Solution Reference Network Design (SRND) for Cisco Instant Connect/Cisco IPICS, Release 4.7

December 10, 2014
CONTENTS

Preface ix
Overview ix
Revision History ix
Organization ix
Related Documentation x
Obtaining Documentation, Obtaining Support, and Security Guidelines x

CHAPTER 1

Introducing Cisco IPICS 1-1
Cisco IPICS Benefits 1-1
Cisco IPICS Components 1-2

CHAPTER 2

Cisco IPICS Component Considerations 2-1
Media Resource Allocation for the Dial Engine 2-1
Virtual Talk Groups 2-2
Cisco IPICS Endpoint Scenarios—Multicast 2-3
Cisco IPICS Endpoint Scenarios—Unicast 2-10
Integrating Cisco IPICS with SIP Providers 2-11
Requirements for SIP Sessions 2-11
Default Dial Peer Scenarios 2-12
Dial Peer Use in Scenarios 2-12
Call Flow and Dial Peer Examples 2-13
Cisco Instant Connect for Android Devices 2-16
DNS Configuration 2-16
Intranet Access Model 2-16
Internet/Intranet Access Model 2-17
Wireless Network Configurations 2-18
Wireless Controller Configuration Example 2-18
Cisco Unified IP Phones 2-20
Cisco Unified Communications Manager Configuration Overview 2-21
Cisco Unified Communications Manager Express Configuration Overview 2-21
Notification 2-22
Email Notification Action 2-22
IP Phone Text Notification Action 2-22
## Contents

- Dial Notification Action  2-23
- Talk Group Notification Action  2-24
- Port Usage  2-24

### CHAPTER 3

**Cisco IPICS UMS**  3-1

- UMS Overview  3-1
- When is a UMS Required?  3-2
- UMS Instances for Locations  3-2
- UMS Scaling  3-3
- UMS Resource Allocation  3-3
- Remote Users  3-4
- UMS Audio Mixing  3-4

### CHAPTER 4

**Cisco IPICS LMR Gateway Configurations**  4-1

- Interfacing the Cisco IPICS LMR Gateway with Land Mobile Radios  4-1
  - Cabling  4-2
  - Analog E&M Interface  4-3
  - Analog E&M signaling Types  4-4
- Cisco IOS LMR Gateway Configurations  4-6
  - Determining Correct Cisco IOS Radio Control  4-6
  - Required Baseline LMR Gateway Configuration  4-7
  - VAD Operated Signaling Configuration  4-8
  - COR/COS Operated Signaling Configuration  4-10
  - DSP Channel Optimization and Allocation  4-11
- Analog Tap Recording Configuration  4-11
- Recording Multicast LMR Traffic  4-12
- Recording Tap Cisco IOS Configuration  4-12

### CHAPTER 5

**Cisco IPICS Infrastructure Considerations**  5-1

- WAN Considerations  5-2
- Multicast Routing  5-2
- Bandwidth Planning  5-4
  - Choosing a Codec  5-4
  - Calculating Codec Bandwidth Use  5-5
  - cRTP, Variable-Payload Sizes and Aggressive VAD  5-6
  - RTP Header Compression  5-7
  - Adjustable Byte Size of the Voice Payload  5-7
Aggressive Voice Activity Detection 5-7
Mixing Voice Streams 5-8
Quality of Service 5-8
QoS Overview 5-9
Cisco IOS Queuing Techniques 5-10
  IP RTP Priority 5-10
  Low Latency Queuing 5-10
QoS with Frame Relay 5-11
  Frame Relay Broadcast Queue 5-13
QoS with Point-to-Point Connections 5-19
QoS for a LAN 5-20
QoS at the WAN Edge 5-20
Policing 5-20
Queuing 5-21
Trust Boundaries 5-21
VPN in Deployment Scenarios 5-23
Port Utilization 5-23
  Guidelines for Using IP Multicast Addresses with Cisco IPICS 5-24
  QOS Policy Considerations 5-25
Securing the Cisco IPICS Infrastructure 5-25
  Secure Socket Layer 5-25
  Firewalls and Access Control Lists 5-25
  Other Security Recommendations 5-25
Cisco IPICS Network Management System 5-26
  Managing the Overall Network 5-26

CHAPTER 6
Understanding Dial Peers 6-1
  Dial Peer Call Legs 6-1
  Inbound and Outbound Dial Peers 6-2
  Destination Pattern 6-3
  Session Target 6-3
  Configuring Dial Peers for Call Legs 6-3
  Matching Inbound and Outbound Dial Peers 6-4

CHAPTER 7
Cisco IPICS Licensing and Sizing Guidelines 7-1
  Resource and License Usage 7-1
  UMS Usage 7-1
  Additional Planning and Sizing Guidelines 7-2
Dial Port Licensing Details 7-2

CHAPTER 8

Cisco IPICS Deployment Models 8-1

Single Site Model 8-1
- Benefits of the Single Site Model 8-2
- Best Practices for the Single Site Model 8-2

Multiple Site Model 8-2
- MPLS with Multicast VPNs 8-3
  - MPLS Terminology 8-4
  - MVPN Basic Concepts 8-5
  - VPN Multicast Routing 8-5
- Configuring the Provider Network for MVPN 8-5
- Verifying the Provider Network for MVPN 8-7
- Optimizing Traffic Forwarding: Data MDT 8-9
- Verifying Correct Data MDT Operation 8-9

- Multicast Islands 8-10
- Multicast over GRE 8-11
- Multicast Singularities 8-13
- VPN Termination for Mobile Clients 8-15
Preface

Overview

This Solution Reference Network Design (SRND) document provides design considerations and guidelines for deploying Cisco Interoperability and Collaboration System (Cisco IPICS) release 4.7. This document should be used with the related documentation that the “Related Documentation” section on page x describes.

For other design documents, go to this URL:

http://www.cisco.com/go/srnd

Revision History

This document may be updated at any time without notice. Check the Cisco.com website periodically for documentation updates.

Organization

This manual is organized as follows:

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1, “Introducing Cisco IPICS”</td>
<td>Provides information about various Cisco IPICS components</td>
<td></td>
</tr>
<tr>
<td>Chapter 2, “Cisco IPICS Component Considerations”</td>
<td>Describes configurations needed to use land mobile radios with Cisco IPICS</td>
<td></td>
</tr>
<tr>
<td>Chapter 4, “Cisco IPICS LMR Gateway Configurations”</td>
<td>Provides information about network infrastructure considerations that you must be aware of when you deploy Cisco IPICS</td>
<td></td>
</tr>
<tr>
<td>Chapter 5, “Cisco IPICS Infrastructure Considerations”</td>
<td>Provides an overview of dial peers, which will help you understand how Cisco IPICS operates</td>
<td></td>
</tr>
</tbody>
</table>
To access the documentation suite for Cisco IP Phone models 7905G and 7912G, go to the following URL:


Cisco also provides a variety of other documentation that includes related information about Cisco IP Phone models 7905G and 7912G components and the configuration of an infrastructure that supports Cisco IP Phone models 7905G and 7912G. References to related documentation is provided throughout this manual as appropriate.
Cisco IPICS release 4.7 is a platform that enables push-to-talk (PTT) communications in Cisco Unified Communications (UC) installations. Customers who used the Sprint Nextel system can use Cisco IPICS with the Cisco Wireless IP Phone 79256 and 7926 to create an on-premises PTT solution. A PTT solution for off-premises can be implemented with the addition of Cisco IPICS for Android devices.

This chapter provides an overview of Cisco IPICS. It describes the advantages and benefits that Cisco IPICS offers to various organizations. It also introduces the primary components of a Cisco IPICS deployment.

This chapter includes these topics:

- Cisco IPICS Benefits, page 1-1
- Cisco IPICS Components, page 1-2

Cisco IPICS Benefits

On-premises PTT is an important requirement in many markets, including the following segments:

- Enterprise (operations and safety and security)
- Commercial
- Retail
- Education
- Healthcare
- Government
- Service provider

Organizations in these market segments typically deploy several wired networks and wireless networks to achieve their business and service goals. However, such disparate solutions often do not support interoperability and collaboration, which can affect operational efficiency and customer satisfaction.

Examples of such disparate networks include:

- Legacy push-to-talk (PTT) radio networks (analog or digital at different frequencies) that are used for voice communications within groups. Communication is usually restricted within a specified group or network because of radio frequency (RF) limitations and proprietary protocols.
• Traditional hoot bridges that are connected over time-division multiplexing (TDM) circuits. These deployments cannot provide audit trails and they do not seamlessly integrate with other PTT or Voice over IP (VoIP) networks. In addition, they do not offer the mobility and serviceability that an IP deployment provides.

• VoIP networks that are used to carry packetized voice on wired or wireless IP phones or on other IP clients. These clients do not interact with the PTT services.

For organizations that use disparate networks, Cisco IPICS provides the following benefits:

• Easy-to-use installation, management, and operational features—Enables a migration path to more robust IP applications, devices, and IP-based solutions to achieve greater operational efficiencies.

• Effective solution—Streamlines operations, and command and control while protecting investments in deployed radio networks or legacy hoot bridges and applications.

• Efficient deployment—Leverages current IP infrastructure with minimal upgrades required, decreasing total cost of ownership.

• Resiliency—Eliminates communications silos and single points of failure.

**Cisco IPICS Components**

A Cisco IPICS deployment involves several hardware and software components to enable true interoperability and collaboration. Components include new products, such as the Cisco IPICS server, Cisco gateways, and VoIP. A deployment also employs applications of new technologies, such as the use of the unified media service (UMS) functionality for channel mixing.

Figure 1-1 illustrates the major components of a Cisco IPICS deployment.

**Figure 1-1  Cisco IPICS Components**
Table 1-1 provides an overview of the Cisco IPICS components. Other chapters in this manual provide more detailed information about using and configuring several of these components. In addition, Cisco provides a wide variety of technical and user documentation that explains in detail Cisco components that are used in the deployment of Cisco IPICS. These documents include information about installing, configuring, operating, managing, maintaining, and troubleshooting components.

For version and compatibility information, see *Cisco IPICS Compatibility Matrix*.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IPICS server</td>
<td>Provides the core functionality of the Cisco IPICS system. The Cisco IPICS server software runs on the Cisco Linux operating system (based on Red Hat Linux) on selected Cisco Unified Computing System (UCS) platforms and performs these functions:</td>
</tr>
<tr>
<td></td>
<td>• Hosts the Cisco IPICS Administration Console, an administration GUI that enables dynamic resource management for users, channels, and virtual talk groups (VTGs).</td>
</tr>
<tr>
<td></td>
<td>• Provides Cisco IPICS authentication and security services</td>
</tr>
<tr>
<td></td>
<td>• Stores configuration and operational data</td>
</tr>
<tr>
<td></td>
<td>• Enables integration with various media resources, such as UMS components, Cisco Unified IP Phones, Cisco Unified Communications Manager, and Cisco IOS SIP gateways</td>
</tr>
<tr>
<td>Cisco Instant Connect for Android Devices</td>
<td>An application for that allows you to use Android devices to interact with other participants in a Cisco IPICS call.</td>
</tr>
<tr>
<td>Cisco Instant Connect MIDlet</td>
<td>An application for certain Cisco Unified Wireless IP Phone models that lets you communicate with other Cisco IPICS users via a point-to-point or standard telephone call, and communicate via channels, VTGs, and incidents by using the IP phone as a PTT device.</td>
</tr>
<tr>
<td></td>
<td>For a list of Cisco Unified Wireless IP Phone models and minimum firmware version that support the Cisco Instant Connect MIDlet, see <em>Cisco IPICS Compatibility Matrix</em>.</td>
</tr>
<tr>
<td></td>
<td>For detailed information about installing and using the MIDlet, see <em>Cisco Instant Connect MIDlet Reference Guide</em>.</td>
</tr>
<tr>
<td>Unified media service (UMS)</td>
<td>Enables media services and provides these capabilities:</td>
</tr>
<tr>
<td></td>
<td>• Provides the functions that are required to combine two or more VTGs.</td>
</tr>
<tr>
<td></td>
<td>• Multicast channel mixing, using the Cisco Hoot ‘n’ Holler feature, to support VTGs.</td>
</tr>
<tr>
<td></td>
<td>• Enables PTT media convergence for multicast, unicast, TDM, and SIP endpoints.</td>
</tr>
<tr>
<td>SIP provider</td>
<td>Handles calls to and from the Cisco IPICS policy engine.</td>
</tr>
<tr>
<td>LMR gateway</td>
<td>LMR gateways provide voice interoperability between radio and non-radio networks by bridging radio channels and talk groups to IP multicast streams. The LMR gateway functionality is available in certain versions of Cisco IOS software.</td>
</tr>
</tbody>
</table>
Chapter 1      Introducing Cisco IPICS

Table 1-1  *Cisco IPICS Component Overview*

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Networking</td>
<td>Include switches, routers, firewalls, mobile access routers, and wireless</td>
</tr>
<tr>
<td>components</td>
<td>access points and bridges.</td>
</tr>
<tr>
<td>Cisco Unified IP</td>
<td>Cisco IPICS integrates selected models of the Cisco Unified IP Phone. Users</td>
</tr>
<tr>
<td>Phone</td>
<td>of these phones can select a channel from a list of channels on which to</td>
</tr>
<tr>
<td></td>
<td>participate when Cisco IPICS is configured as a phone service for Cisco</td>
</tr>
<tr>
<td></td>
<td>Unified Communications Manager or for Cisco Unified Communications Manager</td>
</tr>
<tr>
<td></td>
<td>Express when it is bundled with supported versions of Cisco IOS software.</td>
</tr>
</tbody>
</table>
CHAPTER 2

Cisco IPICS Component Considerations

This chapter provides information about various components and features that can be part of a Cisco IPICS solution. This information will help you to understand how these items interoperate in a Cisco IPICS deployment.

This chapter includes these topics:

- Media Resource Allocation for the Dial Engine, page 2-1
- Virtual Talk Groups, page 2-2
- Integrating Cisco IPICS with SIP Providers, page 2-11
- Cisco Instant Connect for Android Devices, page 2-16
- Wireless Network Configurations, page 2-18
- Cisco Unified IP Phones, page 2-20
- Notification, page 2-22
- Port Usage, page 2-24

Media Resource Allocation for the Dial Engine

When a user dials in to the Cisco IPICS dial engine, the user accesses the system through a SIP-based (unicast) connection and obtains a media connection to the Cisco IPICS Dial Management server (DMS). When the user joins a channel or VTG, Cisco IPICS configures a resource on the UMS to enable a multicast connection from the server to the dial engine. This configuration facilitates a multicast connection between the Cisco IPICS server and the selected channel or VTG.

This multicast connection is made one time for a channel or VTG, regardless of the number of dial-in users who select the channel or VTG. When the last dial-in user disconnects from the channel or VTG, the resource is released in the UMS and becomes available for use.

When a dial-in user makes a unicast media connection to the media driver on a Cisco IPICS server, the policy engine sends and receives multicast streams as follows:

1. After the dial-in user successfully authenticates and selects a resource, Cisco IPICS allocates a UMS resource for the user and allocates a multicast address from the multicast pool. Cisco IPICS then performs an Internet Group Management Protocol (IGMP) join operation on the multicast address so that when additional dial-in users select the same resource, the Cisco IPICS server can continue to use the same multicast address.

