist for Logical Partitioning" section on page 32-1.

To support logical partitioning scenarios that involve participants across clusters requires the following support from SIP trunks and intercluster trunks:

- The geolocation and device type information gets sent from one cluster to another cluster.
- This information gets sent both at call establishment and at midcall joins and redirects.
- The geolocation filter gets configured on the trunk.
  - This configuration allows creation of geolocation identifiers. Based on these geolocation identifiers, policy records may be configured for logical partitioning policy checks.

The geolocation gets sent across clusters if the Send Geolocation Information check box gets checked upon configuration of the SIP trunk or intercluster trunk:

- If geolocation is configured for a device, the geolocation information gets sent in call signaling across the trunk for SIP trunk or intercluster trunk interactions.

Note Location conveyance does not depend on any logical partitioning configuration.

For additional details, see the "Geolocation Conveyance Across SIP Trunks and Intercluster Trunks" section on page 24-22.

The "Configuration Checklist for Location Conveyance" section on page 24-4 provides a detailed checklist for configuring location conveyance.

Additional Information

See the "Related Topics" section on page 32-47.

Logical Partitioning Handling of a Received Geolocation

If the receiving cluster is enabled for logical partitioning, the receiving cluster uses the received PIDF-LO geolocation information for logical partitioning policy checks with the devices on Cisco Unified Communications Manager.

For additional details, see the "Handling a Received Geolocation" section on page 24-23.

Also, see the "Interactions" section on page 32-22 for a list of features that use geolocation information for policy checking.

Additional Information

See the "Related Topics" section on page 32-47.

Logical Partitioning Feature Interactions with Midcall Geolocation Change

If logical partitioning is enabled, the following actions take place:

- SIP trunk or intercluster trunk checks the logical partitioning policy and takes an action that is based on the configured policy.
- The feature layer, such as Conference or Meet-me, rechecks the logical partitioning policy based on the updated geolocation information for the trunk device.

For feature interactions that involve a midcall geolocation change, see the "Feature Interactions with Midcall Geolocation Change" section on page 24-23.

Also, see the "Interactions" section on page 32-22 for a list of features that use geolocation information for policy checking.

Additional Information

See the "Related Topics" section on page 32-47.

Dynamic SIP Trunks

For dynamic SIP trunks, such as Cisco Intercompany Media Engine (IME), Service Advisement Framework (SAF), or Cisco Extension Mobility Cross Cluster (EMCC), the target cluster varies depending on the pointed destination. The device-level geolocation and geolocation filter that can be configured on these trunks may not have the flexibility to vary depending on the destination. Such SIP trunks must be configured appropriately to allow or deny traffic from these trunks. Cisco Systems recommends using location conveyance functionality, which allows the actual geolocation to propagate across clusters and helps in accurate logical partitioning policy checking.

Additional Information

See the "Related Topics" section on page 32-47.

SIP Trunk or Intercluster Trunk Configuration Requirement for Logical Partitioning

A cluster for which logical partitioning is enabled exhibits the following typical behaviors:

1. Traffic between VoIP phones and SIP trunk (or intercluster trunk [ICT]) gets allowed.
2. Traffic between SIP trunk (or ICT) and PSTN gateways gets blocked.
3. VoIP-only traffic between SIP trunk (or ICT) and SIP trunk (or ICT) gets allowed.

Logical partitioning policies must get configured to achieve these behaviors.

Interaction with Non-Location Conveyance Cluster

To achieve behaviors 1 and 3, you need to configure one policy each. If default policy specifies Deny, you do not need any policy for behavior 2.

For behaviors 1 and 3, because no location conveyance exists, a logical partitioning cluster cannot identify whether traffic is VoIP-only or comes from a gateway in a remote cluster. This means that typically, all traffic must be allowed from SIP trunk (or ICT) to VoIP phones or other SIP trunk (or ICT).

Interaction with Location Conveyance Cluster

For behavior 1, the VoIP phone that calls a SIP trunk (or ICT) needs a policy that allows extension of the call on the trunk. This occurs before receipt of location conveyance information from the remote cluster.

For incoming VoIP call from SIP trunk (or ICT), you do not need any policy for calling VoIP phones. If traffic from SIP trunk (or ICT) needs to be allowed to any other ICT or PSTN gateway, you require a corresponding policy.

Example

Ensure the SIP trunk that points from Bangalore to RCDN cluster is configured as follows:

Geolocation = "IN:KA:Bangalore:ICTToRCDN"

Geolocation Filter = "UseCountry, UseA1, UseA3, UseNam"

This configuration specifies the geolocation identifier for SIP trunk as follows:

{“IN:KA:Bangalore:ICTToRCDN”, devType=Border}

Configure logical partitioning policies as follows:

“Border:IN:KA:Bangalore:ICTToRCDN” to Interior = Allow
Result: All VoIP phones in Bangalore cluster can communicate with Richardson.

“Border:IN:KA:Bangalore:ICTToRCDN” to “Border:IN:KA:Bangalore:ICTToRCDN” = Allow
Result: ICTs can communicate.

These policies fulfill behavior 1 and 3 requirements.

For location conveyance scenarios, ensure the policies are configured based on geolocation configurations and device type for devices across the cluster.

Additional Information

See the “Related Topics” section on page 32-47.

System Requirements for Logical Partitioning

Logical partitioning requires the following software components:

- Cisco Unified Communications Manager 7.1 or later
- Cisco CallManager service that is running on at least one server in the cluster
- Cisco Unified Communications Manager Locale Installer, that is, if you want to use non-English phone locales or country-specific tones
- Microsoft Internet Explorer 7 or Microsoft Internet Explorer 8 or FireFox 3.x or Safari 4.xr

Additional Information

See the “Related Topics” section on page 32-47.

Interactions and Limitations

The following sections describe the interactions and restrictions for logical partitioning:

- Interactions, page 32-22
- Limitations, page 32-37

Additional Information

See the “Related Topics” section on page 32-47.

Interactions

The following sections detail the interactions between logical partitioning and the supplementary features and call processing entities that are listed.

Note Configure the Logical Partitioning Default Policy enterprise parameter, and configure a corresponding logical partitioning policy through the **Call Routing > Logical Partitioning Policy Configuration** menu option.

