CHAPTER 5

Cisco Unified CallManager Trunks

Last revised on: February 13, 2008

This chapter discusses design considerations for Cisco Unified Callmanager Release 4.2, but much of the discussion also applies to Cisco Unified CallManager releases 4.1, 4.0, and 3.3.

The use of the term *trunk* in Cisco Unified CallManager is different than the traditional meaning for trunk used when discussing circuit switched systems. The definition of trunk is expanded beyond physical connections such as a PRI, T1, or analog trunk, to also include virtual connections between two entities. The virtual connection defines a TCP/IP session between the two entities that is used for call signaling, and associated with the connection is a path over a TCP/IP network used for the media. The signaling path and the media path may terminate on different sets of endpoints and also may take different paths through the TCP/IP network. In some cases the trunk may define an entity that is the destination where the VoIP media stream of the call ultimately terminates, or it may define an entity that provides an intermediate routing function. In the first case, there must exist a separate configuration for each pair of endpoints, and the relationship between the two entities is peer-to-peer. In the latter case, a single trunk may be defined to specify a gatekeeper that provides a routing function between all entities registered to that gatekeeper. This relationship is one-to-many.

In Cisco Unified CallManager, trunks may be configured with one of two protocols: H.323 or SIP. The following sections introduce the characteristics of these trunks.

H.323 Protocol

There are four different configurations in Cisco Unified CallManager that may be used to communicate to other entities via the H.323 protocol suite:

- H.323 gateway (See Gateways, page 4-1.)

  This type of configuration is used to define a peer-to-peer relationship between the cluster and another H.323 gateway or endpoint without gatekeeper control. It is not a trunk under the definition used by Cisco Unified CallManager but is mentioned here for completeness of the discussion. This configuration may *not* be used to connect two Cisco Unified CallManager clusters.

- H.225 trunk, gatekeeper controlled (See Gatekeeper Controlled Trunks, page 5-2.)

  This trunk configuration defines communication between a Cisco Unified CallManager cluster and one or more H.323 gateways, endpoints, or other clusters under control of an H.323 gatekeeper.

- Intercluster trunk, non-gatekeeper controlled (See Non-Gatekeeper Controlled Trunks, page 5-3.)

  This trunk configuration defines communication between a single pair of Cisco Unified CallManager clusters using an H.323-based protocol. There is no gatekeeper associated with this trunk.

- Intercluster trunk, gatekeeper controlled (See Gatekeeper Controlled Trunks, page 5-2.)

  This configuration allows multiple Cisco Unified CallManager clusters to interconnect via H.323 with a single trunk definition under control of a gatekeeper.

SIP Protocol

Cisco Unified CallManager classifies SIP entities as either line side or trunk side. Entities that are integrated via SIP trunks include gateways, voicemail systems, presence servers, other clusters, SIP proxies, and so forth. Cisco Unified CallManager provides only one type of SIP trunk. (See SIP Trunks, page 5-11.)

SIP standards do not define the term trunk; it is terminology that is specific to the Cisco Unified CallManager implementation. A SIP Trunk configures members of a cluster to behave as a SIP User Agent, and the cluster expects the other SIP entity defined in the configuration to also act as a SIP User Agent.

Support for SIP trunks was first added in Cisco Unified CallManager Release 4.0.

H.323 Trunks

The following types of H.323 trunks can be configured in a Cisco Unified CallManager cluster:

- H.225 trunk (gatekeeper controlled)
- Intercluster trunk (non-gatekeeper controlled)
- Intercluster trunk (gatekeeper controlled)

All three types of H.323 trunks may be used to connect Cisco Unified CallManager clusters (Release 3.2 and later) to each other, but only the H.225 gatekeeper controlled trunk may be used to connect a Cisco Unified CallManager cluster to other H.323 endpoints. When any of these three types of trunks are used to communicate between clusters, extensions to the H.225 protocol are used to provide additional feature transparency between the clusters. The use of these protocol extensions is invoked automatically via autodetection.

Protocol Autodetection

This feature provides the ability to determine, on a call-by-call basis, if the calling device is from Cisco Unified CallManager Release 3.2 or later. When a call is received on an H.323 trunk, Cisco Unified CallManager looks for an H.225 User-to-User Information Element (UUIE) that indicates if the other end is another Cisco Unified CallManager. Only Cisco Unified CallManager 3.2 or later will send this UUIE. When the UUIE is present, then both clusters will utilize the Cisco-specific H.225 protocol extensions. If no UUIE is found, the use of the Cisco extensions are dependant on the configured trunk type.

Gatekeeper Controlled Trunks

You may want to provision a gatekeeper for any of the following reasons:

- To reduce the administration of the full-mesh configuration that might be required for larger numbers of H.323 endpoints.

  With a single Cisco gatekeeper, it is possible to have 100 clusters all registering a single trunk each, with all clusters being able to call each other. With non-gatekeeper controlled trunks, this same topology would require 99 trunks configured in each cluster.

- To provide gatekeeper-based call admission control. (See Call Admission Control, page 9-1, for more information.)
- To improve failover times.