2. When the dial-in user presses 1 on a telephone and begins to talk, Cisco IPICS transmits the audio to the multicast address of the selected resources.
When the UMS receives the multicast packets, it forwards the packets to the multicast address that has been allocated from the multicast pool. Cisco IPICS receives that multicast audio stream and forwards it as a unicast stream to all dial-in users who have selected that resource.

Virtual Talk Groups

A VTG enables participants on various channels to communicate by using a single multicast address. A VTG contains, in a temporary channel, any combination of the following members:

- Channels
- Channel groups
- Users
- User groups
- Incidents

A Cisco IPICS administrator creates Cisco IPICS channels and assigns a multicast address to each one. The administrator also creates VTGs as needed. When an administrator creates a VTG, the Cisco IPICS server automatically allocates to the VTG an available address from the multicast pool. So while VTGs are dynamically assigned addresses from the multicast pool, channels are configured as static addresses that are outside the range of the addresses that are used by VTGs.

A VTG allows communication between endpoints that are assigned different multicast addresses, such as two endpoints that have activated different channels. When a VTG is enabled to facilitate communications between two or more endpoints with different multicast addresses, a UMS must bridge, or mix, the multicast streams of each channel. In this VTG scenario, the Cisco IPICS server allocates a loopback voice port for each channel in the VTG.

For example, assume that a Cisco IPICS administrator creates a VTG named Combined and that this VTG includes the Security channel and Facilities channel as members. Also assume that each LMR voice port is statically configured with a multicast address, so that LMR security users always send to the Security channel, and LMR facilities users always send to the Facilities channel. To provide communication between the Security channel and the Facilities channel, a UMS must bridge the multicast streams from these channels.

In this example, when a user talks on the Security channel (channel 1), the UMS must bridge that multicast stream to the Facilities channel (channel 2) and to the VTG channel. The UMS must perform similar operations when a user talks on channel 2 or on the VTG channel. See Figure 2-1.
Cisco IPICS Endpoint Scenarios—Multicast

When a Cisco IPICS dispatcher activates the Combined VTG (as shown in Figure 2-1), Cisco IPICS configures the UMS to mix the Security, Facilities, and Combined VTG channels. Users who have been added to the VTG will see the new Combined VTG channel on their mobile clients or Cisco Unified IP Phones. LMR endpoints do not have associated users. An LMR channel is statically configured, so an LMR user can send and receive only from the Cisco IPICS channel that is configured with the same multicast address as the LMR channel. An LMR user can communicate only with endpoints that are not using the same channel if the channel of the LMR user is in a VTG with other channels or users.

Figure 2-2 illustrates a scenario in which four users have deactivated their Security or Facilities channels and have activated the Combined VTG channel.
When a user deactivates the Security and Facilities channels and activates the Combined VTG channel, the endpoint sends an Internet Group Management Protocol (IGMP) leave message for the Security and Facilities channels and an IGMP join message for the Combined VTG channel. The LMR voice port channels are statically configured and the VIF will have already joined the configured multicast group. As shown in Figure 2-3, when user A transmits, the system sends the multicast packets via the multicast distribution tree to each endpoint that has joined the combined group, and to the UMS, which mixes the audio and sends it to the channels in the VTG.
When the UMS receives the traffic over the Combined VTG channel, it mixes this channel with the Security and Facilities channels and forwards the mixed stream to the LMR endpoints, as shown in Figure 2-4.

When the LMR Facilities user transmits, the only other endpoint that has joined this multicast channel is the UMS. The multicast distribution tree forwards the multicast voice traffic to the UMS, where it is mixed with the Facilities channel and the Combined VTG channel and then forwarded to the other
Virtual Talk Groups

endpoints in the VTG. See Figure 2-5.

Figure 2-5 LMR Multicast Traffic Flow

Figure 2-6 shows User C with two active channels: the Facilities channel and the Combined VTG channel.

Figure 2-6 Traffic Flow with Two Active Channels
Because User C activated two channels (Facilities and the Combined VTG), two multicast groups are joined through IGMP. As a result, when an endpoint in the Combined VTG transmits, User C will receive the transmitted packets twice. (In this case, the duplicate packets can cause audio quality issues. Take care to avoid this scenario.)

If there are no LMR endpoints in a VTG, UMS resources may not be required for the VTG. For example, consider a financial institution with one Cisco IPICS channel called Stocks and one channel called Bonds. The users who are associated with the Stocks channel can communicate with each other, and the users who are associated with the Bonds channel can communicate with each other. Figure 2-7 illustrates this scenario.

![Figure 2-7 Cisco IPICS Scenario with no LMR Endpoints](image)

If a VTG is created that contains users but no channels, UMS resources are not required. The only resource that is required in this case is a multicast channel from the multicast pool. UMS resources are not needed because Cisco Unified IP Phone users, unlike LMR users, are not statically configured for one channel. If users only are placed in the VTG, users will see the VTG on their Cisco Unified IP Phones. When the VTG activates, these endpoints will simply join the VTG multicast channel that is allocated by the Cisco IPICS server. See Figure 2-8.
You can also avoid consuming UMS resources by creating a new channel and associating all users with that channel, instead of creating a VTG. In this example shown in Figure 2-8, there is a channel called Combined. Users will see two channels on their Cisco Unified IP Phones: the Combined VTG channel, and either the Stocks channel or the Bonds channel.

If you do not want a user (for example, User C) to participate in such a combined VTG channel, you can take either of these actions:

- Create a channel (you could name it Combined) and associate with it all users except User C
- Create a combined VTG with all users except User C

See Figure 2-9 for an illustration of this scenario.
If you create a VTG that includes the Stocks channel, the Bonds channel, and all users except User C, all of the users except User C will see the Combined VTG channel on their Cisco Unified IP Phones. However, because the Stocks channel and the Bonds channel are in the VTG, User C will be able to receive from and transmit to the VTG. See Figure 2-10.

**Figure 2-10 Combined VTG with a User Omitted**

If you create a VTG that includes the Stocks channel, the Bonds channel, and all users except User C, all of the users except User C will see the Combined VTG channel on their Cisco Unified IP Phones. However, because the Stocks channel and the Bonds channel are in the VTG, User C will be able to receive from and transmit to the VTG. See Figure 2-10.
Cisco IPICS Endpoint Scenarios—Unicast

Figure 2-11  Unicast Connection Set Up

Figure 2-12  SIP Signaling Flow
Integrating Cisco IPICS with SIP Providers

The Cisco IPICS dial engine requires a SIP provider to place or receive calls. See *Cisco IPICS Compatibility Matrix* for a list of supported SIP providers (Cisco Unified Communications Manager or Cisco Unified Communications Manager Express with a router running a supported Cisco IOS release).

All calls to or from the Cisco IPICS dial engine go through the configured SIP provider. Because a Cisco IPICS deployment can vary depending on the call flow, it is important to understand how a call flow works so that you can properly configure supporting components. *Cisco IPICS Server Administration* provides instructions for configuring the UMS and the Cisco IOS SIP gateway and SIP provider. The way in which a SIP provider is deployed in a network and the dial plan at your site dictate how components are configured.

The following sections describe how Cisco IOS dial peers are configured to provide connectivity for various scenarios:

- Requirements for SIP Sessions, page 2-11
- Default Dial Peer Scenarios, page 2-12

Requirements for SIP Sessions

Cisco IPICS imposes the following requirements on SIP sessions:

- SIP sessions between the SIP provider and Cisco IPICS are restricted to the following media capabilities:
  - Codec must be G.711u-law
  - Packet size must be 20 bytes (the default value for G.711 u-law)
  - Sampling rate must be 8000 Hz (the default value for G.711 u-law)
  - Telephone event payload must be 101
The multicast packets that Cisco IPICS sends to the UMS must have a Time to Live (TTL) of 64. This value is not configurable.

A firewall must allow TCP and UDP traffic to pass on ports 5060 and 5061 for SIP signaling. A firewall must allow UDP traffic to pass on ports 1600 through 20480 for the voice payload.

The firewall must allow TCP and UDP traffic to pass through on ports 5060 and 5061 and UDP 16000–20480.

NAT traversal is not supported by Cisco IPICS. There cannot be a NAT between Cisco IPICS and the UMS or between Cisco IPICS and the SIP provider.

Default Dial Peer Scenarios

You must configure specific incoming dial peers and outgoing dial peers on the telephony gateway. These configurations vary depending on whether you use the Cisco IOS gateway or Cisco Unified Communications Manager. There also are dial peer requirements when you use the Cisco IPICS direct dial feature. For related information about configuring Cisco IPICS for the direct dial feature, see the “Configuring SIP” section in Cisco IPICS Server Administration.

Dial Peer Use in Scenarios

The following figures describe which dial peers are used in different scenarios:

- Figure 2-14 on page 2-12, “Calls to Policy Engine in Deployment that Uses Cisco Unified Communications Manager”
- Figure 2-15 on page 2-13, “Calls from Policy Engine in Deployment that Uses Cisco Unified Communications Manager”

![Figure 2-14 Calls to Policy Engine in Deployment that Uses Cisco Unified Communications Manager](image)

---

*Figure 2-14 Calls to Policy Engine in Deployment that Uses Cisco Unified Communications Manager*
Call Flow and Dial Peer Examples

The following sections describe possible call flows and provide dial peer configuration examples for various scenarios:

- **Scenario 1: Policy Engine < - > SIP < - > Cisco Unified Communications Manager 8.6(2)**, page 2-13
- **Scenario 2: Policy Engine <-> SIP <-> Cisco IOS SIP Gateway, with no Cisco Unified Communications Manager or Cisco Unified Communications Manager Express**, page 2-14
- **Scenario 3: Policy Engine <-> SIP <-> Cisco IOS SIP Gateway, Cisco Unified Communications Manager**, page 2-14

**Scenario 1: Policy Engine < - > SIP < - > Cisco Unified Communications Manager 8.6(2)**

This scenario requires a SIP trunk between Cisco IPICS and Cisco Unified Communications Manager for dial in and dial out.

Figure 2-16 illustrates this scenario.
This scenario does not include a Cisco IOS SIP gateway, so only relevant dial peer entries are configured in the UMS.

Cisco Unified Communications Express dial peers are configured as follows. The `dtmf-relay rtp-nte` setting is required to allow parties called by the dial engine to enter DTMF digits when the parties connect to the Cisco IPICS telephony user interface (TUI).

```plaintext
dial-peer voice 555 voip
   voice-class codec 2
   session protocol sipv2
   incoming called-number .
   dtmf-relay rtp-nte
   no vad

dial-peer voice 556 voip
   description sip provider
destination-pattern .T
   voice-class codec 1
   session protocol sipv2
   session target ipv4:<Cisco Unified Communications Manager 8.6(2) IP Address>
   session transport tcp
   dtmf-relay rtp-nte
```

**Scenario 2: Policy Engine <-> SIP <-> Cisco IOS SIP Gateway, with no Cisco Unified Communications Manager or Cisco Unified Communications Manager Express**

This scenario is dependent on the desired SIP call routing. The appropriate dial peers must be configured based on your requirements. In most cases, this configuration will be a subset of scenario 3 in which the dial peers that are used for connectivity with the Cisco Unified Communications Manager are modified to reflect the desired dial patterns and destinations.

**Scenario 3: Policy Engine <-> SIP <-> Cisco IOS SIP Gateway, Cisco Unified Communications Manager**

In scenario, the Cisco IOS SIP gateway is the SIP provider and the SIP trunk for direct dial is on a separate router.

*Figure 2-17* illustrates this scenario.
The example dial peer configuration in this scenario assumes the following:

- Phones that are connected to Cisco Unified Communications Manager have five-digit extensions.
- Outbound calls to the PSTN and to other Cisco Unified Communications Manager servers are routed in the Cisco Unified Communications Manager servers by using 9 and 8.
- Dial numbers that ops views use to reach the dial engine are five-digit numbers that start with 251.
- There is no direct dial prefix so no translation rules are required.

This scenario addresses the following call types:

- Calls from Cisco Unified Communications Manager (incoming dial peer 555, outgoing dial peer 25100 on Cisco IOS SIP gateway)
- SIP calls from the dial engine through the Cisco IOS SIP gateway to Cisco Unified Communications Manager (incoming dial peer 555, outgoing dial peers 25000.8000 and 9000 on Cisco IOS SIP

Cisco IOS SIP gateway dial peers are configured as follows:

```plaintext
dial-peer voice 555 voip
   voice-class codec 2
   session protocol sipv2
   incoming called-number .
   dtmf-relay rtp-nte
   no vad
!
dial-peer voice 25000 voip
   destination-pattern ..... 
   voice-class codec 1
   session target ipv4:<Cisco Unified Communications Manager 4.1 IP Address>
   session transport tcp
   dtmf-relay h245-alphanumeric 
!
dial-peer voice 9000 voip
   destination-pattern 9T
   voice-class codec 2
   session target ipv4:<Cisco Unified Communications Manager 4.1 IP Address>
   dtmf-relay h245-alphanumeric 
!
dial-peer voice 8000 voip
```
destination-pattern 8T  
voice-class codec 2  
session target ipv4:<Cisco Unified Communications Manager 4.1 IP Address>  
dtmf-relay h245-alphanumeric

!  
dial-peer voice 25100 voip  
destination-pattern 251..  
session protocol sipv2  
session target ipv4:<Cisco IPICS Server IP Address>  
session transport tcp  
dtmf-relay rtp-nte

Cisco Instant Connect for Android Devices

Cisco Instant Connect is an application for Android devices that allows you to use the device to interact with other participants in a Cisco PICS incident. The device can communicate with Cisco IPICS either via a WiFi network connection or a 3G/LTE connection by using the Cisco Incident app. For detailed information about this application, and information about feature limits when using a WiFi connection, refer to *Cisco Instant Connect for Android Devices User Guide*.

When using an Android device as a mobile client, be aware of the following:

- If you are using a WiFi connection, the Cisco IPICS server and the UMS component must be accessible on the wireless network.
- Network connectivity for all Cisco IPICS components that are to be used with the mobile client should be established before using the mobile client.
- When you view a list of talk lines, the information in the screen updates automatically. The update interval is defined by the IDC Update Poll option in the **Administration > Options > IDC/Client tab** in the Cisco IPCS Administration Console. The default update interval is 5 seconds.

The following sections provide related information:

- DNS Configuration, page 2-16
- Wireless Network Configurations, page 2-18

DNS Configuration

The mobile client uses SSL to communicate with the server. SSL requires that DNS be enabled in your network.

The following sections provide information about the models that you can use to configure DNS in your network.

- Intranet Access Model, page 2-16
- Internet/Intranet Access Model, page 2-17

Intranet Access Model

This section provides guidelines for how to configure DNS when a mobile client will connect to an IPICS server only on a local intranet.

- Ensure that a DNS server is configured in your LAN.
Configure each component in the Cisco IPICS component to use this DNS server for hostname resolution.

Configure the hostname for the DNS server as an entry in the DNS server.

Ensure that you can ping the Cisco IPICS server by its hostname from each mobile client.

If you are using DHCP for IP address assignments, ensure that the correct search domain is configured on the DHCP server or the wireless controller that is acting as a DHCP server. The search domain is not populated automatically.

If you are not using DHCP for IP address assignment, ensure that the correct domain name and client ID are configured on the mobile client in addition to the IP address, mask, and default gateway values.