- Call Forwarding, page 32-23
- Call Transfer, page 32-24
- Ad Hoc Conference, Join, Join Across Lines (JAL), page 32-27
- Meet-Me Conference, page 32-28
- Call Pickup, page 32-29
- Call Park and Directed Call Park, page 32-30
- Cisco Extension Mobility, page 32-31
- Cisco Unified Mobility, page 32-32
- Shared Line, page 32-33
- Barge, cBarge, and Remote Resume, page 32-34
- Route Lists and Hunt Pilots, page 32-35
- CTI Handling, page 32-36

Logical partitioning also interacts with the following Cisco Unified Communications Manager components:

- Bulk Administration Tool—For information on how the Bulk Administration Tool (BAT) supports logical partitioning, see the *Cisco Unified Communications Manager Bulk Administration Guide*.
- Call Detail Records—For logical partitioning failures, existing call termination cause codes and new Cisco-specific call termination cause codes get used. For more information on CDRs, see the *Cisco Unified Communications Manager Call Detail Records Administration Guide*.
- Real Time Monitoring Tool—The Real Time Monitoring Tool provides a set of performance monitoring (perfmon) counters for the Cisco Call Restriction object that increment in the event of logical partitioning failures. The Real Time Monitoring Tool also tracks a Logical Partitioning Failures Total counter in the Call Activity window. For more information on the Real Time Monitoring Tool, see the *Cisco Unified Real Time Monitoring Tool Administration Guide*.
- Cisco Unified Reporting—Cisco Unified Reporting generates reports that provide information about logical partitioning policies. For more information on the reports that Cisco Unified Reporting generates, see the *Cisco Unified Reporting Administration Guide*.

Additional Information

See the "Related Topics" section on page 32-47.

Call Forwarding

This section describes the interaction of logical partitioning with the Call Forwarding feature.

Operation

The logical partitioning policy check gets performed between the geolocation identifier of the device from which call is coming and the device to which the call is forwarded.

Configuration

The caller device and a forwarded device associate with a geolocation and geolocation filter.

When

Logical partitioning handling takes place in the following circumstances:

- When an incoming call is received for a device that is call forwarded to another device, the Forwarding feature invocation takes place.
- One of the devices specifies a PSTN participant.
- Cisco Unified Communications Manager uses the geolocation identifier information that associates with the incoming and forwarded Cisco Unified Communications Manager devices for performing logical partitioning policy checking.
- The configured logical partitioning policy returns to the forwarded Cisco Unified Communications Manager device, which takes action accordingly.
- This handling applies to all variations of call forwarding; for example, Call Forward All (CFwdAll), Call Forward No Answer (CFNA), and Call Forward Busy (CFB).

When Not

Logical partitioning handling does not take place in the following circumstances:

- When both the caller and forwarded devices are VoIP phones (DevType=Interior).
- When geolocation or geolocation filter does not associate with any device.

Deny Handling

Logical partitioning handles a denied call as follows:

- The calling device receives a reorder tone from Cisco Unified Communications Manager.
  - Q.850-compliant devices (phone that is running SCCP, H323, or MGCP device) get cleared by using cause code=63 “Service or option not available.”
  - SIP line or trunk gets cleared by using SIP status code=503 “Service unavailable.”

Additional Information

See the “Related Topics” section on page 32-47.

Call Transfer

This section describes the interaction of logical partitioning with the Call Transfer feature.

Operation

The logical partitioning policy check gets performed between the geolocation identifier of the device that is acting as a transferred party and the geolocation identifier of the device that is acting as a transferred destination.

Configuration

The transferred device and a transferred destination device associate with a geolocation and geolocation filter.

When

Logical partitioning handling takes place in the following circumstances:

- When a phone uses a Transfer softkey to transfer the call, the second Transfer key press results in Transfer feature invocation and processing.
- Similarly, other mechanisms (for example, Direct Transfer, OnHook Transfer, Hook Flash Transfer, CTI-application-initiated Transfer) that result in Transfer feature invocation get included.
- The transferred or/and transferred destination specifies a PSTN participant.
- Cisco Unified Communications Manager uses the geolocation identifier information that associates with the transferred and transferred destination Cisco Unified Communications Manager device to perform logical partitioning policy checking.
- This handling normally gets performed before splitting of the primary and secondary calls and before joining.

When Not

Logical partitioning handling does not take place in the following circumstances:

- When both the Transferred and Transferred Destination devices are VoIP phones (DevType=Interior).
- When geolocation or geolocation filter does not associate with any device.

Deny Handling

Logical partitioning handles a denied call as follows:

- Sends External Transfer Restricted message to the VoIP phone.
- Normal Transfer—For phone that is running SCCP, the primary call remains on hold, and consultation call remains active. For phone that is running SIP, both primary and consultation calls remain on hold and need to be resumed manually after the failure.
- Onhook, HookFlash and Analog-Phone-Initiated Transfer—Both the primary and secondary calls get cleared by using cause code=63 “Service or option not available” with a reorder tone from Cisco Unified Communications Manager.
- The Number of Transfer Failures perfmon counter gets incremented.

Interaction with Block OffNet to OffNet Transfer Service Parameter

The Block OffNet to OffNet Transfer service parameter allows the Transfer feature to block the transfer operation when both Transferred and Transferred Destinations specify offnet calls.

See the “Setting the Block OffNet to OffNet Transfer Service Parameter” section on page 23-7 in the “External Call Transfer Restrictions” chapter of this guide for more information about this service parameter.

The Cisco Unified Communications Manager cluster that is disabled for logical partitioning retains the expected behavior that this service parameter specifies.

Logical Partitioning-Enabled Cluster

In a logical partitioning-enabled Cisco Unified Communications Manager cluster, you can configure the system to allow multiple Voice Gateway (PSTN) participants that use the GeolocationPolicy, GLPolicyX, in a supplementary feature by configuring a policy such as the following one:

GLPolicyX Border GLPolicyX Border Allow

After Cisco Unified Communications Manager configures such a policy, be aware that all features (such as Forwarding, Transfer, Ad Hoc Conference, and so forth) are allowed between participants that use GeolocationPolicy, GLPolicyX Border. For example, forwarding a call that comes from a party that uses GLPolicyX Border to another party that uses GLPolicyX Border gets allowed.

Assume that Cisco Unified Communications Manager deployment requires that all supplementary features except the Transfer feature function for such participants. If so, the Block OffNet to OffNet Transfer service parameter can block transfer between offnet devices even if the logical partitioning policy is allowed.

This service parameter controls only the blocking of offnet-to-offnet transfers and does not impact any other supplementary features. Thus, the following details highlight scenarios that involve voice-gateway-to-voice-gateway transfers.

Details

1. Border-to-Border Logical Partitioning Policy Specifies Deny

   For Transfer operation between parties that use this geolocation policy, Cisco Unified Communications Manager denies the transfer. The “External Transfer Restricted” message displays to the transferring party.

   The Cisco Unified Communications Manager setting (either True or False) for the Block OffNet to OffNet Transfer service parameter does not affect the Transfer operation.

   The logical partitioning Deny policy takes precedence, and Cisco Unified Communications Manager follows the policy strictly.

2. Border-to-Border Logical Partitioning Policy Specifies Allow

   For Transfer operation between parties that use this geolocation policy, Cisco Unified Communications Manager checks the allow policy and also checks the setting of the Block OffNet to OffNet Transfer service parameter. This service parameter thus affects the transfer between offnet participants.

   a. Block OffNet to OffNet Transfer service parameter specifies True—Cisco Unified Communications Manager checks whether both parties (transferred and transferred destination) are offnet. If so, the transfer of such calls gets denied, and the “External Transfer Restricted” message displays to the transferring party.