If a subscriber server in a cluster becomes unreachable, there will be a five-second (default) timeout while the call is attempted. If an entire cluster is unreachable, the number of attempts before either call failure or rerouting over the PSTN will depend on the number of remote servers defined for the trunk and on the number of trunks in the route list or route group. If there are many remote servers and many non-gatekeeper controlled trunks, the call delay can become excessive.

With a gatekeeper controlled trunk, you configure only one trunk that can then communicate via the gatekeeper with all other clusters registered to the gatekeeper. If a cluster or subscriber becomes unreachable, the gatekeeper automatically directs the call to another subscriber in the cluster or rejects the call if no other possibilities exist, thus allowing the call to be rerouted over the PSTN (if required) with little incurred delay.

If a gatekeeper is used, then the following two types of trunks are available:

- H.225 trunk (gatekeeper controlled)

  Always use this configuration to communicate with any combination Cisco Unified CallManager (Release 3.2 or later) or other H.323 endpoints that are all controlled by a common set of gatekeeper(s). Cisco Unified CallManager will use the H.225-based Intercluster Trunk Protocol between clusters and use standard H.225 to other H.323 endpoints. The autodetection feature will invoke the appropriate behavior.

  Do not use this trunk for connection to any version of Cisco CallManager prior to Release 3.2 because earlier versions will not send the UUIE and the connection will use the standard H.225 protocol.

- Intercluster trunk (gatekeeper controlled)

  This trunk must be used only for communication to Cisco Unified CallManagers. The trunk always utilizes the Intercluster Trunk Protocol, which will not be understood by a standard H.323 endpoint. Configure this type of trunk only when interoperability is required with versions of Cisco CallManager prior to Release 3.2.

Non-Gatekeeper Controlled Trunks

If no gatekeeper is used, then the only choice for cluster-to-cluster trunking is an intercluster trunk (non-gatekeeper controlled).

This trunk type is the simplest and is used for connecting to other Cisco Unified CallManager clusters in either a multi-cluster single campus or a distributed call processing deployment. This trunk does not use a gatekeeper for call admission control, although it may use locations configured in Cisco Unified CallManager if bandwidth control is required. This type of trunk must be used only for communication with other Cisco Unified CallManager clusters because it utilizes the Intercluster Trunk Protocol.

When defining this type of trunk, you may define up to three remote Cisco Unified CallManager servers in the same destination cluster. The trunk will automatically load-balance across all defined servers. In the remote cluster, it is important to configure a corresponding intercluster trunk (non-gatekeeper controlled) that has a Cisco Unified CallManager group containing the same servers that were defined as remote Cisco Unified CallManager servers in the first cluster. A similar configuration is required in each Cisco Unified CallManager cluster connected by the intercluster trunks.

For example, if Cluster 1 has a trunk to Cluster 2, and Cluster 2 has a trunk to Cluster 1, the following configurations would be needed:

- Cluster 1
  - Servers B, C, and D are configured as members of the Cisco Unified CallManager group defined in the device pool associated with the trunk to Cluster 2.
  - The non-gatekeeper controlled trunk has Cluster 2's remote servers D, E, and F configured.
- Cluster 2
  - Severs D, E, and F are configured as members of the Cisco Unified CallManager group defined in the device pool associated with the trunk to Cluster 1.
  - The non-gatekeeper controlled trunk has Cluster 1's remote servers B, C, and D configured.

Gatekeeper Trunk Redundancy, Resilience, and Load Balancing

Redundancy can be achieved in several ways, depending on the requirements of the design. The simplest method is to configure a gatekeeper controlled trunk and assign up to three subscribers in the Cisco Unified CallManager group associated with the device pool assigned to that trunk. This configuration will cause all servers to register with the same gatekeeper in the same zone with the same technology prefix. However, the H.323 trunk name that is used for the h323_id will have a suffix of "_*n*" where *n* is the node number in the cluster. This ID is automatically generated and cannot be changed. You configure a single trunk, but the gatekeeper registers multiple trunks, one from each subscriber in the Cisco Unified CallManager group.

If you have additional redundancy requirements, it is possible to configure another gatekeeper controlled trunk with a different name and different subscribers in the Cisco Unified CallManager group, but with all the other parameters identical to the first trunk. This second trunk will cause additional subscribers to register with the gatekeeper.

Cisco recommends assigning device pools that contain a Cisco Unified CallManager group consisting of the two servers that make up the standard subscriber pair. (See Call Processing Subscriber, page 8-6, for more information on subscriber redundancy.) For complete redundancy in a full cluster, four trunks would be needed using four different device pools, resulting in eight subscribers registering with the gatekeeper. (The same result could be achieved with three trunks and larger Cisco Unified CallManager groups.)

During registration, several parameters are passed between Cisco Unified CallManager and the gatekeeper. Cisco Unified CallManager uses an ephemeral User Datagram Protocol (UDP) port for gatekeeper Registration Admission Status (RAS) messages on a per-trunk basis. This port would normally be UDP 1719. However, Cisco Unified CallManager must be able to determine which trunk is the destination for a particular RAS message, therefore it uses a range of UDP ports and assigns them dynamically.