DHCP servers use the client ID to bind the mobile client to a specific IP address. This binding ensures that the mobile client can communicate through firewalls, and access restrictions (Access Control Lists) in your network. If you do not configure a client ID, you cannot access the Incident app on a mobile client.

### Internet/Intranet Access Model

This section provides guidelines for how to configure DNS when a mobile client will connect to an IPICS server via the Internet and a local intranet.

- Ensure that a DNS server is configured in your LAN.
- Configure each component in the Cisco IPICS component to use this DNS server for hostname resolution.
- Configure the hostname for the DNS server as an entry in the DNS server.
- Do not use the Hosts file to bypass the DNS name resolution.
- Ensure that you can ping the Cisco IPICS server by its hostname from each mobile client.
- If you are using DHCP for IP address assignments, ensure that the correct search domain is configured on the DHCP server or the wireless controller that is acting as a DHCP server. The search domain is not populated automatically.
- If you are not using DHCP for IP address assignment, ensure that the correct domain name and client ID are configured on the mobile client in addition to the IP address, mask, and default gateway values.
- If you are not using the DHCP Server for IP Address assignment, then you also need to ensure that you populate the DNS Server address on the mobile client in addition to the IP Address, Mask and Default Gateway that you may specify.
- If the mobile client needs to access two domains (one for the intranet and one for the Internet), the intranet DNS must be configured to forward requests from the mobile client to the Internet DNS, and the Internet DNS must be configured to forward requests to the intranet DNS.
- If the Cisco IPICS server is reachable on the Internet and has a FQDN registered on the web, any Internet DNS can be used to resolve the IP address of the server. In such a scenario, the local DNS should be configured with the DNS address that is provided by the local ISP. Alternatively, you can use a public DNS, such as 4.2.2.2 and 8.2.2.2, to provide name resolution.
Wireless Network Configurations

If your Cisco IPICS deployment will support the following endpoints, you must include a wireless network in the deployment. This network can be a single Lightweight Wireless Access Point (LWAP) or a High Density Unified Wireless Network using wireless LAN controllers.

- Cisco Unified IP Phone 7925G
- Cisco Unified IP Phone 7926
- Cisco Mobile Client App for Android devices
- Cisco Mobile Client App for Apple devices

Cisco recommends that you perform a site survey before you deploy a wireless network to assess RF behavior in your environment. For information about site surveys, see Site Survey Guidelines for WAN Deployment, which is available at:


For additional information that relates to wireless networks, see the following documents:

- **Campus Wireless LAN Technology Design Guide**, which is available at:
- **Wireless LAN Controller (WLC) Configuration Best Practices**, which is available at:

Wireless Controller Configuration Example

The Cisco 5508 Wireless Controller can be used in a Cisco IPICS deployment. Table 2-1 describes guidelines that apply when configuring this controller from its web-based administration interface. When you make updates on a page, make sure to click the Apply button on the page to save the updates.

<table>
<thead>
<tr>
<th>Option</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Controller &gt; General page</strong></td>
<td></td>
</tr>
<tr>
<td>802.3x Flow Control Mode</td>
<td>Choose Disabled from the drop-down list.</td>
</tr>
<tr>
<td>LAG Mode on next reboot</td>
<td>Choose Disabled from the drop-down list.</td>
</tr>
<tr>
<td>Broadcast Forwarding</td>
<td>Choose Enabled from the drop-down list.</td>
</tr>
<tr>
<td>AP Multicast Mode</td>
<td>Choose Multicast from the drop-down list. Set the Multicast Group Address to 239.0.0.0.</td>
</tr>
<tr>
<td>AP Fallback</td>
<td>Choose Enabled from the drop-down list.</td>
</tr>
<tr>
<td>Fast SSID change</td>
<td>Choose Enabled from the drop-down list.</td>
</tr>
<tr>
<td>WebAuth Proxy Redirection Mode</td>
<td>Check this check box.</td>
</tr>
<tr>
<td><strong>Controller &gt; Multicast page</strong></td>
<td></td>
</tr>
<tr>
<td>Enable Global Multicast Mode</td>
<td>Check this check box.</td>
</tr>
</tbody>
</table>
### Chapter 2  
Cisco IPICS Component Considerations

#### Wireless Network Configurations

<table>
<thead>
<tr>
<th>Option</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable IGMP Snooping</td>
<td>Check this check box.</td>
</tr>
<tr>
<td>Wireless &gt; Media Stream &gt; General page</td>
<td></td>
</tr>
<tr>
<td>Multicast Direct feature</td>
<td>Check the <strong>Enabled</strong> check box.</td>
</tr>
<tr>
<td>Wireless &gt; Media Stream &gt; Streams page</td>
<td></td>
</tr>
<tr>
<td>Add New</td>
<td>Follow these steps to create a new media stream:</td>
</tr>
<tr>
<td></td>
<td>1. Click the <strong>Add New</strong> button.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Stream Name</strong> field, enter a name for the media stream.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>Multicast Destination Start IP Address</strong> field, enter the first IP address of the multicast group IP address range.</td>
</tr>
<tr>
<td></td>
<td>4. In the <strong>Multicast Destination End IP Address</strong> field, enter the last IP address of the multicast group IP address range.</td>
</tr>
<tr>
<td></td>
<td>5. In the <strong>Maximum Expected Bandwidth</strong> field, enter 1000.</td>
</tr>
<tr>
<td></td>
<td>6. In the <strong>Average Packet Size</strong> field enter 1200.</td>
</tr>
<tr>
<td></td>
<td>7. Check the <strong>RRC Periodic Update</strong> check box.</td>
</tr>
<tr>
<td></td>
<td>8. In the <strong>RRC Priority</strong> field, enter 8.</td>
</tr>
<tr>
<td></td>
<td>9. Choose best-effort from the <strong>Traffic Profile Violation</strong> drop-down list.</td>
</tr>
<tr>
<td></td>
<td>10. Click the <strong>Apply</strong> button.</td>
</tr>
<tr>
<td>Wireless &gt; 802.11b/g/n &gt; Network page</td>
<td></td>
</tr>
<tr>
<td>Data Rates</td>
<td>Choose <strong>Disabled</strong> from the 1 Mbps, 2 Mbps, 5.5 Mbps, 6 Mbps, and 9 Mbps drop-down lists.</td>
</tr>
<tr>
<td></td>
<td>Choose <strong>Mandatory</strong> from the 11 Mbps and 12 Mbps drop-down lists.</td>
</tr>
<tr>
<td></td>
<td>Choose <strong>Supported</strong> from the remaining Data Rates drop-down lists.</td>
</tr>
<tr>
<td>Wireless &gt; 802.11b/g/n &gt; Media page, Media tab</td>
<td></td>
</tr>
<tr>
<td>Unicast Video Redirect</td>
<td>Check this check box.</td>
</tr>
<tr>
<td>Multicast Direct Enable</td>
<td>Check this check box.</td>
</tr>
<tr>
<td>WLANs &gt; WLANs &gt; WLANs page, General tab</td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td>Check the <strong>Enabled</strong> check box.</td>
</tr>
<tr>
<td>Radio Policy</td>
<td>Choose <strong>802.11b/g only</strong> from the drop-down list.</td>
</tr>
<tr>
<td>Interface/Interface Group</td>
<td>Choose the appropriate Interface from the drop-down list.</td>
</tr>
<tr>
<td>Multicast Vlan Feature</td>
<td>Uncheck the <strong>Enabled</strong> check box.</td>
</tr>
<tr>
<td>Broadcast SSID</td>
<td>Check the <strong>Enabled</strong> check box.</td>
</tr>
<tr>
<td>NAS-ID</td>
<td>Enter the appropriate ID for NAS access requests.</td>
</tr>
</tbody>
</table>

---

**Table 2-1  **  
Cisco 5508 Wireless Controller Configuration (continued)
If your Cisco IPICS deployment includes Cisco Unified Communications Manager or Cisco Unified Communications Manager Express, you can use the Cisco Unified IP Phone services application programming interface (API) to provide PTT capabilities to certain Cisco Unified IP Phone models. A phone with the PTT capability enabled can provide an easy-to-use GUI that allows users to monitor or participate in a PTT channels or VTG over a VoIP network. A phone can participate in one channel or VTG at a time. To participate in a channel or VTG, a phone user chooses the desired channel or VTG from a list that displays on the phone.

The Cisco IP Phone 7925G and Cisco Wireless IP Phone 7926 can use the XML service or the more advanced Instant Connect MIDlet service. The Instant Connect MIDlet service treats channels and VTGs as talk lines. In addition, the Instant Connect MIDlet provides a person to person direct connectivity capability through the Instant Connect directory. (The Instant Connect MIDlet works only with Cisco Unified Communications Manager. Cisco Unified Communications Manager Express does not support this MIDlet.)

To enable this feature, Cisco Unified Communications Manager or Cisco Unified Communications Manager Express must be deployed in your IP telephony (IPT) network, and either of these applications must be configured with the IP address of the Cisco IPICS server. A Cisco Unified IP Phone uses this IP address to locate the server and download the PTT XML application.

For related information about configuring this feature, refer to the “Setting Up the Cisco IP Phone for use with Cisco IPICS” appendix in Cisco IPICS Server Administration Guide. For a list of Cisco Unified IP Phones that Cisco IPICS supports as PTT devices, refer to Cisco IPICS Compatibility Matrix.

This section includes these topics:

- Cisco Unified Communications Manager Configuration Overview, page 2-21
- Cisco Unified Communications Manager Express Configuration Overview, page 2-21

### Cisco Unified IP Phones

<table>
<thead>
<tr>
<th>Table 2-1</th>
<th>Cisco 5508 Wireless Controller Configuration (continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option</td>
<td>Setting</td>
</tr>
<tr>
<td>WLANs &gt; WLANs &gt; WLANs page, Security &gt; Layer 2 tab</td>
<td>To access the Security &gt; Layer 2 tab, choose WLANs &gt; WLANs &gt; WLANs, then click the WLAN that you want to configure.</td>
</tr>
<tr>
<td>Layer 2 Security</td>
<td>Choose WPA+WPA2 from the drop-down list.</td>
</tr>
<tr>
<td>WLANs &gt; WLANs &gt; WLANs page, QoS tab</td>
<td>To access the QoS tab, choose WLANs &gt; WLANs &gt; WLANs, then click the WLAN that you want to configure.</td>
</tr>
<tr>
<td>Quality of Service</td>
<td>Choose Platinum (voice) from the drop-down list.</td>
</tr>
<tr>
<td>Multicast Direct</td>
<td>Check this check box.</td>
</tr>
<tr>
<td>WLANs &gt; WLANs &gt; WLANs page, Advanced tab</td>
<td>To access the Advanced tab, choose WLANs &gt; WLANs &gt; WLANs, then click the WLAN that you want to configure.</td>
</tr>
<tr>
<td>Scan Defer Priority</td>
<td>Check the 0 check box and uncheck the 1, 2, 3, 4, 5, 6, and 7 check boxes.</td>
</tr>
<tr>
<td>Scan Defer Time</td>
<td>Enter 1000.</td>
</tr>
</tbody>
</table>
Cisco Unified Communications Manager Configuration Overview

You use the Cisco IP Phone Services Configuration page in the Cisco Unified Communications Manager Administration application to define and maintain the list of Cisco Unified IP Phone services to which users can subscribe. These services are XML applications that enable the display of interactive content on supported models of a Cisco Unified IP Phone.

After you configure a list of IP phone services, Cisco Unified IP Phone users can access the Cisco Unified Communications Manager User Options menu and subscribe to the services, or an administrator can add services to Cisco Unified IP Phones and device profiles. Administrators can assign services to speed-dial buttons, so users have one-button access to the services.

For detailed information about configuring phone services, refer to the “Cisco IP Phone Services” chapter in Cisco Unified Communications Manager System Guide.

Cisco Unified Communications Manager Express Configuration Overview

The following is a sample Cisco IOS router configuration that enables Cisco Unified Communications Manager Express to support a Cisco Unified IP Phone as a Cisco IPICS PTT device.

Note: The Cisco Instant Connect MIDlet is not supported with Cisco Unified Communications Manager Express.

```
ip dhcp excluded-address 10.1.1.1
!
ip dhcp pool pool1
    network 10.1.1.0 255.255.255.248
domain-name yourdomainname
dns-server dns1 dns2
default-router 10.1.1.1
option 150 ip 10.1.1.1

ip source-address 10.1.1.1 port 2000
auto assign 1 to n
url services http://10.1.2.1/ipics_server/servlet/IPPhoneManager
create cnf-files
max-conferences 8 gain -6
ephone-dn 1 dual-line
    number abcd
ephone-dn 2 dual-line
    number efgh
tftp-server flash:filename1

tftp-server flash:filename2
```
Notification

Notification is the process of Cisco IPICS contacting designated recipients and provide them with information that you specify. Cisco IPICS offers the following notification implementations:

- Policy engine notification—Controlled through the Cisco IPICS Administration Console and can provide notification to recipients that are configured in Cisco IPICS. You designate the way in which notification is provided by configuring notification actions. Policy engine notifications include e-mail, IP phone text, dial, talk group, and dial engine script notifications.
- External (Bulk) notification—Administered outside of the Cisco IPICS Administration Console. The recipient list and prompts are passed to Cisco IPICS by a third-party application.

Cisco IPICS supports multiple Cisco Unified Communications Managers for notification, which enables text and audio paging to Cisco Unified IP Phone devices that are registered on different Cisco Unified Communications Managers.

The following sections describe following policy engine notification actions that you can configure for Cisco IPICS:

- Email Notification Action, page 2-22
- IP Phone Text Notification Action, page 2-22
- Dial Notification Action, page 2-23
- Talk Group Notification Action, page 2-24

Email Notification Action

An Email notification action sends a message that you enter to the e-mail, SMS, and pager addresses that are configured as notification preferences for each user that you designate as a recipient. When this type of notification executes, the policy engine sends the message via SMTP to the SMTP server that is configured on the IPICS Dial Engine Parameters screen. Email notification recipients can be Cisco IPICS users or user groups.

IP Phone Text Notification Action

An IP phone text notification action displays a designated message on supported Cisco Unified IP Phone models when used with Cisco Unified Communications Manager. Cisco Unified Communications Manager Express does not support this feature. The telephone numbers of each phone must be configured as a dial preference for the associated user. This type of notification action requires that you use the Cisco IPICS Administration Console to configure parameters in the Cisco Unified Communications Manager Configuration for IP Phone Notifications area in the SIP Configuration menu. For instructions, see Cisco IPICS Server Administration Guide. Recipients of this notification action can be Cisco IPICS users or user groups.

When an IP phone text notification action executes, several activities, including the following, occur:

1. IPICS sends an AXL query to the first configured Cisco Unified Communications Manager.
2. Cisco Unified Communications Manager returns the IP address of each device for which a DN is configured.
3. Cisco IPICS sends notification via XML to each device for which it receives a valid IP address.

Notes:
The IP phone text notification action requires that the IP phone text notification parameters be configured on the SIP configuration page in the Cisco IPICS Administration Console.

Cisco IPICS sends each DN in the notification list as a query to each Cisco Unified Communications Manager that is configured for notification.

The Cisco Unified Communications Manager must be running the Cisco AXL service.

Each Cisco Unified Communications Manager must be configured in the IP Phone Notification Configuration page with the correct version number, administrator and phone user name and password. This information is required to validate Cisco Unified Communications Manager and send appropriate AXL queries because the queries are different for various Cisco Unified Communications Manager versions.