      Because transfer gets blocked due to the service parameter, the serviceability Perfmon counter for Logical Partitioning Transfer Failures does not increment.

   b. Block OffNet to OffNet Transfer service parameter specifies False—Transfer succeeds.

Offnet/Onnet Behavior for a Device

For outgoing calls, the Call Classification setting in the Route Pattern Configuration window determines the offnet or onnet value. The Call Classification value in the Route Pattern Configuration window overrides the device-level configuration or the corresponding value of the Call Classification service parameter.

For incoming calls, the device-level configuration or the corresponding Call Classification service parameter value determines the offnet or onnet value.

Additional Information

See the “Related Topics” section on page 32-47.

Ad Hoc Conference, Join, Join Across Lines (JAL)

This section describes the interaction of logical partitioning with the Ad Hoc Conference, Join, and JAL features.

Operation

Establishing Conference—The logical partitioning policies get checked between the geolocation identifiers of the devices that are invited to an ad hoc conference.

Established Conference—The logical partitioning policies get checked between the geolocation identifiers of each of the devices that are already in the conference and the device that is invited to the conference.

Configuration

The participant devices associate with a geolocation and a geolocation filter.

The conference bridge does not need to associate with geolocation or geolocation filter; only participants associate, and policy checks get performed for the participants.

When

Logical partitioning handling takes place in the following circumstances:

- A phone uses a Conference softkey to establish or extend an ad hoc conference or a CTI application initiates ad hoc conference.
- The second Conference key press results in conference feature invocation and processing.
- Cisco Unified Communications Manager uses participant geolocation identifier information for policy checking.
- In an established conference, policy checking occurs again, based on changed participant geolocation identifier information for midcall updates. For example, policy checking occurs during call state change, such as Alerting to Answer, Hold/Remote-Resume, Transfer, Call Park Retrieval, Redirection, and so forth.
- PSTN participants are involved.

When Not

Logical partitioning handling does not take place in the following circumstances:

- When all participants are VoIP phones (DevType=Interior).
- When geolocation or geolocation filter does not associate with a device, no policy check takes place for that device.

Deny Handling

Logical partitioning handles a denied conference as follows:

- For the establishing-conference case, the CFB does not get allocated.
- For phones that are running SCCP or phones that are running SIP, the primary call leg gets put on hold and the consultation call remains active. If the primary call leg needs to resume, resumption must take place manually.
- The Conference is Unavailable message gets sent to the VoIP phone that initiates the conference.

- When an analog phone initiates the conference, the secondary call gets cleared by using cause code=63 “Service or option not available” with a reorder tone from Cisco Unified Communications Manager.
- The Number of Adhoc Conference Failures perfmon counter increments.

Additional Information

See the “Related Topics” section on page 32-47.

Meet-Me Conference

This section describes the interaction of logical partitioning with the Meet-Me Conference feature.

Operation

The logical partitioning policies get checked between the geolocation identifiers of each of the devices that are already in the meet-me conference and the device that is attempting to join the conference.

Configuration

The participant devices associate with a geolocation and a geolocation filter.

Be aware that the conference bridge is not required to be associated with a geolocation or geolocation filter; only participants get associated, and policy checks get performed for the participants.

When

Logical partitioning handling takes place in the following circumstances:

- Requirement exists for PSTN participant involvement.
- Policy checks get supported during joining of participants. When a participant dials the meet-me number to join in a meet-me conference, the participant geolocation gets used for policy checking before the new participant is allowed to join the meet-me conference.
- In an established meet-me conference, the updated policy of the participant gets used for policy checking during midcall updates (such as Hold-Resume, Transfer, Barge, cBarge, Call Park Retrieval, and so forth).

When Not

Logical partitioning handling does not take place in the following circumstances:

- When all participants are VoIP phones (DevType=Interior), handling does not occur.
- When geolocation or geolocation filter does not associate with a device, no policy check takes place for that device.

Deny Handling

Logical partitioning handles a denied call as follows:

- The MeetMe is Unavailable message gets sent to the VoIP phone.
- The existing conference does not get affected.
- The call gets cleared with reorder tone from Cisco Unified Communications Manager.
  - Q.850-compliant devices (phone that is running SCCP, H323, or MGCP device) get cleared by using cause code=63 “Service or option not available.”

  - SIP line or trunk gets cleared by using SIP status code=503 “Service unavailable.”
- The Number of Meet-Me Conference Failures perfmon counter increments.

Additional Information

See the “Related Topics” section on page 32-47.

Call Pickup

This section describes the interaction of logical partitioning with the Call Pickup feature.

Operation

The logical partitioning policies get checked between the geolocation identifiers of the calling device and that of the device that picks up the call.

Configuration

The calling device and the device that attempts pickup associate with a geolocation and a geolocation filter.

When

Logical partitioning handling takes place in the following circumstances:

- A PSTN device calls a VoIP phone (A) to which another VoIP phone (B) has a Pickup group relation (for example, both phones belong to the same pickup group).
- When phone B attempts pickup by pressing either Pickup, OPickup, Group Pickup, or BLF Pickup button, the Pickup feature gets invoked.
- Cisco Unified Communications Manager uses geolocation identifier information of the calling device and of device picking up call for policy checking.
- When only one alerting call occurs, the corresponding logical partitioning policy gets treated as final.
- When multiple alerting calls occur, the logical partitioning policy gets checked for each alerting call, starting from the longest alerting call until logical partitioning policy is allowed and call is picked up. If last processed alerting call has logical partitioning Deny policy and no more alerting calls occur, deny handling action takes place.

When Not

Logical partitioning handling does not take place in the following circumstances:

- When the caller consists of a VoIP phone (DevType=Interior), handling does not occur.
- When geolocation or geolocation filter does not associate with devices, no policy check occurs.

Deny Handling

Logical partitioning handles a denied pickup as follows:

- PickUp is Unavailable message gets sent to the VoIP phone that attempts pickup.
- The alerting call does not get affected.
- For multiple alerting calls (mixture of Allowed and Deny policy), if a call with deny policy fails for pickup first, Cisco Unified Communications Manager proceeds by picking up the next alerting call.

- Cisco Unified Communications Manager sends reorder tone to the phone that attempts the pickup.
  - Q.850-compliant devices (phone that is running SCCP) get cleared by using cause code=63 “Service or option not available.”
  - SIP phone gets cleared by using SIP status code=503 “Service unavailable.”
- The Number of Pickup Failures perfmon counter increments.

Additional Information

See the “Related Topics” section on page 32-47.

Call Park and Directed Call Park

This section describes the interaction of logical partitioning with the Call Park and Directed Call Park features.

Operation

The logical partitioning policies get checked between the geolocation identifier of the device that is retrieving the call and the geolocation identifier of the parked party

Configuration

For Retrieval—The parked party and the device that attempts park retrieval associate with a geolocation and geolocation filter.

For Reversion—The parked party and device to which reversion happens associate with a geolocation and geolocation filter.