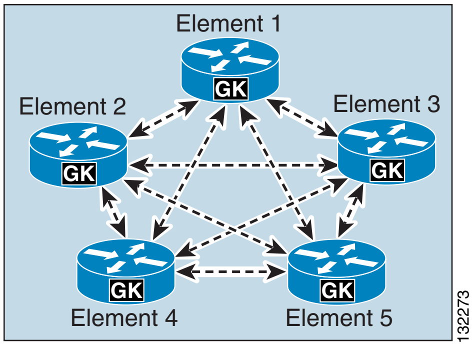
During the registration process, a trunk registers the following information for the other subscribers in its Cisco Unified CallManager group:

- H.225 call signaling port
- h323_id
- CanMapAlias support
- Technology prefix
- H.225 call signaling address

If the recommended clustered gatekeepers are used, the gatekeeper will return a list of alternate gatekeeper addresses that may be used if the primary gatekeeper fails or does not have sufficient available resources.

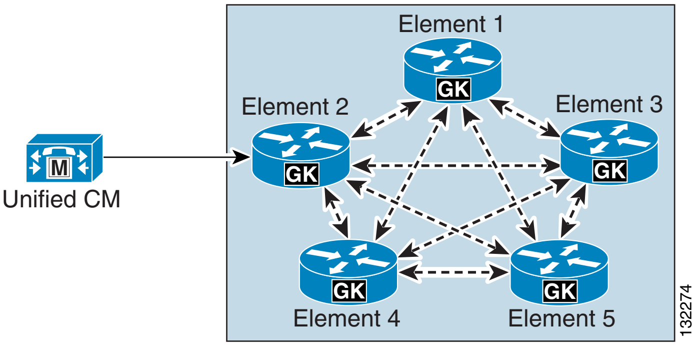
Figure 5-1 shows a cluster of gatekeepers that use Gatekeeper Update Protocol (GUP) to communicate. (See the chapter on Call Processing, page 8-1, for more information on gatekeepers.)

Figure 5-1 Gatekeeper Cluster



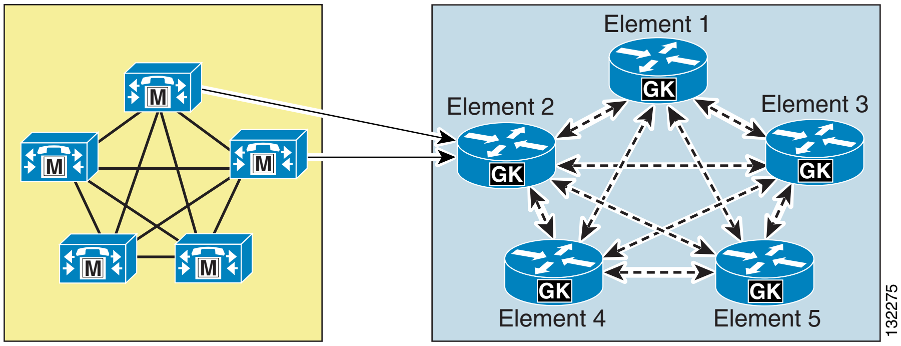
If an H.323 trunk has only a single subscriber in its Cisco Unified CallManager group, there will be only one connection between the configured gatekeeper in Cisco Unified CallManager and the gatekeeper cluster, as illustrated in Figure 5-2.

Figure 5-2 H.323 Trunk with a Single Cisco Unified CallManager Subscriber



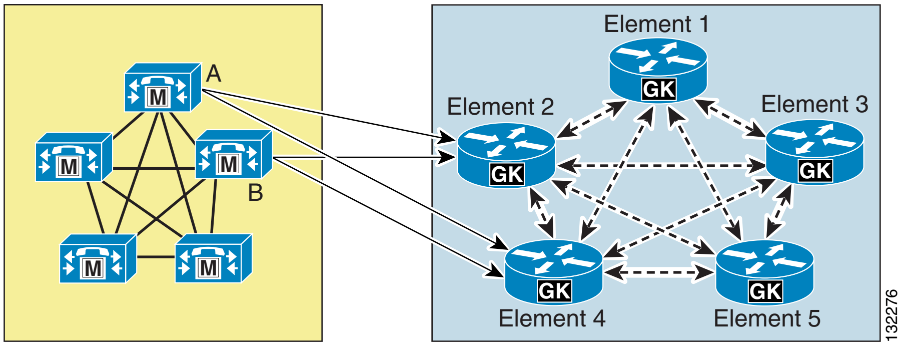
If there are multiple subscribers in the Cisco Unified CallManager group associated with the trunk, additional connections will be established between the Cisco Unified CallManager cluster and the gatekeeper cluster, as illustrated in Figure 5-3.