The configured Cisco Unified Communications Managers must be reachable or “Connection Failure” errors result when the Cisco IPICS attempts to send and AXL query.

The Cisco Unified Communications Manager should be configured to accept SOAP requests.

Cisco Unified Communications Manager limits the number of DNs in an AXL query to 200. It truncates requests that contain more than 200 DNs. To accommodate this limit, Cisco IPICS sends requests that contain no more than 200 DNs. If Cisco IPICS needs more than 200 DNs, it sends requests in batches that contain 200 or fewer DN requests.

Cisco IPICS precedes a text notification with an audible tone, which comes from a prerecorded .wav file that is sent to each phone in the recipient list. Cisco IPICS requires that an available multicast address be configured in the multicast address pool for each batch of simultaneous broadcasts of the alert audio.

If Cisco IPICS cannot reach a Cisco Unified IP Phone or if notification to a phone fails, Cisco IPICS adds the phone to a retry list. When Cisco IPICS completes a round of notification to identified phones, it attempts to resend the notification to the phones in the retry list. Cisco IPICS will attempt notification up to three times (one regular notification attempt and up to two retry notification attempts). Any phones that it cannot reach after these attempts are not notified via IP phone text notification.

Cisco IPICS an AXL query to all Cisco Unified Communications Managers in a cluster. If more than one Cisco Unified Communications Manager is configured with phones that register to the same DN, all the phones associated to that DN are notified.

Dial Notification Action

The policy engine executes a dial notification action as follows:

- If the Cisco Unified Communications Manager Configuration for IP Phone Notifications parameters are configured in the SIP Configuration menu, the Cisco IPICS checks whether each designated user has an associated Cisco Unified IP Phone configured in Cisco Unified Communications Manager. If a user does have an associated phone, Cisco IPICS plays the designated message on the speaker of the phone.

- If Cisco Unified Communications Manager Configuration for IP Phone Notifications parameters are configured but a user does not have an associated Cisco Unified IP Phone, or if the phone of a user is busy, the system calls the user as specified in the dial preferences and plays the designated message.

- If Cisco Unified Communications Manager Configuration for IP Phone Notifications parameters are not configured, the Cisco IPICS calls the user as specified in the dial preferences and plays the designated message.
When you create a dial notification action, you can specify a pre-recorded prompt or record a new prompt. A prompt should be no more than 90 seconds long.

If you use this action to contact Cisco Unified IP Phones, make sure that at least one multicast address is available in the multicast pool.

For more detailed information, see *Cisco IPICS Server Administration Guide*.

**Talk Group Notification Action**

A talk group notification action plays the selected prompt to all participants in the selected VTG.

When you create a talk group notification action, you can specify a pre-recorded prompt or record a new prompt. A prompt should be no more than 90 seconds long.

- When a Talk Group notification executes, the designated message is added to the multicast stream of the VTG. To inform users that a system message is being played, consider starting the message with a statement such as, “This is the Cisco IPICS administrator with an important recorded message.”

- A VTG participant who is dialed in through the TUI and who has the floor does not hear the talk group notification message.

**Port Usage**

*Table 2-2* describes the ports and transport protocols that various components use in a Cisco IPICS deployment.

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Where Used</th>
<th>Function</th>
<th>Transport Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>• Cisco IPICS server</td>
<td>HTTP</td>
<td>TCP</td>
</tr>
<tr>
<td></td>
<td>• Mobile client</td>
<td></td>
<td></td>
</tr>
<tr>
<td>443</td>
<td>• Cisco IPICS server</td>
<td>HTTPS</td>
<td>TCP</td>
</tr>
<tr>
<td></td>
<td>• Mobile client</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1194</td>
<td>• Cisco IPICS server</td>
<td>Administration</td>
<td>TCP</td>
</tr>
<tr>
<td>1196</td>
<td>• Cisco IPICS server</td>
<td>Dial engine heartbeat</td>
<td>TCP</td>
</tr>
<tr>
<td>2224</td>
<td>• Cisco IPICS server</td>
<td>UMS heartbeat</td>
<td>UDP</td>
</tr>
<tr>
<td>2225</td>
<td>• Radio control service</td>
<td>UMS radio control service</td>
<td>UDP</td>
</tr>
<tr>
<td>3444</td>
<td>• UMS</td>
<td>Remote Cisco IPICS server heartbeat</td>
<td>TCP</td>
</tr>
<tr>
<td>3446</td>
<td>• UMS</td>
<td>UMS monitor</td>
<td>UDP</td>
</tr>
<tr>
<td>3447</td>
<td>• UMS</td>
<td>Dial engine monitor</td>
<td>UDP</td>
</tr>
<tr>
<td>3448</td>
<td>• UMS</td>
<td>Radio control service</td>
<td>UDP</td>
</tr>
</tbody>
</table>
### Table 2-2 Port Usage (continued)

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Where Used</th>
<th>Function</th>
<th>Transport Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>4100</td>
<td>Cisco IPICS server</td>
<td>Radio control service</td>
<td>TCP and UDP</td>
</tr>
<tr>
<td>5060</td>
<td>Cisco IPICS server</td>
<td></td>
<td>TCP and UDP</td>
</tr>
<tr>
<td></td>
<td>Mobile client</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>UMS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5061</td>
<td>Cisco IPICS server</td>
<td>SIP</td>
<td>TCP and UDP</td>
</tr>
<tr>
<td></td>
<td>Mobile client</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>UMS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5062</td>
<td>UMS</td>
<td>UMS WebSocket SIP connector</td>
<td>TCP and UDP</td>
</tr>
<tr>
<td>5555</td>
<td>Cisco IPICS server</td>
<td>HTTPS to UMS</td>
<td>TCP and UDP</td>
</tr>
<tr>
<td></td>
<td>Mobile client</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>UMS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6294</td>
<td>Cisco IPICS server</td>
<td>Dial engine</td>
<td>TCP and UDP</td>
</tr>
<tr>
<td>8080</td>
<td>Cisco IPICS server</td>
<td>HTTP to UMS</td>
<td>TCP and UDP</td>
</tr>
<tr>
<td></td>
<td>Mobile client</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>UMS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8443</td>
<td>Tomcat</td>
<td>HTTPS redirect</td>
<td>TCP and UDP</td>
</tr>
<tr>
<td>11099</td>
<td>Cisco IPICS server</td>
<td>Policy engine</td>
<td>TCP and UDP</td>
</tr>
<tr>
<td>20000</td>
<td>Cisco IPICS server</td>
<td>Media engine</td>
<td>TCP and UDP</td>
</tr>
<tr>
<td></td>
<td>Mobile client</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>UMS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>32778</td>
<td>Cisco IPICS server</td>
<td>Remote heartbeat receiver</td>
<td>TCP and UDP</td>
</tr>
<tr>
<td></td>
<td>Mobile client</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>UMS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16384 through 20480</td>
<td>Mobile client</td>
<td>Media mixer</td>
<td>TCP and UDP</td>
</tr>
<tr>
<td>21000, 21001</td>
<td>Cisco IPICS server</td>
<td>RTP / RTCP multicast</td>
<td>TCP and UDP</td>
</tr>
<tr>
<td></td>
<td>Mobile client</td>
<td></td>
<td></td>
</tr>
<tr>
<td>25000 through 29096</td>
<td>Cisco IPICS server</td>
<td>TGMS (restreamer)</td>
<td>TCP and UDP</td>
</tr>
<tr>
<td></td>
<td>Mobile client</td>
<td></td>
<td></td>
</tr>
<tr>
<td>35000 through 39096</td>
<td>Cisco IPICS server</td>
<td>Dial Media Service (DMS)</td>
<td>TCP and UDP</td>
</tr>
<tr>
<td></td>
<td>Mobile client</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4000 through 20480</td>
<td>Mobile client</td>
<td>RTP/RTCP, SRTP</td>
<td>TCP and UDP</td>
</tr>
<tr>
<td>8005, 8443</td>
<td>Cisco IPICS server</td>
<td>Tomcat</td>
<td>TCP and UDP</td>
</tr>
<tr>
<td></td>
<td>Mobile client</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Cisco IPICS UMS

A Cisco IPICS deployment includes or more Cisco Unified Communications Server (UCS) components that host virtual instances of the Unified Media Service (UMS).

For information about UMS system requirements and capacity, see *Cisco IPICS Compatibility Matrix*. For information about the ports and transport protocols that the UMS uses, see Table 2-2 on page 2-24.

This chapter includes these topics:

- UMS Overview, page 3-1
- When is a UMS Required?, page 3-2
- UMS Instances for Locations, page 3-2
- UMS Scaling, page 3-3
- UMS Resource Allocation, page 3-3
- Remote Users, page 3-4
- UMS Audio Mixing, page 3-4

**UMS Overview**

The UMS is a highly available, software-based media engine that performs several core functions in a Cisco IPICS deployment including:

- Media transcoding between G.711 and G.729 media streams
- Media stream mixing and floor control
- Talker ID for P25 and SIP based endpoints
- SIP termination
- SIP to multicast, SIP to SIP, multicast to SIP, and multicast to multicast media connectivity
- Floor control for mobile clients and Cisco Unified IP Phone clients

*Figure 3-1* illustrates the use of a UMS in a Cisco IPICS deployment.
When is a UMS Required?

A UMS is required for any Cisco IPICS deployment in which unicast and multicast endpoints are joined or channels are combined.

Examples include:

- Using VTGs
- Using Cisco IPICS incidents
- Having dial-in users

Dial-in users joining VTGs or channels

UMS Instances for Locations

Cisco IPICS relies upon the concept of resource *locations* to effectively manage network traffic. A location is a multicast enabled domain within a network. A domain can comprise multiple geographic locations. Some networks may be fully multicast enabled across the entire network while others may not route multicast traffic beyond a geographic boundary or a single subnet. Cisco IPICS considers each separate multicast domain to be a different location. Any resources (channels, radios, endpoints, and so on) that are not in the same multicast domain as the Cisco IPICS server are considered to be in the *Remote* location.
A UMS is assigned to a location when it is configured. All IPICS servers and components that are in the same multicast domain should be assigned to the same location. While a single IPICS server can administer UMS resources in multiple locations, multicast media is confined to its originating location. Media can move between locations via a Multicast–Unicast–Multicast (MUM) trunk configured on a T1 or E1 loopback or via a GRE tunnel. Only baseband audio data is carried across the MUM trunk; talker ID, control data and supplemental services are not distributed between locations.

The following guidelines apply to locations:

- A channel is associated to a location
- A VTG is a global resource and can be used to span a channel to another channel in another location
- Cisco Mobile Client users are always considered to be remote

**UMS Scaling**

Each instance of the UMS supports up to 100 simultaneous audio streams. A Cisco IPICS deployment can be scaled to support many hundreds of users by adding UMS resources. The number of UMS resources that are required is the based on sum of the streams. Cisco The IPICS server maintains a list of available UMSs and locations and distributes media streams on a round-robin basis.

Clients consume resources differently; the UMS sends one audio stream to a registered mobile client regardless of how many channels are displayed on the client. When deploying Cisco IPICS to support more than 1,000 simultaneous audio streams, server and media streams must be distributed across multiple physical servers. Additional virtual cores and memory may be required for optimized performance. Consult your Cisco representative for assistance with large scale installations.

**UMS Resource Allocation**

UMS resources are dynamically allocated in the following situations:

- Activating or deactivating a VTG—When a VTG is activated by a Cisco IPICS user or triggered by a Cisco IPICS policy, one UMS resource is allocated for each channel in the VTG. The UMS resource is released when the user deactivates the VTG.

- Activating or changing an incident—An incident is a special case of a VTG in which media other than voice can be associated with an event. Each channel or VTG in an incident consumes one UMS resource.

- Authenticating a mobile client—Mobile clients connect to Cisco IPICS via a SIP session between the client and the UMS, which consumes one UMS resource.

- Authenticating a Cisco video surveillance IP camera—Cisco video surveillance cameras that run the SIP client create a SIP session between the camera and the UMS, which consumes one UMS resource.

- A dial-in user joining a channel or VTG—Each Channel or VTG that the Cisco IPICS dial engine accesses consumes one UMS resource. (This UMS resource can service multiple users simultaneously.)
Remote Users

A Cisco IPICS mobile client user is, by definition, a remote user. A remote user accesses Cisco IPICS through a SIP-based (unicast) connection and obtains a media connection to the Cisco IPICS server. When the user joins a channel or VTG, Cisco IPICS configures a resource on the UMS to enable a multicast connection from the UMS to the user.

This multicast connection is made one time for a channel or VTG, regardless of the number of users who select the channel or VTG. When the last remote user disconnects from the channel or VTG, the resource is released in the UMS and becomes available.

When a remote user obtains a media connection on the Cisco IPICS server, the UMS sends and receives multicast streams as follows:

1. After the user selects a resource, Cisco IPICS allocates a UMS resource for the user and allocates a multicast address from the multicast pool. Cisco IPICS then performs an IGMP join operation on the multicast address so that when additional users select the same resource, the Cisco IPICS server can continue to use same the multicast address.

2. When the user begins to talk, Cisco IPICS transmits the audio to the multicast address of the selected resources.

3. When the UMS receives the multicast packets, it forwards the packets to the multicast address that has been allocated from the multicast pool. Cisco IPICS receives that multicast audio stream and forwards it as a unicast stream to all remote users who have selected that resource.

UMS Audio Mixing

The UMS uses a communications system called Hoot ‘n’ Holler (or hootie) in which the three most recent talkers are mixed into one multicast output stream. The UMS provides “always on” multi-user conferences. The UMS version of Hoot ‘n’ Holler is based on the hardware implementation of audio mixing that available in Cisco devices that run UN-enabled versions of Cisco IOS.

In the Cisco Hoot ‘n’ Holler over IP implementation, all participants in a VTG can speak simultaneously, However, when voice packets from various sources arrive at the UMS, the arbitration algorithm selects only the three most active voice streams and mixes them. If other voice streams are present, the UMS drops the longest talker by using a round-robin arbitration algorithm. See Figure 3-2.

Figure 3-2 Mixing Voice Streams

Table 3-1 shows an example of how mixing works in a VTG that has four active users on a channel.
### Table 3-1 Mixing Example

<table>
<thead>
<tr>
<th>Event</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>User A starts speaking.</td>
<td>1 user speaking.</td>
</tr>
<tr>
<td>User B and User C join User A.</td>
<td>3 users speaking simultaneously. Cisco arbitration engine at the UMS receives 3 voice streams.</td>
</tr>
<tr>
<td>User D starts speaking while the other 3 users continue speaking.</td>
<td>Cisco arbitration engine at the UMS receives 4 voice streams. The algorithm can present up to 3 voice streams. It drops the voice stream from the longest talker, User A, and adds User D to the streams that it presents. The voice streams are now from User B, User C, and User D.</td>
</tr>
<tr>
<td>After 2 seconds, all 4 users are still speaking.</td>
<td>The current longest talker, User B, is dropped, and User A is added. Voice streams are now User C, User D, and User A.</td>
</tr>
<tr>
<td>After 2 seconds, all 4 users are still speaking.</td>
<td>The current longest talker, User C, is dropped, and User A is added. Voice streams are now User D, User A, and User B.</td>
</tr>
<tr>
<td>All users continue speaking.</td>
<td>The round-robin process of dropping the current longest talker and adding the other user every 2 seconds continues.</td>
</tr>
</tbody>
</table>
UMS Audio Mixing

Chapter 3      Cisco IPICS UMS

Solution Reference Network Design (SRND) for Cisco IPICS Release 4.7
Cisco IPICS LMR Gateway Configurations

This chapter provides an overview of how to install and configure a land mobile radio (LMR) gateway to interface to audio devices. These audio devices typically consist of radios.