When

Logical partitioning handling takes place in the following circumstances:

- When a parked call exists and a device attempts a park retrieval, the Park retrieval feature gets invoked.
- When a parked call exists and the reversion timer expires, the Park reversion feature gets invoked.
- One party must be a PSTN participant.
- For Park retrieval, Cisco Unified Communications Manager uses geolocation identifier information of the parked device and of the device that performs park retrieval for policy checking.
- For Park reversion, Cisco Unified Communications Manager uses geolocation identifier information of the parked device and of the device to which call is redirected for policy checking.

When Not

Logical partitioning handling does not take place in the following circumstances:

- When the involved devices are VoIP phones (DevType=Interior), handling does not occur.
- When geolocation or geolocation filter does not associate with devices, no policy check occurs.

Deny Handling

Logical partitioning handles a denied retrieval/reversion as follows:

- For retrieval, Cannot Retrieve Parked Call message gets sent to the VoIP phone.
- Cisco Unified Communications Manager sends reorder tone to the phone that is attempting retrieval.
  - Q.850-compliant devices (phone that is running SCCP, H323, or MGCP device) get cleared by using cause code=63 “Service or option not available.”
  - Phone that is running SIP or SIP trunk gets cleared by using SIP status code=503 “Service unavailable.”
- For reversion, the parked call gets cleared with reorder tone.
- The Number of Park Retrieval Failures perfmon counter gets incremented (for both Call Park and Directed Call Park retrievals that get denied).

Additional Information

See the “Related Topics” section on page 32-47.

Cisco Extension Mobility

This section describes the interaction of logical partitioning with the Cisco Extension Mobility feature.

Operation

A user logs on to a VoIP phone by using Cisco Extension Mobility within the same Cisco Unified Communications Manager cluster. The incoming or outgoing calls from the phone get logical partitioning policy checked.

Configuration

The VoIP phone that is logged on to Cisco Extension Mobility and the PSTN access device both associate with a geolocation and geolocation filter.

When

Logical partitioning handling takes place in the following circumstances:

- A user logs on, by using Cisco Extension Mobility, to a device in a different geolocation as the device profile, and the user makes a PSTN call by using a gateway in the user home site, or the user receives an incoming PSTN call.
- Cisco Unified Communications Manager uses geolocation identifier information of the Cisco Extension Mobility logged-on device and the PSTN gateway device for policy checking.
- The configured logical partitioning policy returns to an outgoing Cisco Unified Communications Manager device layer, which takes action accordingly.

When Not

Logical partitioning handling does not take place in the following circumstances:

- Geolocation or geolocation filter does not associate with a VoIP phone that is logged on to Cisco Extension Mobility nor with the calling party nor called party device.
- The VoIP phone that is logged on to Cisco Extension Mobility calls or receives a call from a VoIP phone (DevType=Interior).

Deny Handling

Logical partitioning handles a denied call as follows:

- If the VoIP phone that is logged in to Cisco Extension Mobility places a PSTN call that should be denied per logical partitioning, the call gets rejected with a reorder tone.
- If the VoIP phone that is logged in to Cisco Extension Mobility receives a PSTN call that should be denied per logical partitioning, the call gets rejected with a reorder tone.

Additional Information

See the "Related Topics" section on page 32-47.

Cisco Unified Mobility

This section describes the interaction of logical partitioning with the Cisco Unified Mobility feature. These interactions apply to calls that involve Mobile Connect or Mobile Voice Access.

Operation

Logical partitioning interacts with Cisco Unified Mobility as follows:

- Single-Number-Reach (SNR) Call—The SNR call gets logical partitioning policy checked between a calling device and a PSTN gateway that connects the mobile device.
- Cell Pickup—The Cell Pickup operation from a desktop phone attempts to join the already connected call with a PSTN gateway that connects the remote destination mobile device. The logical partitioning policy gets checked before joining the call by using the geolocation identifiers for the involved devices.
- Mobile Voice Access—The logical partitioning policy gets checked between the geolocation identifier of the incoming gateway and the geolocation identifier of the called party device.

Configuration

The involved devices and the PSTN access gateway must associate with a geolocation and geolocation filter.

When

Logical partitioning handling takes place in the following circumstances:

- Single-Number-Reach (SNR) Call

  Cisco Unified Mobility gets configured for an enterprise extension, and a call is received for SNR from a VoIP phone or another PSTN gateway.

  Cisco Unified Communications Manager uses the geolocation identifier information that associates with calling and called Cisco Unified Communications Manager device to perform logical partitioning policy checking.

  The configured logical partitioning policy returns to the called Cisco Unified Communications Manager device layer, which takes action accordingly.

- Cell Pickup

  Cisco Unified Mobility gets configured for an enterprise extension, and a call is active between a VoIP phone (SNR) and another VoIP phone or a PSTN gateway (termed the connected party).

  The VoIP phone (SNR) performs Cell Pickup to Mobile, which tries to join the connected party with the PSTN gateway that was used to reach the mobile phone.

Cisco Unified Communications Manager uses the geolocation identifier information that associates with the PSTN gateway and the connected party for performing logical partitioning policy checking.

The configured logical partitioning policy decides whether the Cell Pickup operation succeeds or fails.

- Mobile Voice Access

  Cisco Unified Mobility gets configured for an enterprise extension, and a mobile phone calls from a PSTN gateway to an enterprise VoIP phone.

  Cisco Unified Communications Manager uses the geolocation identifier information that associates with the calling PSTN gateway and called VoIP phone to perform logical partitioning policy checking.

  The configured logical partitioning policy returns to the called Cisco Unified Communications Manager device layer, which takes action accordingly.

When Not

Logical partitioning handling does not take place in the following circumstances:

- Geolocation or geolocation filter does not associate with the involved devices.
- No logical partitioning support exists when a dual-mode phone is used.

Deny Handling

Logical partitioning handles a denied call as follows:

- For SNR and Mobile Voice Access, the call gets cleared or rejected with a reorder tone.
- For cell pickup, the original call between connected party and VoIP phone (SNR) gets restored, and the Cannot Send Call to Mobile message displays on the VoIP phone.

Additional Information

See the "Related Topics" section on page 32-47.

Shared Line

This section describes the interaction of logical partitioning with the Shared Line feature.

Operation

The call to or from a shared line uses the same processing for logical partitioning checks as a basic call.

The shared-line device on Cisco Unified Communications Manager performs logical partitioning policy checks for displaying remote-in-use (RIU) information. The policy gets checked between the geolocation identifier for the connected party and the shared-line device that shows RIU information.

Configuration

The shared-line devices and the PSTN access device (a VoIP gateway) associate with a geolocation and geolocation filter.

When

Logical partitioning handling takes place in the following circumstances for a basic call:

- A shared line exists for the VoIP phones that span different geolocations, and one of the VoIP phones makes or receives a PSTN call through its local PSTN gateway.