Figure 5-3 H.323 Trunk with Multiple Cisco Unified CallManager Subscribers



This approach provides redundancy for subscriber failures as well as gatekeeper failures after registration because the alternate gatekeeper is communicated when the trunk registers. This approach does not, however, provide redundancy if the configured gatekeeper is unavailable at initial registration or following a reset because the list of alternate gatekeepers is dynamic and not stored in the database. To provide an additional level of redundancy as well as load balancing, an additional gatekeeper from the gatekeeper cluster is configured in Cisco Unified CallManager. For example, if the original trunk is registered with Element 2, the additional gatekeeper could be configured as Element 4, as illustrated in Figure 5-4.

Figure 5-4 Additional Gatekeeper Configured for Load Balancing and Additional Redundancy



The Cisco Unified CallManager configuration for the example in Figure 5-4 would contain the following components:

- Two gatekeepers for Element 2 and Element 4
- Two H.323 trunks defined with a Cisco Unified CallManager group containing subscriber servers A and B

Using this approach, the Cisco Unified CallManager cluster will still be able to register when either Element 2 or Element 4 is not reachable during initial registration (that is, during power-up or trunk reset).

Load balancing of calls inbound to the Cisco Unified CallManager cluster is done automatic by default because the gatekeeper randomly selects one of the subscribers registered within the zone. If this is not the desired behavior, you can use the **gw-priority** configuration command in the gatekeeper to modify this default behavior, as illustrated in Example 5-1.

Example 5-1 Using the gw-priority Command to Direct Calls to a Particular Trunk

```
gatekeeper
 zone local SJC cisco.com 10.0.1.10
 zone prefix SJC 1408....... gw-priority 10 sjc-trunk_2
 zone prefix SJC 1408....... gw-priority 9 sjc-trunk_3
 zone prefix SJC 1408....... gw-default-priority 0
 gw-type-prefix 1#* default-technology
 arq reject-unknown-prefix
 no shutdown
 endpoint ttl 60
```

In Example 5-1, the H.323 trunk was configured as sjc-trunk in Cisco Unified CallManager, and the "_2" and "_3" suffixes are appended automatically by the Cisco Unified CallManager subscribers to indicate which node number they are in the cluster. Therefore, this example uses node 2 as the first choice, which should be the highest-priority Cisco Unified CallManager in the CallManager group for this trunk. Node 3 is the second choice in this case.

The use of **gw-default-priority 0** is optional. It was used in this example to disable the use of any other trunk that might accidentally be configured to register in this zone.

Outbound calls from a Cisco Unified CallManager cluster can be load-balanced in any of the following ways:

- A single H.323 trunk in a route group will always use the highest-priority subscriber available in the Cisco Unified CallManager group. Lower-priority subscribers are used only when higher-priority subscribers are unavailable.
- Multiple H.323 trunks in a circular route group provide equal call loading across all H.323 trunks in the group.

The following examples list how to configure load balancing in various scenarios.

All calls originate from a single subscriber in a cluster:

- Single H.323 trunk in a route group

Calls spread across four primary subscribers in a cluster:

- Four H.323 trunks with four Cisco Unified CallManager groups, all contained within a circular route group
- Cisco Unified CallManager groups defined as follows:
  - Subscriber A, Subscriber B
  - Subscriber C, Subscriber D
  - Subscriber E, Subscriber F
  - Subscriber G, Subscriber H

  Where subscribers A, C, E, and G are all primaries and subscribers B, D, F, and H are the backups.

Calls spread across eight subscribers in a cluster:

- Eight H.323 trunks with eight different Cisco Unified CallManager groups, each containing only one subscriber, and all contained within a circular route group
- Cisco Unified CallManager groups defined as follows:
  - Subscriber A
  - Subscriber B
  - Subscriber C

  - Subscriber D
  - Subscriber E
  - Subscriber F
  - Subscriber G
  - Subscriber H

H.323 Trunks with Media Termination Points

Media termination points (MTPs) are generally not required for normal operation of the H.323 trunk. They are, however, required for communication with devices that are H.323 Version 1 or that do not support the Empty Capabilities Set (ECS) for supplementary services.

To test whether or not an MTP is required, use the following simple procedure:

1. Place a call from a phone via the H.323 trunk to the other device. This call should work normally.
2. Place the call on hold, then resume it. If the call drops, then it is highly likely that an MTP is required to ensure interoperability between Cisco Unified CallManager and the other device.

MTPs are very useful for terminating media streams from other devices that make calls over the H.323 trunk and for re-originating the media streams with the same voice payload; however, in such cases the IP address is changed to that of the MTP. With this fact in mind, you can utilize MTPs in the following scenarios:

- If the phones, gateways, and other devices within your enterprise all use RFC 1918 private addresses, you might still want to connect to other systems on a public network without using Network Address Translation (NAT) for all your voice and video devices. If the Cisco Unified CallManager subscriber that communicates to the public network is using a public IP address, the signaling will be routed. If all MTPs are also using public addresses, the media from the devices with RFC 1918 addresses will be terminated on the MTP and then originated again, but this time with a public address that is routable on the public network. This approach allows tens of thousands of devices with RFC 1918 addresses to communicate with the public network. This same method can be used to conceal the real IP addresses of devices in an enterprise network when communicating with other enterprises or service providers.
- Trust boundaries can be established to traverse firewalls or to allow access through an access control list (ACL). Normally, for media to traverse a firewall, you could either use an Application Layer Gateway (ALG) or fix-up to provide access dynamically for the media streams or you could allocate a wide range of addresses and ports for use by all voice devices that need to communicate across the firewall. All calls that use the H.323 trunk and traverse a firewall or ACL will have media that is sourced from the MTP(s), which may use either a single IP address or a small range of IP addresses.