The Cisco Hoot ‘n’ Holler feature is used to enable land mobile radios (LMRs) in a Cisco IPICS solution. An LMR is integrated by providing an ear and mouth (E&M) interface to an LMR or to other PTT devices, such as Sprint and Nextel phones. This interface is in the form of a voice port that is configured to provide an appropriate electrical interface to the radio. The voice port is configured with a connection trunk entry that corresponds to a VoIP dial peer, which in turn associates the connection to a multicast address. You can configure a corresponding channel in Cisco IPICS, using the same multicast address, which enables Cisco IPICS to provide communication paths between the desired endpoints.

For information about Cisco Land Mobile Radio (LMR) over IP, refer to the documentation at the following URLs:


This chapter includes these topics:

- Interfacing the Cisco IPICS LMR Gateway with Land Mobile Radios, page 4-1
- Cisco IOS LMR Gateway Configurations, page 4-6
- Analog Tap Recording Configuration, page 4-11

Interfacing the Cisco IPICS LMR Gateway with Land Mobile Radios

Audio connections between the radio and Cisco IPICS solution is accomplished by using a software feature license with Cisco E&M interface cards. (These cards have been used for years to interface telephone switching equipment and Cisco routers.) The combination of the feature license and the E&M card creates an LMR gateway.

Figure 4-1 shows a VIC2 or VIC3 -2E&M card.
This section describes how to determine the proper cable to use when connecting a device to E&M card.

The LMR signaling enhancements in Cisco IOS software apply to the analog E&M interface for LMR signaling only. For a description of how the leads on the analog E&M interface are implemented on Cisco IOS voice gateways, Cisco recommends that you review *Understanding and Troubleshooting Analog E&M Interface Types and Wiring Arrangements* before proceeding further. This document is available at this URL:


LMR cable building requires an understanding of the radio. Some equipment requires components in the cable, such as resistors, capacitors, inductors, or inverters. It is important that you understand the LMR side of the cable and which signals are expected to and from the LMR before connecting it to the E&M port on the router.

An LMR gateway is configured to support 2-wire or 4-wire audio. The audio and control signals enter and exit the E&M port via an RJ-45 jack on the E&M card. The simplest cable is a standard Category 5 Ethernet cable on which one end is unterminated. Stripping back the wire jacket exposes four pairs of wires:

- The blue pair of wires (Tip-1 and Ring-1) maps to pins 4 and 5 on the RJ-45 plug of the E&M card. In a 4-wire operation, this pair of wires carries the outbound audio from the gateway card. The leads are transformer-isolated with an impedance of 600 ohms across each pair, providing a 600 ohm transformer coupled audio appearance to radios. These leads typically connect to a microphone jack or pin on an LMR. In two-wire operation, the Tip-1 and Ring-1 leads carry the full-duplex audio.

- The green pair of wires (Tip and Ring) maps to pins 3 and 6 on the RJ-45 plug of the E&M card. In 4-wire operation, this pair of wires carries the inbound audio to the gateway card. The leads are transformer-isolated with an impedance of 600 ohms across each pair, providing a 600 ohm transformer coupled audio appearance to radios. These leads typically connect to a speaker jack or pin on an LMR. In two-wire operation, the Tip and Ring leads are not used.

- The brown pair of wires maps to pins 7 and 8 on the RJ-45 plug of the E&M card. This pair of wires is used to signal PTT to the LMR. In E&M type II and III, signaling polarity must be observed: pin 8 maps to Signal Ground (SG) and pin 7 maps to the “E” lead, which also is the PTT connection of the LMR.

![Figure 4-1 VIC2 or VIC3 -2E&M](image-url)
The orange pair of wires maps to pins 1 and 2 on the RJ-45 plug of the E&M card. This pair of wires is optional and used only if the LMR provides signaling for Carrier Operated Relay (COR) or Carrier Operated Squelch (COS) functionality. If the LMR does not provide COR/COS output signals, this pair of wires is not used. In E&M type II and III signaling, polarity must be observed: pin 1 maps to Battery Voltage (SB) and pin 2 maps to the “M” lead.

Figure 4-2 shows the sequential pin orientation on a standard RJ-45 connector.

![Figure 4-2 RJ-45 Pinout](image)

Table 4-1 shows the pin orientation of a standard RJ-45 connector.

<table>
<thead>
<tr>
<th>Router RJ-45 Pin No.</th>
<th>Router Function</th>
<th>Category 5 Color Code</th>
<th>Radio Connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Signal Battery (SB)</td>
<td>Orange</td>
<td>Signal Battery (SB)</td>
</tr>
<tr>
<td>2</td>
<td>M-Lead</td>
<td>White/Orange</td>
<td>COR/COS</td>
</tr>
<tr>
<td>3</td>
<td>Ring</td>
<td>White/Green</td>
<td>Speaker +</td>
</tr>
<tr>
<td>4</td>
<td>Ring-1</td>
<td>Blue</td>
<td>Microphone –</td>
</tr>
<tr>
<td>5</td>
<td>Tip-1</td>
<td>White/Blue</td>
<td>Microphone +</td>
</tr>
<tr>
<td>6</td>
<td>Tip</td>
<td>Green</td>
<td>Speaker –</td>
</tr>
<tr>
<td>7</td>
<td>E-Lead</td>
<td>White/Brown</td>
<td>PTT</td>
</tr>
<tr>
<td>8</td>
<td>Signal Ground (SG)</td>
<td>Brown</td>
<td>Ground</td>
</tr>
</tbody>
</table>

**Analog E&M Interface**

For analog connections, the E&M interface card is used to attach leads from an LMR device to the gateway. Only the E&M interfaces can accommodate the many different audio and signaling configurations in the wide variety of radio systems. The E&M port can be configured to transmit and receive audio information by using one pair or two pairs of leads. It also has four configurations for control of the signaling leads. Some radio systems may present an E&M interface for their wire-side connections, which simplifies the connection process. However, many systems require planning for their connection.
Analog E&M signaling Types

Cisco LMR routers support Type II, Type III, and Type V E&M signaling. With each signaling type, the router supplies one signal, known as the M (for Mouth) signal, and accepts one signal, known as the E (for Ear) signal. Conversely, the LMR equipment accepts the M signal from the router and provides the E signal to the router. The M signal that is accepted by the LMR equipment at one end of a circuit becomes the E signal that is output by the remote LMR interface.

When configuring a voice port, you must select the E&M interface type that is matched to the connected device.

Type II indicates the following lead configuration:
- E—Output, relay to SG
- M—Input, referenced to ground
- SB—Feed for M, connected to –48V
- SG—Return for E, galvanically isolated from ground

Figure 4-3 shows the lead designations and functions for the Type II E&M interface.

![E&M Type II Interface Diagram](image-url)
Type III indicates the following lead configuration:
- E—Output, relay to ground
- M—Input, referenced to –48V
- SB—Connected to –48V
- SG—Connected to ground

Figure 4-4 shows the lead designations and functions for the Type III E&M interface.

![Figure 4-4 E&M Type III Interface](image)

Type V indicates the following lead configuration:
- E—Output, relay to ground
- M—Input, referenced to –48V

Figure 4-5 shows the lead designations and functions for the Type V E&M interface.
Cisco IOS LMR Gateway Configurations

This section describes the Cisco IOS configurations that are used for different types of radios. An LMR port must have a configuration that is similar to what is described in this section.

This section includes these topics:

- Determining Correct Cisco IOS Radio Control, page 4-6
- Required Baseline LMR Gateway Configuration, page 4-7
- VAD Operated Signaling Configuration, page 4-8
- COR/COS Operated Signaling Configuration, page 4-10

Determining Correct Cisco IOS Radio Control

Router configuration and connections typically are determined by the capabilities of the radio to be interfaced. There are three basic types of Cisco IOS radio control configurations. Use the router configuration that best matches your situation.
VAD Operated Signaling—Typically used when the radio device does not provide COR/COS signaling. Without the COR/COS signaling interface from the radio device, the router uses the voice activation detection (VAD) function within Cisco IOS to determine when a signal is being received from the radio device and to begin sending VoIP packets on the designated multicast address. Typically, this option is used when a portable radio device is the endpoint because these devices do not normally provide signaling for COR/COS.

COR/COS Signaling—Should be used when a radio device has the ability to provide COR/COS signaling. In this situation, the router begins sending VoIP packets on the assigned multicast address when this line is activated by the radio device. Typically, this approach provides the most reliable audio reception and eliminates the clipping at the beginning of a conversation that may occur when the VAD Operated Signaling function is employed.

Required Baseline LMR Gateway Configuration

The following baseline Cisco IOS configuration commands are required regardless of the signaling that is implemented:

```plaintext
voice service voip
ip address trusted list
ipv4 0.0.0.0 0.0.0.0
allow-connections h323 to h323
allow-connections sip to h323
allow-connections sip to sip
fax protocol cisco
h323
sip
bind control source-interface Loopback0
bind media source-interface Loopback0!
ip multicast-routing
voice class codec 1
codec preference 1 g729r8
codec preference 2 g711ulaw
!
interface Loopback0
ip address 192.168.4.6 255.255.255.255
ip pim sparse-dense-mode
!
interface Vif1
ip address 192.168.3.5 255.255.255.252
ip pim sparse-dense-mode
duplex auto
speed auto
!
ip pim rp-address 192.168.1.1 bi-dir
ip rtcp report interval 5001
!
gateway
timer receive-rtcp 5
timer receive-rtp 1200
```
### VAD Operated Signaling Configuration

You must issue the `lmr m-lead inactive` command for VAD Operated Signaling. When this configuration is used, the router ignores signals that are sent by voice on the M-lead. The flow of voice packets is determined by VAD. Typically, six of the eight wires are employed.

Table 4-2 shows the wiring connections that are used when interfacing to a VAD-operated radio.

**Table 4-2 VAD Physical LMR Connections**

<table>
<thead>
<tr>
<th>Router RJ-45 Pin No.</th>
<th>Router Function</th>
<th>Category 5 Color Code</th>
<th>Radio Connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Signal Battery (SB)</td>
<td>Orange</td>
<td>Not Connected</td>
</tr>
<tr>
<td>2</td>
<td>M-Lead</td>
<td>White/Orange</td>
<td>Not Connected</td>
</tr>
<tr>
<td>3</td>
<td>Ring</td>
<td>White/Green</td>
<td>Speaker +</td>
</tr>
<tr>
<td>4</td>
<td>Ring-1</td>
<td>Blue</td>
<td>Microphone –</td>
</tr>
<tr>
<td>5</td>
<td>Tip-1</td>
<td>White/Blue</td>
<td>Microphone +</td>
</tr>
<tr>
<td>6</td>
<td>Tip</td>
<td>Green</td>
<td>Speaker –</td>
</tr>
<tr>
<td>7</td>
<td>E-Lead</td>
<td>White/Brown</td>
<td>PTT</td>
</tr>
<tr>
<td>8</td>
<td>Signal Ground (SG)</td>
<td>Brown</td>
<td>Ground</td>
</tr>
</tbody>
</table>

1. Does not apply to this configuration.

Cisco VAD has two layers: application programming interface (API) layer and processing layer. There are three states into which the processing layer classifies incoming signals:

- speech
- unknown
- silence

The state of the incoming signals is determined by the noise threshold, which can be configured with the `threshold noise` command.

If the incoming signal cannot be classified, the variable thresholds that are computed with the speech and noise statistics that VAD gathers are used to make a determination. If the signal still cannot be classified, it is marked as unknown. The final VAD qualification is made by the API. In some scenarios, the audio that is classified as unknown can create unwanted voice packet traffic, which can consume extra bandwidth. The sound quality of the connection is slightly degraded with VAD, but the connection takes much less bandwidth.

**VAD Command States**

The following VAD command states are possible:

- Silence State—If the voice level is below the noise threshold, the signal is classified as silence and no VoIP packets are sent over the network
- Speech/Unknown States—Signals classified as Speech and Unknown are sent over the network as VoIP packets

**VAD Aggressive Command States**

When the aggressive keyword is used with the `vad` command in dial peer configuration mode, the VAD noise threshold is reduced from –78 to –62 dBm. Noise that falls below the –62 dBm threshold is considered to be silence and is not sent over the network.
• Silence / Unknown States—If the voice level is below the noise threshold, the signal is classified as silence and no VoIP packets are sent. Additionally, unknown packets are considered to be silence and are discarded when the aggressive keyword is used.

• Speech State—Only the incoming signal that is classified as speech causes packets to be sent over the network.

The following shows a sample configuration for an LMR voice port that is configured for VAD operated signaling.

In this example, type \{ 2 | 3 | 5 \} typically is type 3, but see Figure 4-3 on page 4-4, Figure 4-4 on page 4-5, and Figure 4-5 on page 4-6 to select the type that best matches your radio requirements. Input gain \{ -27 - 16 \} typically is 10, but adjust this value as needed to best receive audio on Cisco IPICS endpoints. Output attenuation \{ -16 - 27 \} typically is 10, but adjust this value as needed to best receive audio on radios. When connecting a radio to a voice port in an LMR gateway, you may need to make adjustments to properly balance the audio levels. A radio typically provides gain adjustments, and the level of the signal from the radio to the voice port and the level of the signal from the voice port to the radio may require some adjustments on the radio and the voice port. When using a tone controlled radio, it is important to note that the tones that are sent from the LMR gateway to the radio also are affected by the voice ports output attenuation settings. When optimizing these settings to achieve the desired audio levels, take care to ensure that the voice port adjustments do not have an adverse effect on the level and quality of the tone signals.

```conf
voice class permanent 1
signal timing oos timeout disabled
signal keepalive disabled
signal sequence oos no-action
!
voice-port 0/2/1
voice-class permanent 1
auto-cut-through
operation 4-wire
type \{ 2 | 3 | 5 \}
signal lmr
lmr e-lead voice
bootup e-lead off
lmr duplex half
lmr led-on
input gain \{ -27 - 16 \}
output attenuation \{ -16 - 27 \}
no echo-cancel enable
no comfort-noise
timeouts call-disconnect 3
timeouts wait-release 3
timing hookflash-in 10
timing hangover 80
timing delay-voice tdm 40
connection trunk 102
description VAD Operated Voice Port
threshold noise -40
!
dial-peer voice 102 voip
destination-pattern 102
session protocol multicast
session target ipv4:239.193.1.2:21000
codec g711ulaw
vad aggressive
```
COR/COS Operated Signaling Configuration

When the COR/COS operated signaling configuration is used, the router employs signals that are sent by voice on the M-lead pin 2. The M-lead corresponds to the COR/COS of the radio system, which indicates receive activity on the radio system. The `lmr m-lead audio-gate-in` command configures the voice port to generate VoIP packets only when a seize signal is detected on the M-Lead. The router stops generating VoIP packets when the seize signal is removed from the M-lead. It is important to understand that even if there is audio on pins 3 and 6 coming from the radio, the router begins to send VoIP packets on the assigned multicast address only if the signal on pin 2 has become active. Typically all eight wires are employed.

Table 4-3 shows the wiring connections that are used when interfacing to a COR/COS operated radio.