- For completing the call from a shared line to a PSTN gateway, Cisco Unified Communications Manager uses the geolocation identifier information that associates with the calling shared-line phone and with the called PSTN gateway to perform logical partitioning policy checking.
- For completing the call from a PSTN gateway to a shared line, Cisco Unified Communications Manager uses the geolocation identifier information that associates with the calling PSTN gateway and with each of the called shared-line phones to perform logical partitioning policy checking.
- The configured logical partitioning policy gets returned to the called Cisco Unified Communications Manager device layer, which takes action accordingly.
- For determining whether to display the remote-in-use (RIU) information, Cisco Unified Communications Manager uses the geolocation identifier information of each device that associates with the shared line and that of the connected party (calling or called) to perform logical partitioning policy checking.

When Not

Logical partitioning handling does not take place in the following circumstances:

- When both the caller and the callee devices are VoIP phones (DevType=Interior), no handling occurs.
- When geolocation or geolocation filter does not associate with any device, no handling occurs.

Deny Handling

Logical partitioning handles a denied call as follows:

- Cisco Unified Communications Manager drops the call (or does not extend the call) to the called shared-line devices that are in unauthorized geolocations for the calling device.
- The call instance information does not display on the shared-line device in the remote-in-use state.

Additional Information

See the "Related Topics" section on page 32-47.

Barge, cBarge, and Remote Resume

This section describes the interaction of logical partitioning with the Barge, cBarge, and Remote Resume features.

Operation

The Barge, cBarge, or Remote-Resume operations on a shared line depend on the availability of call instance information in the remote-in-use (RIU) state.

The same logical partitioning policy checks that apply to shared-line interactions determine the availability of RIU information.

For logical partitioning deny cases, the RIU call instance gets withdrawn on a restricted shared line.

Configuration

The shared-line devices and the PSTN access device associate with a geolocation and geolocation filter.

When

Logical partitioning handling takes place in the following circumstances:

- A shared line exists for the VoIP phones that span different geolocations and one VoIP phone makes or receives a PSTN call through its local PSTN gateway.
- The display of remote-in-use (RIU) information gets handled as in the shared-line call scenario.
- During Hold for an active call by a shared-line device, no Remote Resume button is available.
- Because Barge and cBarge buttons are not available, these scenarios remain impossible.

When Not

Logical partitioning handling does not take place in the following circumstances:

- When both the caller and the callee devices are VoIP phones (DevType=Interior), logical partitioning policy checks get ignored.
- When geolocation or geolocation filter does not associate with any device, no handling occurs.
- When the connected party is a conference bridge due to an active feature, such as Conference or Meet-Me, and an active shared-line device associates with a geolocation that is allowed for all the devices in the conference, the remote-in-use shared-line device shows call instance information. In this case, the remote-in-use phone can always perform the cBarge/Barge feature even if a disallowed participant participates in the conference. For the participants in cBarge/Barge, no logical partitioning policy checking exists, and you cannot prevent logical-partitioning-denied scenarios.

Deny Handling

Logical partitioning handles a denied call as follows:

- The call instance information does not display.

Additional Information

See the "Related Topics" section on page 32-47.

Route Lists and Hunt Pilots

This section describes the interaction of logical partitioning with route lists and hunt pilots.

Operation

For route lists, the call from a device to gateways or MGCP ports that belong to route lists and route groups gets checked for logical partitioning policy by using the geolocation identifier of the involved calling party and called party devices as a basis.

For hunt pilots, the call from a PSTN device to a line device that belongs to a hunt list or hunt group gets checked for logical partitioning policy by using the geolocation identifier of the involved calling party and called party devices as a basis.

Configuration

The calling party and called party devices associate with a geolocation and geolocation filter.

When

Logical partitioning handling takes place in the following circumstances:

- A basic call takes place from a VoIP phone or a PSTN gateway through a route list to a PSTN gateway.

- A basic call takes place from a PSTN gateway through a hunt list to a set of VoIP phones.
- Cisco Unified Communications Manager uses the geolocation identifier information that associates with the incoming and outgoing Cisco Unified Communications Manager devices to perform logical partitioning policy checking.
- The configured logical partitioning policy returns to an outgoing Cisco Unified Communications Manager device layer, which takes action accordingly.

When Not

Logical partitioning handling does not take place in the following circumstances:

- When both the calling party and called party devices specify VoIP phones (DevType=Interior), handling does not occur.
- All devices must associate with both a geolocation and geolocation filter. If any device does not associate with both geolocation and geolocation filter, handling does not occur.

Deny Handling

Logical partitioning handles a denied call as follows:

- The call gets cleared or rejected with a reorder tone from Cisco Unified Communications Manager.

Additional Information

See the "Related Topics" section on page 32-47.

CTI Handling

This section describes the CTI interaction of logical partitioning with all features that perform Join or Redirects.

Operation

All the operations involving calls, joins, or redirects to a PSTN gateway get logical partitioning policy checked, and a CTI error gets generated for logical partitioning failures in the following instances:

- Basic call
- Transfer
- Conference
- Park retrieval and similar functions

Configuration

The involved devices associate with a geolocation and geolocation filter.

When

Logical partitioning handling takes place in the following circumstances:

- One of the devices specifies a PSTN participant.
- The logical partitioning policy gets checked in the context of an operation.

When Not

Logical partitioning handling does not take place in the following circumstances:

- When a geolocation or geolocation filter does not associate with any device, handling does not occur.
- When all the involved devices specify VoIP phones (DevType=Interior), handling does not occur.

Deny Handling

Logical partitioning handles a denied call by generating an operation-based CTI cause code as follows:

- Basic call—CTICCMSIP503SERVICENOTAVAILABL.
- Redirection—CTIERR_REDIRECT_CALL_PARTITIONING_POLICY.
- Join, Transfer, Conference, and others.—CTIERR_FEATURE_NOT_AVAILABLE.

Additional Information

See the "Related Topics" section on page 32-47.

Limitations

The following limitations apply to logical partitioning:

- SIP trunk User Agent Server (UAS) location conveyance in UPDATE

  The UAS uses UPDATE request to communicate geolocation of the called party to the User Agent Client (UAC). This normally happens after 180 Ringing.

  The logical partitioning policy checks in logical partitioning-aware cluster that receives this geolocation may CANCEL the call if policy gets denied. A convenient end user experience may not occur.

- The logical partitioning checks do not get supported for participants across conferences in conference chaining.

  For example, meet-me and ad hoc chained conferences can have participants that are logical partitioning denied.

- Limitation with QSIG intercluster trunk (ICT)

  Be aware that the ICT with Q.SIG protocol is not allowed to communicate geolocation info for the caller or callee device. The ICT configuration for "Send Geolocation Information" gets disabled when the Q.SIG tunneled protocol gets selected.

- Shared Line Active Call Info

  For logical partitioning restricted scenario, the shared line drops the active call information for the duration of the call, even if some feature moves the shared-line call to allowed category.

- cBarge/Barge

  Barge/cBarge does not occur because it gets prevented by not allowing shared lines to attempt these features based on logical partitioning deny policy with the connected party (the call instance gets dropped).