With both of these methods, if the **MTP Required** box is checked, the default behavior is to allow calls on the H.323 trunks even if MTP resources are unavailable or exhausted. This default behavior might result in no voice path for the call, but the behavior can be changed by setting the Cisco CallManager service parameter **Fail Call if MTP allocation fails** under the H.323 section to **True**.

H.323 Operation in Cisco Unified CallManager

This section provides information on how the H.323 protocol is used and implemented in Cisco Unified CallManager, and it explains how and why certain features work the way they do.

The most important point to understand is which subscribers run the call signaling daemons. These daemons are pieces of code that make and receive H.323 calls. They are usually referred to as H.225 daemons, or H.225Ds. H.225 is part of the H.323 protocol and is mainly responsible for call control. H.245 is the other major component of H.323 that is responsible for the media control of a call.

The subscribers listed in the Cisco Unified CallManager group for a particular H.323 device determine which subscribers run the daemons and when. This point is a very important because calls sent to an incorrect subscriber might be rejected or handled by a different H.225D. For example, this situation would occur if a Cisco IOS H.323 gateway is configured with dial peers that send calls to subscriber C in a Cisco Unified CallManager cluster but the Cisco Unified CallManager group for that gateway has only subscribers A and B in its list. In such a case, the call will fail or be handled by an H.323 trunk daemon if one happens to be configured on the subscriber.

The following scenarios describe where and when H.225Ds are created on subscribers:

- H.323 client

  The H.225D is active on only the highest-priority subscriber available in the Cisco Unified CallManager group associated with the H.323 client.

  If the H.323 client is gatekeeper controlled, the RasAggregator device registers from only the highest-priority subscriber available in the Cisco Unified CallManager group associated with the gatekeeper controlled H.323 client.

  The RasAggregator is a special device that registers in gatekeeper zones for the purpose of providing two specific features:

  - If H.323 clients use DHCP, they cannot be used with a Cisco Unified CallManager using DNS unless they support Dynamic DNS. With the RasAggregator, Cisco Unified CallManager can obtain the IP address of a specific H.323 client that is registered with the gatekeeper whenever a call is placed. The gatekeeper registration is done using standard RAS ARQ messages that contain the E.164 address of the H.323 client. The gatekeeper resolves the E.164 address and provides the IP address back to Cisco Unified CallManager in an ACF message.
  - The RasAggregator also ensures that all calls by the H.323 clients are made through Cisco Unified CallManager and not directly between the clients themselves, thus ensuring that dialing rules and codec restrictions are enforced.

- H.323 gateway

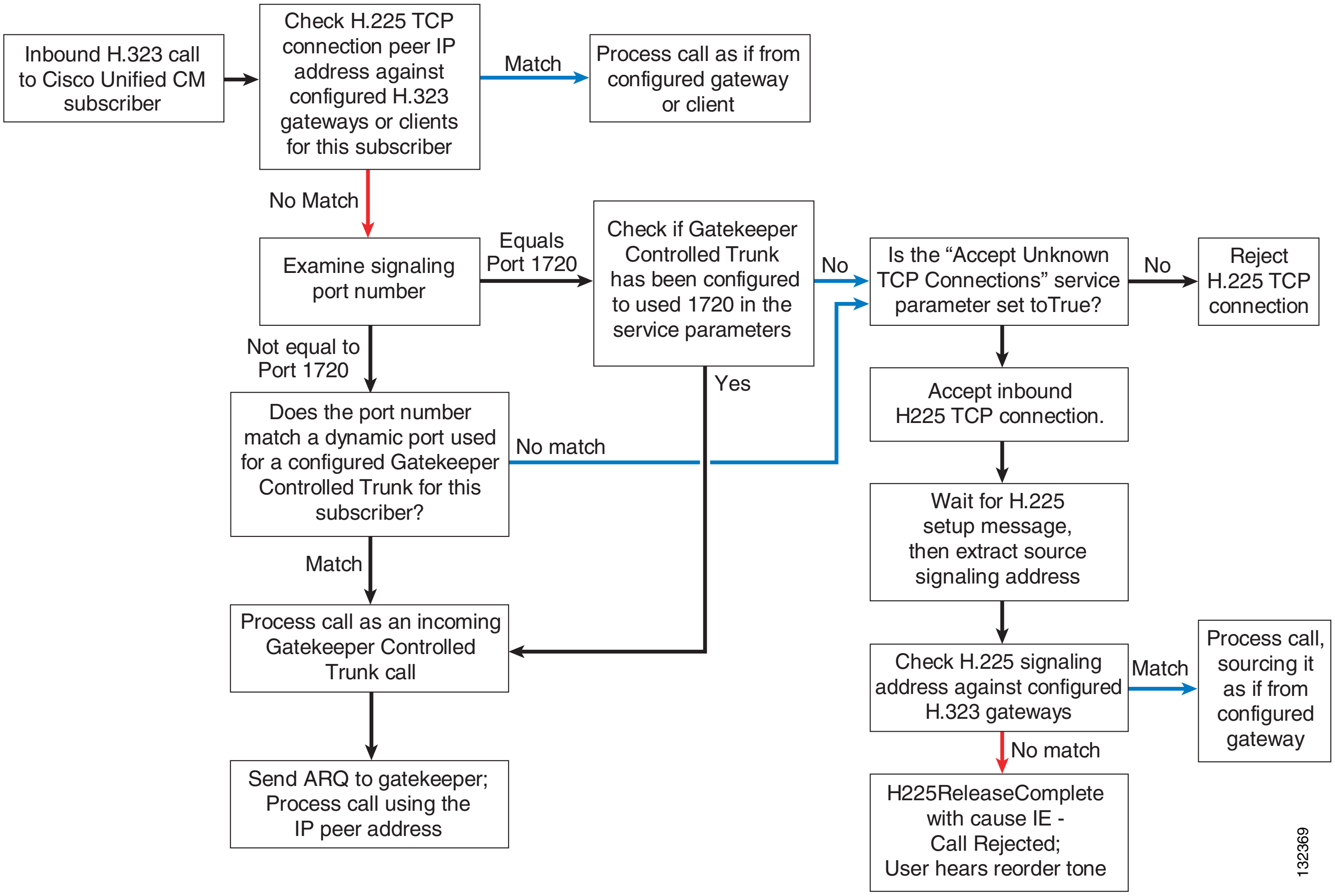
  The H.225D is active on all subscribers in the Cisco Unified CallManager group associated with the H.323 gateway.