<table>
<thead>
<tr>
<th>Router RJ-45 Pin No.</th>
<th>Router Function</th>
<th>Category 5 Color Code</th>
<th>Radio Connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Signal Battery (SB)</td>
<td>Orange</td>
<td>Signal Battery (SB)</td>
</tr>
<tr>
<td>2</td>
<td>M-Lead</td>
<td>White/Orange</td>
<td>COR/COS</td>
</tr>
<tr>
<td>3</td>
<td>Ring</td>
<td>White/Green</td>
<td>Speaker +</td>
</tr>
<tr>
<td>4</td>
<td>Ring-1</td>
<td>Blue</td>
<td>Microphone –</td>
</tr>
<tr>
<td>5</td>
<td>Tip</td>
<td>White/Blue</td>
<td>Microphone +</td>
</tr>
<tr>
<td>6</td>
<td>Tip</td>
<td>Green</td>
<td>Speaker –</td>
</tr>
<tr>
<td>7</td>
<td>E-Lead</td>
<td>White/Brown</td>
<td>PTT</td>
</tr>
<tr>
<td>8</td>
<td>Signal Ground (SG)</td>
<td>Brown</td>
<td>Ground</td>
</tr>
</tbody>
</table>

The following shows a sample configuration for an LMR voice port that is configured for COR/COS operated signaling.

```
voice class permanent 1
signal timing oos timeout disabled
signal keepalive disabled
signal sequence oos n4o-action

voice-port 0/2/0
voice-class permanent 1
auto-cut-through
operation 4-wire
type { 2 | 3 | 5 }
signal lmr

lmr m-lead audio-gate-in ! RX audio IP packets only sent when this lead is active.
```
Analog Tap Recording Configuration

The following sections provide information about recording multicast LMR traffic:

- Recording Multicast LMR Traffic, page 4-12
- Recording Tap Cisco IOS Configuration, page 4-12

DSP Channel Optimization and Allocation

Follow these recommendations for optimizing DS0 channels and DSP channels:

- So that digital signal processors (DSPs) can be shared, first enable dspfarm, and make sure that all modules are participating in the network clock.

- When you enable dspfarm, you add specific voice cards to the DSP resource pool. This configuration allows several interface cards to share the installed DSP resources. (DSPs can be shared among digital modules or ports (such as T1/E1) and the motherboard, but DSPs cannot be shared among analog ports (such as an FXS)).

- At a minimum, you should enable one dspfarm.

- After the dspfarm is enabled on all modules that have DSPs installed, and all modules are participating in the main network clock, Cisco IOS interacts with these DSPs as part of the DSP resource pool.

To help calculate the DSPs that you need for your configuration, refer to High-Density Packet Voice Digital Signal Processor Modules, which is available at the following URL:


For detailed information about configuring DSP farms, refer to the “Configuring the Cisco IPICS RMS Component” appendix in Cisco IPICS Server Administration Guide, Release 4.0(2).
Recording Multicast LMR Traffic

Recording the traffic of radios that are connected to the Cisco IPICS network can be accomplished with readily available third-party recording solutions.

The “Recording Tap Cisco IOS Configuration” section on page 4-12 explains how to configure an E&M port that is dedicated to providing an analog audio output to an external recording device. Typically, each radio channel should be recorded on its own recording track so that when the recording plays back, the end user hears only the radio traffic for the channel that was selected. If that radio channel was a member of a Cisco IPICS virtual talk group, the audio from all the members of that talk group would also be heard. To accomplish this type of channel-only recording, an E&M port is required for each radio channel that needs to be recorded. For example, if there are four radios, each connected to its own E&M port as the interface to the Cisco IPICS network, an additional four E&M ports are required if each channel needs to be recorded. In this case, eight E&M ports are required. If the recording device is in a location other than the radios, it may require a dedicated ISR to provide the analog taps for the recording device.

Recording Tap Cisco IOS Configuration

When the configuration that is described in this section is used, the router captures the multicast traffic for a particular channel and converts it to an analog signal that can be sent to a recording device. If the recorder requires a signal to indicate when to start recording, the E-lead pin 7 can be employed. The E-lead corresponds to the PTT signal of the radio system, which indicates audio activity on the LMR system. If the recording device is continuous or triggered by the presence of audio, only pins 4 and 5 should be required. Typically four of the eight wires are employed.

Table 4-4 shows the configuration for four of the eight wires.

Table 4-4 Physical Connections For Recording Device

<table>
<thead>
<tr>
<th>Router RJ-45 Pin No.</th>
<th>Router Function</th>
<th>Category 5 Color Code</th>
<th>Router Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Signal Battery (SB)</td>
<td>Orange</td>
<td>No Connection</td>
</tr>
<tr>
<td>2</td>
<td>M-Lead</td>
<td>White/Orange</td>
<td>No Connection</td>
</tr>
<tr>
<td>3</td>
<td>Ring</td>
<td>White/Green</td>
<td>No Connection</td>
</tr>
<tr>
<td>4</td>
<td>Ring-1</td>
<td>Blue</td>
<td>TX &amp; RX Audio</td>
</tr>
<tr>
<td>5</td>
<td>Tip-1</td>
<td>White/Blue</td>
<td>TX &amp; RX Audio</td>
</tr>
<tr>
<td>6</td>
<td>Tip</td>
<td>Green</td>
<td>No Connection</td>
</tr>
<tr>
<td>7</td>
<td>E-Lead</td>
<td>White/Brown</td>
<td>Start Recording</td>
</tr>
<tr>
<td>8</td>
<td>Signal Ground (SG)</td>
<td>Brown</td>
<td>Ground</td>
</tr>
</tbody>
</table>

1. Not used in this configuration.

The following example shows the E&M Voice-Port & Dial Peer configurations that are required for recording multicast traffic on an analog recording device.

In this example, type \{ 2 | 3 | 5 \} typically is type 3, but see Figure 4-3 on page 4-4, Figure 4-4 on page 4-5, and Figure 4-5 on page 4-6 to select the type that best matches your radio requirements. Input gain \{-27 - 16\} typically is 10, but adjust this value as needed to best receive audio on Cisco IPICS endpoints. Output attenuation \{-16 - 27\} typically is 10, but adjust this value as needed to best receive audio on radios. When connecting a radio to a voice port in an LMR gateway, you may need to make
adjustments to properly balance the audio levels. A radio typically provides gain adjustments, and the level of the signal from the radio to the voice port and the level of the signal from the voice port to the radio may require some adjustments on the radio and the voice port. When using a tone controlled radio, it is important to note that the tones that are sent from the LMR gateway to the radio also are affected by the voice ports output attenuation settings. When optimizing these settings to achieve the desired audio levels, take care to ensure that the voice port adjustments do not have an adverse effect on the level and quality of the tone signals.

```
ip multicast-routing
!
voice class codec 1
codec preference 1 g729r8
codec preference 2 g711ulaw
!
voice class permanent 1
signal timing oos timeout disabled
signal keepalive disabled
signal sequence oos no-action
!
voice-port 0/2/0
voice-class permanent 1
auto-cut-through
operation 4-wire
type { 2 | 3 | 5 }
signal lmr
  lmr m-lead audio-gate-in
  lmr e-lead voice
  bootup e-lead off
  lmr duplex half
  lmr led-on
  output attenuation { -16 - 27 }
  no echo-cancel enable
  no comfort-noise
  timeouts call-disconnect 3
  timeouts wait-release 3
  timing hookflash-in 10
  timing hangover 80
  connection trunk 11101
  description Recording Tap Radio 0/2/0
  threshold noise -40
!
dial-peer voice 11101 voip
destination-pattern 11101
session protocol multicast
session target ipv4: { Multicast address of radio channel to be recorded }
  codec g711ulaw
  vad aggressive
```
Chapter 4 Cisco IPICS LMR Gateway Configurations

Analog Tap Recording Configuration
Cisco IPICS Infrastructure Considerations

This chapter contains information about infrastructure issues that you must be aware of when you deploy Cisco IPICS.

For related information, refer to the following documents:

- IP multicast—Refer to *Cisco IOS IP Multicast Configuration Guide, Release 12.4*:
  

- Quality of Service—Refer to *Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.4*:
  

- Voice Configuration—Refer to *Cisco IOS Voice Configuration Library*:
  

- Hoot ‘n’ Holler—Refer to *Hoot ‘n’ Holler Solution*:
  

This chapter includes these topics:

- WAN Considerations, page 5-2
- Multicast Routing
- Bandwidth Planning
- Quality of Service, page 5-8
- VPN in Deployment Scenarios, page 5-23
- Port Utilization, page 5-23
- Securing the Cisco IPICS Infrastructure, page 5-25
- Cisco IPICS Network Management System, page 5-26
WAN Considerations

To ensure the successful deployment of Cisco IPICS over a WAN, you must carefully plan, design, and implement the WAN. Make sure to consider the following factors:

- **Delay**—Propagation delay between two sites introduces 6 microseconds per kilometer. Other network delays may also be present.

- **Quality of Service**—The network infrastructure relies on QoS engineering to provide consistent and predictable end-to-end levels of service for traffic. QoS-enabled bandwidth must be engineered into the network infrastructure.

- **Jitter**—Varying delay that packets incur through the network as a result of processing, queue, buffer, congestion, or path variation delay. Jitter for the multicast voice traffic must be minimized by using Quality of Service (QoS) features. For related information, see the “Quality of Service” section on page 5-8.

- **Packet loss and errors**—The network should be engineered to provide sufficient prioritized bandwidth for all voice traffic. Standard QoS mechanisms must be implemented to avoid congestion and packet loss. For related information, see the “Quality of Service” section on page 5-8.

- **Bandwidth**—Provision the correct amount of bandwidth between each site for the expected call volume. This bandwidth is in addition to bandwidth for other applications and traffic that share the network. The provisioned bandwidth must have QoS enabled to provide prioritization and scheduling for the different classes of traffic. In general, the bandwidth should be over-provisioned and under-subscribed.

Multicast Routing

Cisco supports the Protocol Independent Multicast (PIM) routing protocol for both sparse mode (SM) and dense mode (DM). However, because of its periodic broadcast and prune mechanism, DM PIM is not recommended for production networks.

Cisco recommends using bidirectional PIM for Cisco IPICS. Bidirectional PIM is an extension of the PIM suite of protocols that implements shared sparse trees with bidirectional data flow. In contrast to PIM-sparse mode, bidirectional PIM avoids keeping source-specific states in a router and allows trees to scale to an arbitrary number of sources while requiring only minimal additional overhead.

The shared trees that are created in PIM SM are unidirectional. Therefore, a source tree must be created to bring a data stream to the rendezvous point (RP), which is the root of the shared tree. Then the data can be forwarded down the branches to receivers. In the unidirectional mode, source data cannot flow up the shared tree toward the RP.

In bidirectional mode, traffic is routed only along a bidirectional shared tree that is rooted at the RP for the group. In bidirectional PIM, the IP address of the RP acts as the key to having all routers establish a loop-free spanning tree topology rooted in that IP address. This IP address does not need to be a router. It can be any unassigned IP address on a network that is reachable throughout the PIM domain.

*Figure 5-1* shows a bidirectional shared tree. In this example, data from the source can flow up the shared tree (*, G) toward the RP, and then down the shared tree to the receiver. There is no registration process so source tree (S, G) is created.
Bidirectional PIM is derived from the mechanisms of PIM SM and has many of the same shared tree operations. Bidirectional PIM also has unconditional forwarding of source traffic toward the RP upstream on the shared tree, but no registering process for sources, as provided by PIM SM. These modifications are necessary and sufficient to allow forwarding of traffic to all routers based only on the (*, G) multicast routing entries. Bidirectional PIM eliminates any source-specific state and allows scaling to an arbitrary number of sources.

In a Cisco IPICS deployment, bidirectional PIM solves the problem of scalability in the following ways:

- Forwarding traffic based on the shared tree (*, G)—This functionality helps scale the multicast routing table by creating a single routing entry per channel. In SM, a routing entry is created per group and per source. So, for example, if a channel has 100 participants, it will have 101 multicast routing entries in the routing table. With bidirectional PIM, only a single multicast routing entry in the routing table is created, regardless of the number of participants.

- Basing the Reverse Path Forwarding (RPF) decision on the route to the RP—In SM, RPF decisions about (S, G) entries are based on the source address of the flow, and for bidirectional (*, G), RPF decisions are based on the RP. This functionality eliminates the need to configure hundreds of ip mroute entries to force multicast traffic on the Cisco IPICS Permanent Virtual Circuit (PVC). With bidirection, forcing the multicast traffic on the Cisco IPICS PVC is achieved by tuning the unicast routing protocol to prefer the Cisco IPICS PVC as the best route to reach the RP.

If you are using Auto-RP and a Cisco IOS release earlier than 12.2(7), sparse dense mode is required. If you are using Auto-RP and Cisco IOS release 12.2(7) or later, use the `sparse mode` and `ip pim auto rp listener` commands. Multicast types other than auto-rp can use sparse mode.

---

**Note**

Cisco recommends that static RPs be used in a large deployments. This approach helps with control of the multicast tree and provides a stable and a deterministic path for Cisco IPICS traffic.
To ensure sufficient bandwidth for the operation of Cisco IPICS, consider the following issues as you plan and deploy your network. These issues include:

- Codec used for VoIP—See the “Codecs” section on page 5-4
- The number of voice streams that will be mixed—See the “Mixing Voice Streams” section on page 5-8

In addition, you should consider the guaranteed bandwidth that is available on the VoIP network. Make sure to take into account both LAN and WAN bandwidth, and to consider factors such as Frame Relay, Committed Information Rate (CIR) or Asynchronous Transfer Mode Peak Cell Rate (ATM PCR), Sustained Cell Rate, and burst. For additional information see the “Quality of Service” section on page 5-8.

### Codecs

Cisco IPICS uses either the G.711 or G.729a codec. This section provides the following information about codecs:

- Choosing a Codec, page 5-4
- Calculating Codec Bandwidth Use, page 5-5

The Cisco IPICS policy engine supports only G.711 u-law. If you use the policy engine, you must use this codec.

#### Choosing a Codec

When choosing a codec for Cisco IPICS, consider the issues that are described in Table 5-1.

<table>
<thead>
<tr>
<th></th>
<th>G.711</th>
<th>G.729a</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delay</td>
<td>Total delay is 25 ms less per sample than for G.729a.</td>
<td>Total delay is 25 ms greater per sample than for G.711.</td>
</tr>
<tr>
<td></td>
<td>Transcoding increases delay.</td>
<td>Some Cisco IPICS deployments that use G.729a require additional transcoding to convert the G.729a streams to the G.711 stream for mixing. This additional DSP function increases delay significantly.</td>
</tr>
</tbody>
</table>
Calculating Codec Bandwidth Use

This section explains how to calculate bandwidth use for codecs.

By default, Cisco IOS sends all VoIP traffic (that is, media traffic that uses RTP) at a rate of 50 packets/second. In addition to the voice sample, each packet includes an IP, UDP, and RTP header, which adds 40 bytes to the packet. Layer 2 headers (such as Frame Relay, Point-to-Point Protocol, Ethernet) also add bytes to each packet.

The amount of bandwidth that is consumed by a VoIP call depends on the codec that is used, and can be calculated as follows. Make sure to also add the appropriate number of bytes for the layer 2 header to determine the actual bandwidth that is consumed.