  However, when the connected party is a conference bridge due to an active feature, such as Conference or Meet-Me, and an active shared-line device associates with a geolocation that is allowed for all the devices in the conference, the remote-in-use shared-line device shows call instance information. In this case, the remote-in-use phone can always perform the cBarge/Barge

feature even if a disallowed participant participates in the conference. For the participants in cBarge/Barge, no logical partitioning policy checking exists, and you cannot prevent logical-partitioning-denied scenarios.

- Cisco Unified Communications Manager does not communicate geolocation info to H.323 or MGCP gateway.

  Communication to a SIP gateway can get disabled from a SIP trunk check box.

- Cisco Unified Communications Manager does not communicate geolocation information over a H.225 gatekeeper-controlled trunk.

  Scenario: Cisco Unified Communications Manager 1 remains logical partitioning enabled, but Cisco Unified Communications Manager 2 stays logical partitioning disabled.

  Phone A on CCM1 calls Phone B on CCM2 (using ICT or SIP trunk).

  Phone B presses conference and invites PSTN to conference.

  Limitation: The conference gets established.

  After phone B goes on hook, the call between phone A and the PSTN on Cisco Unified Communications Manager 2 gets cleared with a reorder tone.

- Mobility Cell Pickup: Logical partitioning Deny handling takes place after call gets answered on the mobile phone.

  The logical partitioning policy check does not happen before the call gets placed to the mobile phone (as it happens for a basic SNR call). The current design checks logical partitioning policy only after SsJoinReq processing, which takes place after the mobile phone answers the call.

- Cisco Extension Mobility logs in to a phone in a different geolocation

  Outgoing PSTN calls can occur when Local Route Groups are configured.

  Incoming PSTN calls do not get placed to the phone but receive a reorder tone.

- BLF SD or BLF Pickup Presence notifications do not get checked for logical partitioning policy.

  Currently, no logical partitioning infrastructure gets added for notifications.

  For forwarding failures, the RTMT Number of Forwarding Failures performance monitor counter does not increment. Instead, the Number of Basic Call Failures performance monitor counter increments.

- No reorder tone is provided on IOS H.323 and SIP gateways upon release of connected calls due to logical partitioning policies during supplementary features.

  Example

  Remote destination (RD) phone behind IOS SIP or H.323 gateway calls VoIP phone A.

  After authentication completes, RD phone makes a call to phone C, but the call gets denied due to logical partitioning restricted policy.

  Call gets cleared to RD phone with cause 63 (Service or option not available), but no reorder tone gets played to the RD phone.

  Note This cause code is common to all logical partitioning failure cases.

  This behavior occurs due to a design limitation on the IOS gateway side, which does not play reorder tone after the CONNECT state. The only tones that play after the CONNECT state specify 17 (Busy) or 44 (No Circuit Available).

  Similar limitations apply for Hook Flash, Onhook Transfer, and other supplementary features.

- No configuration exists for forwarding the call to voice mail for logical partitioning failures.
- No announcements occur for logical partitioning deny failures.
- Cisco Unified Communications Manager does not support the logical partitioning feature for calls that involve Cisco Unified MeetingPlace or Cisco Unified MeetingPlace Express.

Additional Information

See the "Related Topics" section on page 32-47.

Configuring Logical Partitioning

This section contains information on the following topics:

- Geolocation Configuration, page 32-39
- Geolocation Filter Configuration, page 32-39
- Logical Partitioning Policy Configuration, page 32-40

Tip Before you configure logical partitioning, review the "Configuration Checklist for Logical Partitioning" section on page 32-1.

Additional Information

See the "Related Topics" section on page 32-47.

Geolocation Configuration

Use the **System > Geolocation Configuration** menu option in Cisco Unified Communications Manager Administration to configure geolocations.

For details of geolocation configuration, see the "Geolocation Configuration" section on page 24-10.

Additional Information

See the "Related Topics" section on page 32-47.

Geolocation Filter Configuration

Use the **System > Geolocation Filter** menu option in Cisco Unified Communications Manager Administration to configure geolocation filters.

For details of geolocation filter configuration, see the "Geolocation Filter Configuration" section on page 24-17.

Additional Information

See the "Related Topics" section on page 32-47.

Logical Partitioning Policy Configuration

Use the **Call Routing > Logical Partitioning Policy Configuration** menu option in Cisco Unified Communications Manager Administration to configure logical partitioning policies.

To configure logical partitioning policies, see the following sections:

- Finding a Logical Partitioning Policy, page 32-40
- Configuring a Logical Partitioning Policy, page 32-41
- Deleting a Logical Partitioning Policy Record, page 32-42
- Deleting a Logical Partitioning Policy Pair Configuration, page 32-42
- Updating a Logical Partitioning Policy Pair Configuration, page 32-43
- Logical Partitioning Policy Configuration Settings, page 32-43

Additional Information

See the "Related Topics" section on page 32-47.

Finding a Logical Partitioning Policy

Because you might have multiple logical partitioning policies in your network, Cisco Unified Communications Manager lets you search for logical partitioning policies on the basis of specified criteria. Follow these steps to search for a specific logical partitioning policy in the Cisco Unified Communications Manager database.

Note During your work in a browser session, Cisco Unified Communications Manager Administration retains your logical partitioning policy search preferences. If you navigate to other menu items and return to this menu item, Cisco Unified Communications Manager Administration retains your logical partitioning policy search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **Call Routing > Logical Partitioning Policy Configuration.**

The Find and List Policies window displays. Records from an active (prior) query may also display in the window.

Step 2 To find all records in the database, ensure the dialog box is empty; go to Step 3.

To filter or search records

- From the first drop-down list box, choose a search parameter.
- From the second drop-down list box, choose a search pattern.
- Specify the appropriate search text, if applicable.

Note To add additional search criteria, click the **+** button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the **–** button to remove the last added criterion or click the **Clear Filter** button to remove all added search criteria.

Step 3 Click **Find**.

All matching records display. You can change the number of items that display by choosing a different value from the Rows per Page drop-down list box.

Note You can delete multiple records from the database by checking the check boxes next to the appropriate record and clicking **Delete Selected**. You can delete all configurable records for this selection by clicking **Select All** and then clicking **Delete Selected**.

Step 4 From the list of records that display, click the link for the record that you want to view.

Note To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

Additional Information

See the "Related Topics" section on page 32-47.

Configuring a Logical Partitioning Policy

Perform the following procedure to add or update a logical partitioning policy.

Procedure

Step 1 Choose **Call Routing > Logical Partitioning Policy Configuration**.

The Find and List Policies window displays.

Step 2 Perform one of the following tasks:

- To add a new logical partitioning policy, click **Add New**.

  The Logical Partitioning Policy Configuration window displays.

- To update a logical partitioning policy, locate a specific logical partitioning policy as described in the "Finding a Logical Partitioning Policy" section on page 32-40.

Step 3 Enter the appropriate settings as described in Table 32-4.

Step 4 Click **Save**.