- H.323 trunks

  The H.225D is active on all subscribers in the Cisco Unified CallManager group associated with the H.323 trunk. A RAS daemon registers the trunk with the gatekeeper from all subscribers in the associated Cisco Unified CallManager group.

When an incoming H.323 call is made to a subscriber in a Cisco Unified CallManager cluster, various decisions are made to determine if the call is accepted or rejected and which H.225D will receive the call if it is accepted. Figure 5-5 shows how this process works.

Figure 5-5 Process for Determining if an H.323 Call is Accepted or Rejected


Inbound H.323 call to Cisco Unified CM subscriber
Check H.225 TCP connection peer IP address against configured H.323 gateways or clients for this subscriber
Match
Process call as if from configured gateway or client
No Match
Examine signaling port number
Equals Port 1720
Check if Gatekeeper Controlled Trunk has been configured to used 1720 in the service parameters
No
Is the "Accept Unknown TCP Connections" service parameter set toTrue?
No
Reject H.225 TCP connection
Not equal to Port 1720
Yes
Accept inbound H225 TCP connection.
Does the port number match a dynamic port used for a configured Gatekeeper Controlled Trunk for this subscriber?
No match
Wait for H.225 setup message, then extract source signaling address
Match
Process call as an incoming Gatekeeper Controlled Trunk call
Check H.225 signaling address against configured H.323 gateways
Match
Process call, sourcing it as if from configured gateway
No match
Send ARQ to gatekeeper; Process call using the IP peer address
H225ReleaseComplete with cause IE - Call Rejected; User hears reorder tone
132369

Cisco Unified CallManager H.323 protocol includes the following additional features:

- Protocol Auto Detect

  This feature provides the ability to determine, on a call-by-call basis, if the calling device is from Cisco Unified CallManager Release 3.2 or later. Whenever a call is received, Cisco Unified CallManager looks for an H.225 User-to-User Information Element (UUIE) that indicates if the other end is another Cisco Unified CallManager. If it is, it will always use the Intercluster Trunk Protocol. If no UUIE is found, it will use the configured protocol for that device. This feature enables an H.225 gatekeeper controlled trunk to switch between Intercluster Trunk Protocol and H.225 on a call-by-call basis, allowing a mixture of Cisco Unified CallManager clusters and other H.323 devices to use the gatekeeper. Intercluster Trunk Protocol is the same as H.225 except for several differences that enable specific features to work correctly between Cisco Unified CallManager clusters.

- Tunneled Q.SIG or H.323 Annex M1

  With the release of Cisco Unified CallManager 4.1(3), this feature can be enabled on all H.323 trunks. It allows specific H.323 Annex M1 features to be implemented between Cisco Unified CallManager clusters and other verified systems that also support H.323 Annex M1. These features include:

  - Path replacement
  - Message waiting indication (MWI)
  - Callback

- Alternate Endpoints

  When registering with a gatekeeper that supports this feature, such as a Cisco Multimedia Conference Manager (MCM) Gatekeeper, Cisco Unified CallManager can inform the gatekeeper of alternate destinations for calls to the H.323 trunk. These alternate endpoints or destinations are sent to the calling device by the gatekeeper when this H.323 trunk is called. They are the other subscribers listed in the Cisco Unified CallManager group associated with the H.323 trunk that registers with the gatekeeper.