**G.729a (8 KB CS-ACELP)**

50 packets/second

20 ms samples / packet = 20 bytes
AP/UDP/RTP headers/packet = 40 bytes

\[(20 \text{ bytes [payload]} + 40 \text{ bytes [headers]}) \times 50 \text{ packets/second} = 3,000 \text{ bytes} \times 8 \text{ bits} = 24 \text{ kbps}\]

**G.711 (64 KB PCM)**

50 packets/second

20 ms samples / packet = 160 bytes
AP/UDP/RTP headers/packet = 40 bytes

\[(160 \text{ bytes [payload]} + 40 \text{ bytes [headers]}) \times 50 \text{ packets/second} = 10,000 \text{ bytes} \times 8 \text{ bits} = 80 \text{ kbps}\]
Table 5-2 shows sample bandwidth consumption. In this table,

- The examples assume a payload size (bytes) of 20 ms samples per packet with 50 packets per second.
- The value \( n \) is equal to the number of voice streams in a session.
- The encompassed bandwidth includes IP/UDP/RTP headers (40 bytes) in the bandwidth calculation.
- Compressed RTP (cRTP) reduces the IP/UDP/RTP headers to between 2 and 4 bytes per packet. The calculation of compressed bandwidth uses 4 bytes for a compressed IP/UDP/RTP headers per packet.
- Make sure to add the appropriate number of bytes for the layer 2 header to determine the actual bandwidth consumed.

<table>
<thead>
<tr>
<th>Codec</th>
<th>Payload Size (bytes)</th>
<th>Bandwidth/Voice Stream (kbps)</th>
<th>RTCP Bandwidth per Cisco IPICS Session (kbps)</th>
<th>Example: 1 Voice Stream in a Session (kbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Uncompressed</td>
<td>Compressed</td>
<td></td>
</tr>
<tr>
<td>G.729a</td>
<td>20</td>
<td>24</td>
<td>9.6</td>
<td>3.6</td>
</tr>
<tr>
<td>G.711</td>
<td>160</td>
<td>80</td>
<td>65.6</td>
<td>12.0</td>
</tr>
</tbody>
</table>

According to RFC 1889 (RTP: A Transport Protocol for Real-Time Applications), the RTCP traffic for any RTP stream is limited to a maximum of 5% of the voice stream (RTP + RTCP). This limitation applies to the three streams that participate in a Cisco IPICS session. Therefore, the RTCP Bandwidth per Cisco IPICS Session is calculated by multiplying the bandwidth per voice stream by 3 and then multiplying that product by 0.05.

When you design a Cisco IPICS network within a campus network, you should not run into any bandwidth-related issues because IP multicast is used to replicate a voice stream and map it to an IP multicast group, in which UMS resources are not used. When remote users connect over a WAN that is not multicast enabled, the UMS converts a multicast stream to an IP unicast stream, which conserves bandwidth on the WAN. When the IP unicast voice stream arrives, the UMS converts the IP unicast stream to a multicast stream. When the voice streams traverse a WAN, the UMS resources are used.

Note: Each Cisco IPICS dial engine port uses the G.711 codec. Bandwidth calculations must consider the G.711 connectivity between the Cisco IPICS server and connected endpoints.

**cRTP, Variable-Payload Sizes and Aggressive VAD**

There are several methods that you can use to modify the bandwidth consumed by a call. These methods include the following:

- RTP Header Compression, page 5-7
- Adjustable Byte Size of the Voice Payload, page 5-7
- Aggressive Voice Activity Detection, page 5-7
RTP Header Compression

As described in the “Codecs” section on page 5-4, IP/UDP/RTP headers add 40 bytes to each packet. However, a packet header is typically unchanged throughout a call. You can enable cRTP for VoIP calls, which reduces the size of IP/UDP/RTP headers to 2 to 4 bytes per packet.

For detailed information about cRTP, refer to Understanding Compression (Including cRTP) and Quality of Service, which is available at this URL:


Adjustable Byte Size of the Voice Payload

You can control the size of the voice payload that is included in each Cisco IPICS voice packet. To do so, use the bytes parameter in a VoIP dial peer. For example:

dial-peer voice 1 voip
destination-pattern 4085551234
codec g729r8 bytes 40
session protocol multicast
session target ipv4:239.192.1.1:21000

Modifying the number of bytes per packet changes the number of packets that are sent per second. You can calculate the number of packets that are sent per second as shown in these examples:

**G.729a codec, with default 20byte payload/packet**

Codec rate: 8,000 bits/second * 8 bits = 1,000 bytes/second
Sampling interval: 10 ms
Default payload size: 20 bytes/packet (2 samples/packet)
1,000 bytes/sec/20bytes/pkt = 50 packets/sec

**G.729a codec, with 40 bytes defined in VoIP dial-peer**

Codec rate: 8,000 bits/second * 8 bits = 1,000 bytes/second
Sampling interval: 10 ms
Payload size: 40 bytes/packet
1,000 bytes/sec/40 bytes/pkt = 25 packets/sec

---

**Note**
Increasing payload size increases the delay per sample by the same amount. For example, increasing payload size from 20 ms to 40 ms increases the delay per sample by 20 ms.

Aggressive Voice Activity Detection

Voice Activation Detection (VAD) is a mechanism that allows a DSP to dynamically sense pauses in conversation. When such pauses occur, no VoIP packets are sent into the network. VAD can reduce the amount of bandwidth used for a VoIP call by up to 50%.

Although VAD conserves bandwidth in VoIP, it disrupts and marginalizes Cisco IPICS signaling, which is used for LMR and PTT packet streams. Be aware of this issue if you use VAD in a Cisco IPICS deployment.
When configuring LMR gateway ports, VAD should not be used if the radio supports Carrier Operated Relay (COR) or Carrier Operated Squelch (COS). Radios that support COR/COS signaling can provide hardwired signaling to the LMR port to start generating packets. Using COR/COS gating is an efficient way to control the audio input and to avoid the possibility of dropping short burst of voice data that may fall below the VAD activation values.

Each voice port has different environmental noises and different users, which can cause a wide variation in noise and speech levels. Conventional VAD can manage these variations, but it is designed for unicast. Conventional VAD usually prefers over-detection to under-detection, as good voice quality is typically given precedence over bandwidth conservation. But in a multicast environment, over-detection and under-detection are not desirable because they degrade voice quality.

Aggressive VAD can be used in a multicast environment to avoid over-detection. With aggressive VAD, when a DSP detects signals with an unknown signal-to-noise ratio (SNR), the DSP does not transmit any spurious packets. With conventional VAD, when the DSP detects signals with an unknown SNR, the DSP continues to transmit packets, which can cause unwanted traffic to take over all slots that are available for voice streams.

You can enable aggressive VAD by enabling the `vad aggressive` configuration setting under a dial peer as follows:

```
dial-peer voice 10 voip
destination-pattern 111
session protocol multicast
session target ipv4:239.192.1.1:21000
vad aggressive
```

### Mixing Voice Streams

As described in the “Virtual Talk Groups” section on page 2-2, the DSPs in a Cisco IPICS deployment can mix up to three voice streams. However, the DSPs do not perform a summation function. So, for example, if three G.729a streams (24 KB each with headers) are received by a router or gateway, the mixed stream would consume 72 KB bandwidth. Even though each user in a VTG or a channel in the VTG receives a single mixed audio stream, the DSP does not send a single 24 KB stream.

It is important to consider this issue when you plan bandwidth in a Cisco IPICS network. It is especially important when planning WAN bandwidth, which can be more expensive and less available than LAN bandwidth.

Because the Cisco Hoot ‘n’ Holler feature mixes up to three voice streams at a time, you do not need to provision voice bandwidth for more than three times the per-call bandwidth for each WAN site that includes routers with the Cisco Hoot ‘n’ Holler feature.

An audio channel that is mixed through a VTG experiences an additional 60 ms of delay.

### Quality of Service

There are several QoS features that should be enabled so that a Cisco IPICS deployment can deliver toll-quality VoIP QoS. This section provides an overview of these features for Point-to-Point Protocol (PPP) and Frame Relay WAN topologies and for deployments on LAN media.

This section includes these topics:

- QoS Overview, page 5-9
QoS Overview

QoS provides consistent voice latency and minimal packet loss. The following recommendations apply to QoS in campus LAN and WAN environments:

- Classify voice RTP streams as expedited forwarding (EF) or IP precedence 5 and place them into a priority queue on all network elements.
- Classify voice control traffic as assured forwarding 31 (AF31) or IP precedence 3 and place it into a second queue on all network elements.

As you design a VoIP network to deploy real-time applications such as Cisco IPICS, consider the following issues, which can affect voice quality:

- Packet loss—Causes voice clipping and skips. The industry-standard codec algorithms that are used in DSPs can correct for up to 30 ms of lost voice. Cisco VoIP technology uses 20 ms samples of voice payload per VoIP packet. Therefore, for the codec correction algorithms to be effective, only a single packet can be lost during any time. Packet loss can be a significant problem for real-time applications because they are not designed to retransmit packets.

- Delay—Causes either voice quality degradation due to the end-to-end voice latency or packet loss if the delay is variable. If the delay is variable, such as queue delay in bursty data environments, there is a risk of jitter buffer overruns at the receiving end. Longer delays can cause buffer overflow and underflow, and unnatural pauses in human conversations. Because Cisco IPICS supports a PTT service, the typical one-way delay requirement of 150 ms as recommended in the International Telecommunication Union (ITU) G.114 specification does not directly apply. PTT users are aware of radio protocol, so a more reasonable delay is 400 ms as outlined in the ITU G.173 specification.

- Jitter—Variable delay. While some delay is acceptable, delay that constantly changes can cause inconsistent and inefficient DSP buffering. It also can cause inconsistent voice quality.

- Ability to Prioritize VoIP traffic—Involves the use of queuing techniques, such as IP RTP Priority and Low-Latency Queuing, that are available in Cisco IOS.

- Ability to make VoIP traffic best fit the LAN or WAN network—Involves making sure that small VoIP packets do not get delayed behind large data packets (an event called serialization).

If networks are designed and built to provide low delay, limited jitter, and limited packet loss, real-time applications such as Cisco IPICS solution can be successful.
Cisco IOS Queuing Techniques

Cisco IOS provides a wide variety of QoS features. The following features are particularly useful for a Cisco IPICS deployment:

- **IP RTP Priority**, page 5-10
- **Low Latency Queuing**, page 5-10

For more detailed documentation about IP RTP Priority, refer to the “Congestion Management Overview” chapter in *Cisco IOS Quality of Service Solutions Configuration Guide*, which is available at this URL:


**IP RTP Priority**

IP RTP Priority can be applied to point-to-point links and to Frame Relay PVCs. It allows you to provision a fixed amount of bandwidth (in KB) that is always available for Cisco IPICS packets. If there are no Cisco IPICS packets present in the network (that is, nobody is speaking), the bandwidth is available to other data applications. This predefined amount of bandwidth is serviced as a strict priority-queue within the overall structure of Weighted-Fair Queuing (WFQ). The entrance criteria to this priority queue is a range of UDP ports that are used by Cisco IPICS to send IP packets.

Cisco IPICS uses the UDP port that is selected on the VoIP dial peer, and the next sequential port. The ports can range from 21000 through 65534. The first port must be an even number within this range.

The following example shows the UDP port (24100) defined in the VoIP dial-peer, so the range for the IP RTP Priority is 24100-24101:

```plaintext
dial-peer voice 1 voip
destination-pattern 1111
session protocol multicast
codec g711ulaw
session target ipv4:239.10.0.100:24100
interface serial 0/0
ip address 10.1.1.1
ip rtp priority 24100 2 64
```

**Low Latency Queuing**

Low-Latency Queuing (LLQ) applies to point-to-point links and to Frame Relay PVCs. LLQ creates a strict priority queue, as does IP RTP Priority, but LLQ applies the strict priority queue as a service-class within Class-Based Weighted Fair Queueing (CBWFQ). The functionality of fixed allocation but dynamic usage is again similar to IP RTP Priority.

A primary difference between IP RTP Priority and LLQ is that LLQ allows the usage of access control lists (ACLs) as the entrance criteria to the priority queue. This capability provides you with flexibility in determining what types of traffic are allowed into the priority queue.

The following example shows how LLQ is used to prioritize Cisco IPICS traffic:

```plaintext
access-list102 permit udp host 10.1.1.1 host 239.10.0.100 range 24100 24101
! class-map voice
match access-group 102
```
policy-map policy1
class voice
priority 50
!
multilink virtual-template 1
!
interface virtual-template 1
ip address 172.17.254.161 255.255.255.248
no ip directed-broadcast
no ip mroutecache
service-policy output policy1
ppp multilink
ppp multilink fragment-delay 20
ppp multilink interleave
!
interface serial 2/0
bandwidth 256
no ip address
no ip directed-broadcast
encapsulation ppp
no fair-queue
clockrate 256000
ppp multilink
multilink-group 1

QoS with Frame Relay

If you deploy Cisco IPICS in a Frame Relay network, be aware that Frame Relay does not inherently provide QoS. Frame Relay is a best-effort service that expects upper-layer applications to handle retransmissions that occur because of packet loss in the Frame Relay cloud.

Frame Relay typically provides the following parameters:

- **Committed Information Rate (CIR)**—Amount of bandwidth that the Frame Relay carrier guarantees to be available at all times for a particular PVC. The carrier does not make any guarantees for packets sent above CIR.

- **Burst**—Maximum amount of data that the Frame Relay carrier allows to be sent on a particular PVC. To offer the QoS over Frame service, carriers use a technique called *over-provisioning bandwidth*, in which they sell more bandwidth than they can provide at a particular time. This technique works because not all Frame Relay customers require all available bandwidth at one time.

Some Frame Relay carriers also guarantee a Frame Relay network that is always available and that will not drop any customer packets.

A Frame Relay carrier employs a variety of methods to offer a CIR + Burst service, including the following:

- Marking packets with discard eligible (DE) or drop the packets—Because real-time applications such as VoIP use UDP for transport, there is no mechanism for packets to be retransmitted. This situation is not a problem for VoIP because users would not want to hear a dropped word later in a sentence. Packet loss is generally not acceptable for real-time VoIP applications because it can result in choppy audio and garbled speech.

- Buffering all packets above the CIR—Eliminates lost packets, but can introduce jitter and delay because of the depth or rate at which the Frame Relay switches empty buffers.

Table 5-3 summarizes key recommendations when deploying Cisco IPICS on a network with Frame Relay.
Consider a Cisco IPICS Frame Relay network with the following characteristics:

- Three routers connected through 64 KB Frame Relay PVCs in a hub and spoke topology, with Router-1 being the hub.
- All routers configured to traffic-shape their data and voice on the WAN to CIR, and all routers that are using IP RTP Priority to guarantee QoS for the Cisco IPICS packets.
- Frame Relay broadcast-queue enabled on the serial interfaces.
- One Cisco IPICS channel configured.

Because the broadcast queue is only 40 packets deep by default and Cisco IPICS components transmit packets at 50 packets/second, the broadcast-queue must be set to prevent voice packets from dropping and to maintain voice quality. The recommended setting for the broadcast-queue is 64,000 bytes per second (64,000 bps), and 25 packets per second.