If you added a logical partitioning policy, the list box at the bottom of the window now includes the new logical partitioning policy.

Additional Information

See the "Related Topics" section on page 32-47.

Deleting a Logical Partitioning Policy Record

Perform the following procedure to delete an existing logical partitioning policy record.

Procedure

Step 1 Choose **Call Routing > Logical Partitioning Policy Configuration**.

The Find and List Policies window displays.

Step 2 To locate a specific logical partitioning policy, enter search criteria and click **Find**.

A list of geolocation filter logical partitioning policies that match the search criteria displays.

Step 3 Perform one of the following actions:

- Check the check boxes next to the logical partitioning policies that you want to delete and click **Delete Selected**.
- Delete all logical partitioning policies in the window by clicking **Select All** and then clicking **Delete Selected**.
- From the list, choose the name of the logical partitioning policy that you want to delete and click **Delete**.

A confirmation dialog displays.

Step 4 Click **OK**.

The specified logical partitioning policy and all pair policies for this record get deleted.

Additional Information

See the "Related Topics" section on page 32-47.

Deleting a Logical Partitioning Policy Pair Configuration

In this case, select a logical partitioning policy record and display the configuration window of that record.

The policies are currently configured in pairs. For example,

GLP-1 Border GLP-2 Interior Allow

GLP-1 Border GLP-3 Interior Allow

If the second policy needs to be deleted, choose the second policy and select the Use Default Policy setting.

After you save, the corresponding pair of policies gets deleted from the matrix of policies.

Note that no change is made in the GLP-1 record.

Additional Information

See the "Related Topics" section on page 32-47.

Updating a Logical Partitioning Policy Pair Configuration

In this case, select a logical partitioning policy record and display the configuration window of that record.

The policies are currently configured in pairs. For example,

GLP-1 Border GLP-2 Interior Allow

GLP-1 Border GLP-3 Interior Allow

If the second policy needs to be updated, choose the second policy and specify either Allow or Deny in the Policy setting.

After you save, the corresponding pair of policies gets updated from the matrix of policies.

Additional Information

See the "Related Topics" section on page 32-47.

Logical Partitioning Policy Configuration Settings

Ensure logical partitioning policies are configured for the required interconnection behavior between the following entities:

- Between PSTN gateways and VoIP phones
- Between PSTN gateway and PSTN gateway
- Between an intercluster trunk (ICT) and a VoIP phone
- Between an ICT and a VoIP gateway

The System Default Policy enterprise parameter (Default value=DENY) represents the default policy when no configured policy is found.

In the Logical Partitioning Policy Configuration window (**Call Routing > Logical Partitioning Policy Configuration** menu option in Cisco Unified Communications Manager Administration), the administrator must create geolocation policy records from a subset of the fields that are configured for geolocations.

Configure logical partitioning policies between pairs of geolocation policy records and device types.

Ensure Allow and Deny policies are configured. See the "Allow and Deny Policies" section on page 32-6 for configuration details.

See the "Logical Partitioning Policies" section on page 32-11 for more information about logical partitioning policies, including examples.

Table 32-4 describes the configuration settings that are used for configuring logical partitioning policies.

Table 32-4 Logical Partitioning Policy Configuration Settings

Field	Description
Logical Partitioning Policy Configuration	
Name	Enter a unique name (between 1 and 50 characters) for this logical partitioning policy. You may use all characters except quotes (“), close angle bracket (>), open angle bracket (<), backslash (\), ampersand (&), and percent sign (%).

Table 32-4 Logical Partitioning Policy Configuration Settings (continued)

Field	Description
Description	Enter a description for this logical partitioning policy.
Country	From the drop-down list box, choose a country for this logical partitioning policy. You can leave the <*None*> value if you do not want to specify this field for this logical partitioning policy.
A1	From the drop-down list box, choose an A1 value for this logical partitioning policy. You can leave the <*None*> value if you do not want to specify this field for this logical partitioning policy.
A2	From the drop-down list box, choose an A2 value for this logical partitioning policy. You can leave the <*None*> value if you do not want to specify this field for this logical partitioning policy.
A3	From the drop-down list box, choose an A3 value for this logical partitioning policy. You can leave the <*None*> value if you do not want to specify this field for this logical partitioning policy.
A4	From the drop-down list box, choose an A4 value for this logical partitioning policy. You can leave the <*None*> value if you do not want to specify this field for this logical partitioning policy.
A5	From the drop-down list box, choose an A5 value for this logical partitioning policy. You can leave the <*None*> value if you do not want to specify this field for this logical partitioning policy.
A6	From the drop-down list box, choose an A6 value for this logical partitioning policy. You can leave the <*None*> value if you do not want to specify this field for this logical partitioning policy.
PRD	From the drop-down list box, choose a PRD value for this logical partitioning policy. You can leave the <*None*> value if you do not want to specify this field for this logical partitioning policy.
POD	From the drop-down list box, choose a POD value for this logical partitioning policy. You can leave the <*None*> value if you do not want to specify this field for this logical partitioning policy.
STS	From the drop-down list box, choose an STS value for this logical partitioning policy. You can leave the <*None*> value if you do not want to specify this field for this logical partitioning policy.
HNO	From the drop-down list box, choose an HNO value for this logical partitioning policy. You can leave the <*None*> value if you do not want to specify this field for this logical partitioning policy.
HNS	From the drop-down list box, choose an HNS value for this logical partitioning policy. You can leave the <*None*> value if you do not want to specify this field for this logical partitioning policy.
LMK	From the drop-down list box, choose an LMK value for this logical partitioning policy. You can leave the <*None*> value if you do not want to specify this field for this logical partitioning policy.
LOC	From the drop-down list box, choose a LOC value for this logical partitioning policy. You can leave the <*None*> value if you do not want to specify this field for this logical partitioning policy.

Table 32-4 Logical Partitioning Policy Configuration Settings (continued)

Field	Description
FLR	From the drop-down list box, choose a FLR value for this logical partitioning policy. You can leave the <*None*> value if you do not want to specify this field for this logical partitioning policy.
NAM	From the drop-down list box, choose an NAM value for this logical partitioning policy. You can leave the <*None*> value if you do not want to specify this field for this logical partitioning policy.
PC	From the drop-down list box, choose a PC value for this logical partitioning policy. You can leave the <*None*> value if you do not want to specify this field for this logical partitioning policy.
Configured Policies	
Device Type	After you configure a relationship between this logical partitioning policy and another (or the same) logical partitioning policy, a new row displays in this pane for the configured relationship. This column displays the device type of the current logical partitioning policy for this relationship. **Note** Only relationships that do not specify Use Default Policy display in this pane.
Geolocation Policy	After you configure a relationship between this logical partitioning policy and another (or the same) logical partitioning policy, a new row displays in this pane for the configured relationship. This column displays the other geolocation policy for this relationship. **Note** Only relationships that do not specify Use Default Policy display in this pane.
Other Device Type	After you configure a relationship between this logical partitioning policy and another (or the same) logical partitioning policy, a new row displays in this pane for the configured relationship. This column displays the device type of the other logical partitioning policy for this relationship. **Note** Only relationships that do not specify Use Default Policy display in this pane.
Policy	After you configure a relationship between this logical partitioning policy and another (or the same) logical partitioning policy, a new row displays in this pane for the configured relationship. This column displays the configured logical partitioning policy value for this relationship. **Note** Only relationships that do not specify Use Default Policy display in this pane.