- Alternate Gatekeeper

  When an H.323 trunk registers with a gatekeeper that supports this feature (for example, a Cisco gatekeeper cluster), Cisco Unified CallManager is dynamically informed about other gatekeepers that can process registrations, call admission requests, and other RAS functions in the event that this gatekeeper fails or exhausts its own resources.

- CanMapAlias

  When an H.323 trunk sends an admission request (ARQ) to the gatekeeper, it might receive a different E.164 number in the admission confirmation message (ACF), indicating that the original called number should be replaced with this new one. This feature requires a route server using Gatekeeper Transaction Message Protocol (GKTMP) to communicate with Cisco gatekeepers.

  Note CanMapAlias is supported for the called number only.

- Bandwidth Requests

  H.323 trunks can update the gatekeeper with bandwidth information to indicate a change in the requested bandwidth allocated to a specific call. This feature is disabled by default and is controlled by setting the Cisco CallManager service parameter **BRQ Enabled** to **True**, under the H.323 section. This feature is especially important when video is used on an H.323 trunk because the original bandwidth request is for the maximum amount allowed. Enabling this feature ensures that call admission control uses the actual bandwidth negotiated during call setup.

SIP Trunks

Support for SIP trunks was first added in Cisco Unified Callmanager Release 4.0.

A SIP trunk configuration causes members of a Cisco Unified CallManager cluster to behave as a SIP User Agent, and the cluster expects the other SIP entity defined in the configuration to act as a SIP User Agent also. The SIP trunk is used to configure communication to any SIP entity that can act as a SIP User Agent, which includes SIP proxies, SIP gateways, SIP redirect servers, or other Cisco Unified CallManager clusters. Specifically, it also includes Cisco Unity and Cisco Unified MeetingPlace SIP interfaces.

In Cisco Unified CallManager 4.2 and earlier releases, SIP trunks have the following characteristics:

- Each SIP trunk defined in the system must use a unique incoming port number.
- Each call using a SIP trunk requires a media termination point (MTP) resource.
- The codec for all calls established over a given trunk is restricted to either G.711 mu-law or a-law.
- Q.SIG Tunneling using Annex M1 is not supported.
- The trunk may be used to connect only to devices that implement early media support. In other words, Cisco Unified CallManager will initiate calls by sending an Invite message with Session Description Protocol (SDP), and the far end must be capable of accepting this Invite message.
- Secure Real-Time Transport Protocol (SRTP) is not supported.
- Video calls are not supported.
- TLS is not supported.

Note Refer to the *Cisco Unified Communications SRND for Cisco Unified CallManager 5.0* to understand which of the above restriction no longer apply for that release.

SIP Trunk Redundancy

One of the main benefits of using SIP trunks for intercluster trunking is call survivability. Unlike H.323 trunks in Cisco Unified CallManager Release 3.3 and later, SIP trunks can point to only a single IP address or DNS Server (SRV) record. To provide failover and load balancing for intercluster SIP trunks that are not capable of DNS SRV, configure multiple SIP trunks. In addition, these SIP trunks must be members of route groups and route lists.

It is important to note that Cisco Unified CallManager accepts calls only from a SIP device whose IP address matches one of the destination addresses of the configured SIP trunks. In addition, the incoming port number of the SIP messages has to match the port number configured for that SIP trunk. As a consequence, Cisco recommends that you configure as many SIP trunks with destination addresses as needed to match all IP addresses of any far-end SIP devices that can potentially place an inbound call. This method is not desirable for deployments with more than two Cisco Unified CallManager clusters, and it is better to use SIP trunks with DNS SRV if there are more than two clusters. Figure 5-6 shows the call flow for an intercluster SIP trunk call using DNS SRV.