Table 32-4 Logical Partitioning Policy Configuration Settings (continued)

Field	Description
Configure Relationship to Other Geolocation Policies	
Device Type	From the drop-down list box, choose one of the following values to configure the relationship of this logical partitioning policy to other geolocation policies: • Border—Choose this device type for devices that specify PSTN trunks, gateways, and MGCP ports. • Interior—Choose this device type for devices that specify VoIP phones or internal endpoints. **Note** See Table 32-2 for a listing of which Cisco Unified Communications Manager devices can be associated with each device type (border or interior).
Geolocation Policy	In this pane, choose the name of another geolocation policy to configure the relationship between this logical partitioning policy and that geolocation policy.
Other Device Type	From the drop-down list box, choose the device type of the other geolocation policy that you selected in the Geolocation Policy column. Choose one of the following values: • Border—Choose this device type for devices that specify PSTN trunks, gateways, and MGCP ports. • Interior—Choose this device type for devices that specify VoIP phones or internal endpoints. **Note** See Table 32-2 for a listing of which Cisco Unified Communications Manager devices can be associated with each device type (border or interior).
Policy	From the drop-down list box, choose the policy to apply between this logical partitioning policy and the geolocation policy that you selected in the Geolocation Policy column. Choose one of the following values: • Use Default Policy—Choose this value to apply the default policy that the Logical Partitioning Default Policy enterprise parameter specifies. • Allow—Choose this value to specify a policy of Allow between this logical partitioning policy and the other geolocation policy. • Deny—Choose this value to specify a policy of Deny between this logical partitioning policy and the other geolocation policy.

Additional Information

See the "Related Topics" section on page 32-47.

Logical Partitioning Configuration Upon Upgrade From Previous Releases

During upgrade of Cisco Unified Communications Manager from a release that preceded Release 7.1(2), the following values get assigned for the entities that associate with logical partitioning configuration:

- Enable Logical Partitioning enterprise parameter specifies **False**.
- Logical Partitioning Default Policy enterprise parameter specifies **Deny**.
- Geolocation
  - No configured geolocation records exists in the geolocation table.
  - Default Geolocation enterprise parameter specifies **Unspecified**.
  - Device pools specify Geolocation value **None**.
  - Devices specify Geolocation value **Default**.
- Geolocation filter
  - No configured geolocation filter records exist in geolocation filter table.
  - Logical Partitioning Default Filter enterprise parameter specifies **None**.
  - Device pools specify Geolocation Filter value **None**.
  - Devices specify Geolocation Filter value **None**.
- Logical partitioning policy
  - No configured GeolocationPolicy records and policies exist in geolocationpolicy and geolocationpolicymatrix tables.

Additional Information

See the "Related Topics" section on page 32-47.

Troubleshooting Logical Partitioning

For information on troubleshooting logical partitioning, see the *Troubleshooting Guide for Cisco Unified Communications Manager*.

Additional Information

See the "Related Topics" section on page 32-47.

Related Topics

- Configuration Checklist for Logical Partitioning, page 32-1
- Introducing Logical Partitioning, page 32-4
- Applicability to Requirements From Indian Telecom Regulations, page 32-6
- History, page 32-7
- Overview of Logical Partitioning Architecture, page 32-8
- Logical Partitioning Use of Geolocations and Geolocation Filters, page 32-8

- Logical Partitioning Geolocation Usage for Shared Lines and Route Lists, page 32-10
- Enterprise Parameters for Logical Partitioning, page 32-10
- Logical Partitioning Policies, page 32-11
- LPPolicyManager and Policy Tree, page 32-13
- Logical Partitioning Policy Search Algorithm, page 32-15
- Policy Matching, page 32-17
- Deny Policy Handling, page 32-18
- LPSession Infrastructure and Policy Checking, page 32-18
- Logical Partitioning Handling for a Basic Call, page 32-19
- Logical Partitioning Handling of a Received Geolocation, page 32-20
- Logical Partitioning Interaction with Geolocation Conveyance Across SIP Trunks and Intercluster Trunks, page 32-19
- Logical Partitioning Feature Interactions with Midcall Geolocation Change, page 32-20
- SIP Trunk or Intercluster Trunk Configuration Requirement for Logical Partitioning, page 32-21
- System Requirements for Logical Partitioning, page 32-22
- Interactions and Limitations, page 32-22
- Interactions, page 32-22
- Call Forwarding, page 32-23
- Call Transfer, page 32-24
- Ad Hoc Conference, Join, Join Across Lines (JAL), page 32-27
- Meet-Me Conference, page 32-28
- Call Pickup, page 32-29
- Call Park and Directed Call Park, page 32-30
- Cisco Extension Mobility, page 32-31
- Cisco Unified Mobility, page 32-32
- Shared Line, page 32-33
- Barge, cBarge, and Remote Resume, page 32-34
- Route Lists and Hunt Pilots, page 32-35
- CTI Handling, page 32-36
- Limitations, page 32-37
- Configuring Logical Partitioning, page 32-39
- Geolocation Configuration, page 32-39
- Geolocation Filter Configuration, page 32-39
- Logical Partitioning Policy Configuration, page 32-40
- Logical Partitioning Policy Configuration Settings, page 32-43
- Logical Partitioning Configuration Upon Upgrade From Previous Releases, page 32-47
- Troubleshooting Logical Partitioning, page 32-47
- Device Pool Configuration, *Cisco Unified Communications Manager Administration Guide*

- Enterprise Parameter Configuration, *Cisco Unified Communications Manager Administration Guide*
- CTI Route Point Configuration, *Cisco Unified Communications Manager Administration Guide*
- Gateway Configuration, *Cisco Unified Communications Manager Administration Guide*
- Cisco Unified IP Phone Configuration, *Cisco Unified Communications Manager Administration Guide*
- Trunk Configuration, *Cisco Unified Communications Manager Administration Guide*

Additional Cisco Documentation

- *Cisco Unified Communications Manager Administration Guide*
- *Cisco Unified Communications Manager System Guide*
- *Cisco Unified Serviceability Administration Guide*
- *Cisco Unified Communications Manager Call Detail Records Administration Guide*
- *Cisco Unified Real-Time Monitoring Tool Administration Guide*
- *Cisco Unified Reporting Administration Guide*
- *Cisco Unified Communications Manager Bulk Administration Guide*
- *Cisco Unified Communications Solution Reference Network Design (SRND) for Cisco Unified Communications Manager*
- *Cisco Unified Communications Manager Security Guide*
- *Cisco Unified Communications Manager Assistant User Guide*