Figure 5-6 Call Flow for Intercluster SIP Trunk Using DNS SRV

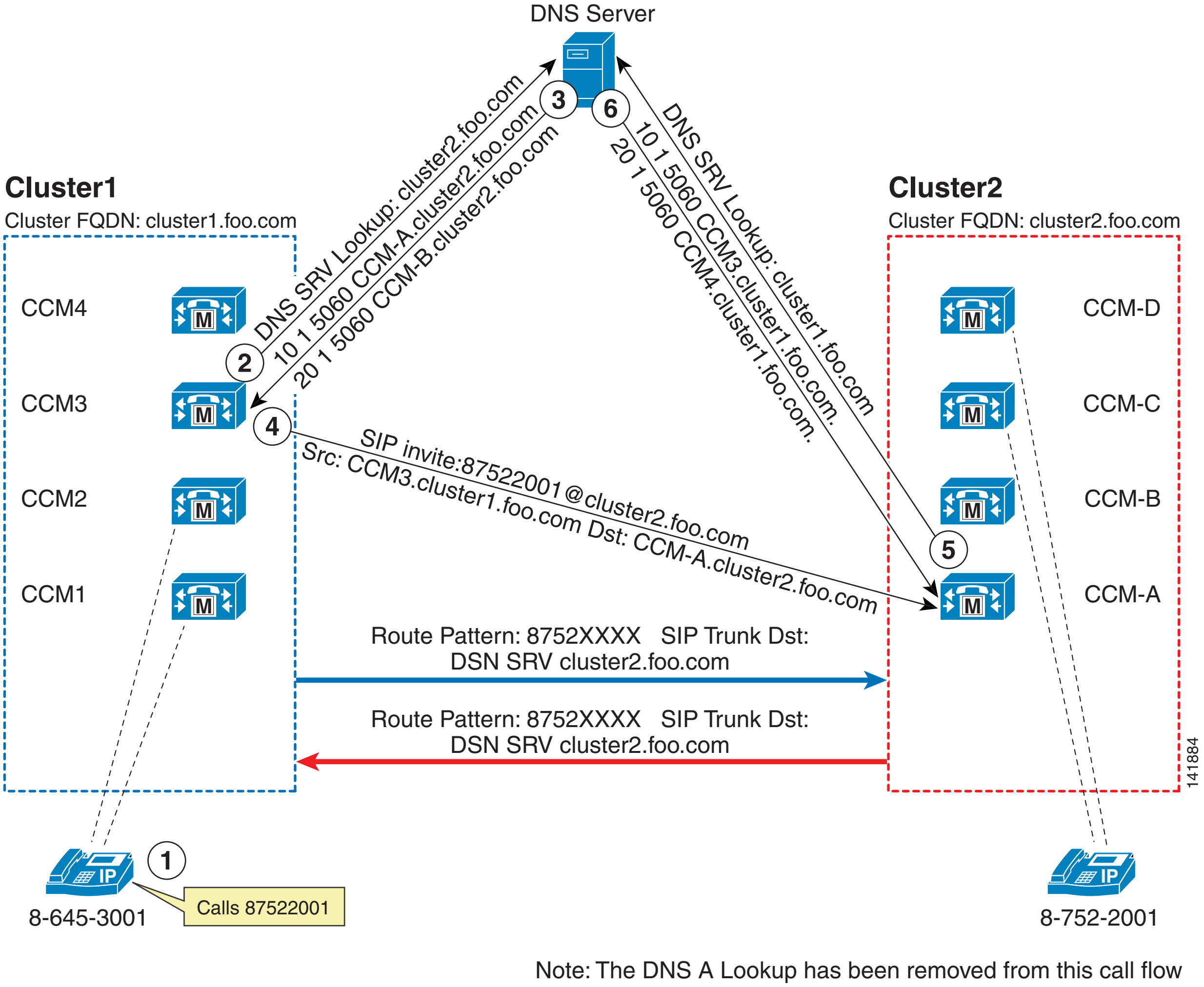

DNS Server
Cluster1
Cluster FQDN: cluster1.foo.com
CCM4
CCM3
CCM2
CCM1
M
Cluster2
Cluster FQDN: cluster2.foo.com
CCM-D
CCM-C
CCM-B
CCM-A
2
DNS SRV Lookup: cluster2.foo.com
3
10 1 5060 CCM-A.cluster2.foo.com
20 1 5060 CCM-B.cluster2.foo.com
6
DNS SRV Lookup: cluster1.foo.com
10 1 5060 CCM3.cluster1.foo.com.
20 1 5060 CCM4.cluster1.foo.com.
4
SIP invite:87522001@cluster2.foo.com
Src: CCM3.cluster1.foo.com Dst: CCM-A.cluster2.foo.com
5
Route Pattern: 8752XXXX SIP Trunk Dst:
DSN SRV cluster2.foo.com
Route Pattern: 8752XXXX SIP Trunk Dst:
DSN SRV cluster2.foo.com
141884
1
IP
Calls 87522001
8-645-3001
8-752-2001
Note: The DNS A Lookup has been removed from this call flow

Figure 5-6 illustrates the following steps in the call flow:

1. The IP phone in Cluster1 calls 87522001.
2. The call matches a route pattern of 8752XXXX that is pointing to SIP Trunk with DNS SRV of cluster2.foo.com. CCM3 in Cluster1 is the node handling this call because the SIP trunk is registered to it. CCM3 sends a DNS SRV lookup for cluster2.foo.com
3. The DNS server replies with two records: CCM-A.cluster2.foo.com and CCM-B.cluster2.foo.com. Because CCM-A.cluster2.foo.com has a higher priority, the call is attempted to this Cisco Unified CallManager. Before sending the SIP Invite, another DNS lookup is done for CCM-A.cluster2.foo.com.
4. CCM3 sends a SIP Invite to 87522001@cluster2.foo.com with destination address set to the IP address of CCM-A.
5. Cisco Unified CallManager interprets this call as a local call because the host portion of the uniform resource identifier (URI) matches the Cluster FQDN enterprise parameter. Cluster2 does not have any SIP trunk configured with a destination of CCM3, so it does a DNS SRV lookup for all domains configured under the SIP trunks with DNS SRV. In this case, the example shows a single trunk with a DNS SRV destination of cluster1.foo.com

6. The DNS server returns two entries, and one of them matches the source IP address of the invite. The cluster accepts the call and extends it to extension 87522001.