### Table 5-3 Recommendations when Deploying Cisco IPICS with Frame Relay

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Technique</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>To avoid introducing packet loss or jitter into a Cisco IPICS network, make sure that traffic that exceeds the CIR is not sent into a Frame Relay network.</td>
<td>Use the Cisco IOS Frame Relay Traffic Shaping (FRTS) feature.</td>
<td>Allows a router to police traffic on a per-PVC basis so that it does not send any traffic above the CIR.</td>
</tr>
<tr>
<td>In a Frame Relay environment, make sure that packets that are sent across a WAN link do not exceed the Committed Information Rate (CIR)</td>
<td>Enable the FRF.12 feature in the Frame network.</td>
<td>FRF.12 is a Frame-Relay-Forum Implementation Agreement that specifies how to fragment and reassemble packets on a Frame Relay network at Layer 2 of the Open Systems Interconnection (OSI) model. By fragmenting large data packets, the smaller Cisco IPICS packets will not be delayed, or subject to serialization, which helps to eliminate delay and jitter of the Cisco IPICS packets. Because the fragmentation and reassembly is done at Layer 2 of the OSI model, it does not adversely effect any upper-layer protocols (such as IPX or Appletalk or IP with DNF bits set) that do not handle fragmentation.</td>
</tr>
<tr>
<td>Implement a queuing technique that provides strict priority to Cisco IPICS packets.</td>
<td>Use a technique such as Low-Latency Queuing (LLQ)</td>
<td>The LLQ feature brings strict priority queuing to the Class-Based Weighted Fair Queuing (CBWFQ) method. Strict priority queuing allows delay-sensitive data such as voice to be dequeued and sent first (before packets in other queues are dequeued), giving delay-sensitive data preferential treatment over other traffic.</td>
</tr>
</tbody>
</table>
Frame Relay Broadcast Queue

Broadcast queue is a feature that is used in medium and large IP or IPX networks where routing and service access point (SAP) broadcasts must flow across a Frame Relay network. The broadcast queue is managed independently of the normal interface queue, has its own buffers, and has a configurable size and data rate.

To enable the broadcast queue, use this interface command:

```
frame-relay broadcast-queue size byte-rate packet-rate
```

A broadcast queue is given a maximum transmission rate (throughput) limit, which is measured in bytes per second and packets per second. The queue is serviced to ensure that only this maximum is provided. Because the broadcast queue has priority when transmitting at a rate below the configured maximum, it has a guaranteed minimum bandwidth allocation. The two transmission rate limits are intended to avoid flooding the interface with broadcasts. The actual limit in any second is the first rate limit that is reached. Given the transmission rate restriction, additional buffering is required to store broadcast packets.

The broadcast queue can be configured to store a large number of broadcast packets. You should set the queue size to a value that avoids loss of broadcast routing update packets. The exact size depends on the protocol being used and the number of packets required for each update. To be safe, the queue size should be set so that one complete routing update from each protocol and for each data-link connection identifier (DLCI) can be stored. As a general rule, start with 20 packets per DLCI. The byte rate should be less than both of the following:

- \( \frac{n}{4} \) times the minimum remote access rate (measured in bytes per second), where \( n \) is the number of DLCIs to which the broadcast must be replicated
- 1/4 the local access rate (measured in bytes per second)

The packet rate is not critical if the byte rate is set conservatively. In general, the packet rate should be set assuming 250-byte packets. The `frame-relay broadcast-queue` command defaults are as follows:

- **Size**—64 packets
- **Byte-rate**—256000 bytes per second
- **Packet-rate**—36 packets per second

The following configuration is an example of a Frame Relay connection with an ear and mouth (E&M) port:

```
Router-1 (Hub Router)

hostname FR-1
!
ip multicast-routing
!
voice class permanent 1
  signal timing oos timeout disabled
  signal keepalive disabled
  signal sequence oos no-action
!
interface Vif1
  ip address 1.1.1.1 255.255.255.0
  ip pim sparse-mode
!
routing rip
  network 1.1.1.0
  network 5.5.5.0
  network 5.5.6.0
!
interface Serial0/0
  no frame-relay broadcast-queue
```
encapsulation frame-relay
traffic-shaping
broadcast-queue 64 8000 250
!
interface Serial0/0.1 point-to-point
ip address 5.5.5.1 255.255.255.0
ip pim sparse-mode
frame-relay class ipics
interface-dlci 100
ip rtp header-compression
!
interface Serial0/0.1 point-to-point
ip address 5.5.6.1 255.255.255.0
ip pim sparse-mode
frame-relay class ipics
interface-dlci 100
ip rtp header-compression
!
map-class frame-relay ipics
cir 128000
bc 1280
mincir 128000
no adaptive-shaping
fair-queue
fragment 160
ip rtp priority 16384 16384 128
!
dial-peer voice 1 voip
destination-pattern 111
voice class permanent 1
session protocol multicast
session target ipv4:239.111.0.0:21000
ip precedence 5
!
Router-2 (Spoke Router)
hostname FR-2
ip multicast-routing
!
voice class permanent 1
signal timing oos timeout disabled
signal keepalive disabled
signal sequence oos no-action
!
interface Vif1
ip address 1.1.2.1 255.255.255.0
ip pim sparse-mode
!
router rip
network 1.1.2.0
network 5.5.5.0
!
interface Serial0/0
no broadcast-queue
circumference frame-relay
traffic-shaping
broadcast-queue 64 8000 250
!
interface Serial0/0.1 point-to-point
ip address 5.5.5.2 255.255.255.0
ip pim sparse-mode
frame-relay class ipics
frame-relay interface-dlci 100
frame-relay ip rtp header-compression
!
map-class frame-relay ipics
frame-relay cir 128000
frame-relay bc 1280
frame-relay mincir 128000
no frame-relay adaptive-shaping
frame-relay fair-queue
frame-relay fragment 160
frame-relay ip rtp priority 16384 16384 128
!
voice-port 1/0/0
connection trunk 111
operation 4-wire
!
dial-peer voice 1 voip
destination-pattern 111
voice class permanent 1
session protocol multicast
session target ipv4:239.111.0.0:21000
ip precedence 5
!
Router-3 (Spoke Router)

hostname FR-3
!
interface Vif1
ip address 1.1.3.1 255.255.255.0
ip pim sparse-mode
!
router rip
network 1.1.3.0
network 5.5.6.0
!
interface Serial0/0
no frame-relay broadcast-queue
encapsulation frame-relay
frame-relay traffic-shaping
frame-relay broadcast-queue 64 8000 250
!
interface Serial0/0.1 point-to-point
ip address 5.5.6.2 255.255.255.0
ip pim sparse-mode
frame-relay class ipics
frame-relay interface-dlci 100
frame-relay ip rtp header-compression
!
map-class frame-relay ipics
frame-relay cir 128000
frame-relay bc 1280
frame-relay mincir 128000
Quality of Service

Configuration with Bidirectional PIM Multicast

Bidirectional PIM multicast is preferred over unidirectional multicast when two PVCs, one dedicated to channel traffic and the other to data traffic, are used. It helps to reduce the number of \texttt{ip mroute} entries that are needed in the router to route multicast traffic. Bidirectional PIM requires one router in the network to act as the rendezvous point (RP).

In the following configuration example, the RP is the loopback interface of Router-1. (The RP can be any interface on any router in the network, as long as it is reachable.)

Router-1 (RP node)

```
hostname bidir-rp
! ip multicast-routing
! voice class permanent 1
  signal timing oos timeout disabled
  signal keepalive disabled
  signal sequence oos no-action
! voice class permanent 2
  signal timing oos timeout disabled
  signal keepalive disabled
  signal sequence oos no-action
! interface Loopback1
  ip address 10.10.2.1 255.255.255.0
  ip pim sparse-mode
! interface Vif1
  ip address 10.1.2.1 255.255.255.0
  ip pim sparse-mode
  load-interval 30
! router rip
  network 10.1.2.0
  network 10.100.0.0
  network 10.101.0.0
! interface Serial0/0
  no ip address
  encapsulation frame-relay IETF
  load-interval 30
```

Configuration

```bash
no frame-relay adaptive-shaping
frame-relay fair-queue
frame-relay fragment 160
frame-relay ip rtp priority 16384 16384 128
!
voice-port 1/0/0
!connection trunk 111
!operation 4-wire
!
dial-peer voice 1 voip
!destination-pattern 111
!voice class permanent 1
!session protocol multicast
!session target ipv4:239.111.0.0:21000
!ip precedence 5
!
end
```
no fair-queue
frame-relay traffic-shaping
frame-relay lmi-type cisco
!
interface Serial0/0.1 point-to-point
description channel pvc
bandwidth 256
ip address 10.100.100.1 255.255.255.0
ip pim sparse-mode
frame-relay interface-dlci 100
class channel
!
interface Serial0/0.2 point-to-point
description data pvc
ip address 10.101.101.1 255.255.255.0
frame-relay interface-dlci 200
class data
!
ip classless
ip pim bidir-enable
ip pim rp-address 10.10.2.1 10 override bidir
!
map-class frame-relay channel
frame-relay cir 128000
frame-relay bc 1000
frame-relay be 0
no frame-relay adaptive-shaping
!
map-class frame-relay data
frame-relay cir 768000
frame-relay mincir 128000
frame-relay adaptive-shaping becn
!
voice-port 1/0/0
voice class permanent 1
timeouts wait-release 3
timing dialout-delay 70
connection trunk 111
operation 4-wire
signal lmr
!
dial-peer voice 1 voip
destination-pattern 111
session protocol multicast
session target ipv4:239.111.0.0:21000
ip precedence 5
!
end

Router-2 (non-RP node)

hostname bidir-2
!
ip multicast-routing
!
voice class permanent 1
signal timing oos timeout disabled
signal keepalive disabled
signal sequence oos no-action
!
voice class permanent 2
signal timing oos timeout disabled
signal keepalive disabled
signal sequence oos no-action
interface Loopback1
  ip address 10.10.3.1 255.255.255.0
  ip pim sparse-mode

interface Vif1
  ip address 10.1.3.1 255.255.255.0
  ip pim sparse-mode

load-interval 30

router rip
  network 10.1.3.0
  network 10.100.0.0
  network 10.101.0.0

! interface Serial0/0
  no ip address
  encapsulation frame-relay IETF
  load-interval 30
  no fair-queue
  frame-relay traffic-shaping
  frame-relay lmi-type cisco

! interface Serial0/0.1 point-to-point
  description channel pvc
  bandwidth 256
  ip address 10.100.100.2 255.255.255.0
  ip pim sparse-mode
  frame-relay interface-dlci 100
  class channel

! interface Serial0/0.2 point-to-point
  description data pvc
  ip address 10.101.101.2 255.255.255.0
  frame-relay interface-dlci 200
  class data

! ip classless
  ip route 10.10.2.1 255.255.255.255 Serial0/0.1
  ip pim bidir-enable
  ip pim rp-address 10.10.2.1 10 bidir

  map-class frame-relay channel
  frame-relay cir 128000
  frame-relay bc 1000
  frame-relay be 0
  no frame-relay adaptive-shaping

  map-class frame-relay data
  frame-relay cir 768000
  frame-relay mincir 128000
  frame-relay adaptive-shaping becn

voice-port 1/0/0
  voice class permanent 1
  playout-delay nominal 100
  playout-delay minimum high
  playout-delay mode adaptive
  playout-delay maximum 250
  timeouts wait-release 3
  timing dialout-delay 70
  connection trunk 111
  operation 4-wire
  signal lmr
QoS with Point-to-Point Connections

This section provides information for WANs that have point-to-point connections that include any of these encapsulations:

- Point-to-Point Protocol (PPP)
- Multilink Point-to-Point Protocol (MLPPP)
- High-Level Data Link Control (HDLC)

Guaranteed bandwidth is not an issue on point-to-point (or leased) lines, but you do need to consider connection speed and queuing in these situations. As described in the “QoS with Frame Relay” section on page 5-11, links below 768 KB require that larger data packets be fragmented to avoid serialization. In addition, you should use a queuing technique that provides strict priority to Cisco IPICS packets, such as IP RTP Priority, or Low-Latency Queuing.

The FRF.12 fragmentation and reassembly technique that is discussed in the “QoS with Frame Relay” section on page 5-11 does not apply to point-to-point links. For point-to-point links below 768 KB, use Multilink PPP (MLPPP) for encapsulation. MLPPP provides feature called Link Fragmentation and Interleaving (LFI). LFI is similar in operation to FRF.12 in that it handles fragmentation at Layer 2. LFI is not required for networks with link speeds above 768k because 1,500 bytes packet do not cause more than approximately 10 ms of transport delay. This delay should be acceptable for most delay budgets, so for these networks, HDLC or PPP encapsulation are acceptable.

The following example shows configuring MLPPP with LFI:

```
interface Serial0
bandwidth 64
no ip address
no ip directed-broadcast
encapsulation ppp
no ip route-cache
no ip mroute-cache
no fair-queue
ppp multilink
multilink-group 1
!
interface Multilink 1
ip address 10.1.1.1 255.255.255.252
no ip directed-broadcast
no ip route-cache
ip rtp header-compression iphc-format
ip tcp header-compression iphc-format
no ip mroute-cache
fair-queue 64 256 1000
ppp multilink
ppp multilink fragment-delay 10
ppp multilink interleave
multilink-group 1
ip rtp priority 16384 16383 30
!
```
Quality of Service

QoS for a LAN

When you deploy QoS in a LAN, classify and mark applications as close to their sources as possible. For example, implement QoS in a Cisco Catalyst switch for Cisco Unified IP Phones that connect to the Cisco IPICS server via multicast. For LMRs, implement QoS in the dial peer that is configured for the E&M port that connects to the radios.

To classify and mark applications, follow these recommendations:

- Use Differentiated Services Code Point (DSCP) markings whenever possible.
- Follow standards-based DSCP per-hop behaviors (PHB) to ensure interoperability and provide for future expansion. These standards include:
  - RFC 2474 Class Selector Codepoints
  - RFC 2597 Assured Forwarding Classes
  - RFC 3246 Expedited Forwarding.

QoS at the WAN Edge

QoS should be configured at the WAN edge so that QoS settings are forwarded to the next-hop router. When you configure QoS at the WAN edge, follow these recommendations:

- If the combined WAN circuit-rate is significantly below 100 Mbps, enable egress shaping on the Cisco Catalyst switches (when supported).
- If the combined WAN circuit-rate is significantly below 100 Mbps and the Cisco Catalyst switch does not support shaping, enable egress policing (when supported).

Policing

Policing is configured so that traffic of a certain class that exceeds the allocated bandwidth is marked as discard eligible (DE) or is dropped, so it prevents denial of service (DoS) or a virus attacks. When you configure policing, follow these recommendations:

- Police traffic flows as close to their sources as possible.
- Perform markdown according to standards-based rules, whenever supported.
- RFC 2597 specifies how Assured Forwarding traffic classes should be marked down (AF11 > AF12 > AF13). You should follow this specification when DSCP-Based WRED is supported on egress queues.
- Cisco Catalyst platforms do not support DSCP-Based WRED. Scavenger-class remarking is a viable alternative.
- Non-AF classes do not have a markdown scheme defined in standards, so Scavenger-class remarking is a viable option.
- Profile applications to determine what constitutes “normal” or “abnormal” flows (within a 95% confidence interval).
- Deploy campus access-edge policers to remark abnormal traffic to Scavenger.
- Deploy a second-line of defense at the distribution-layer via per-user microflow policing.
- Provision end-to-end “less-than-best-Effort” scavenger-class queuing policies.
Queuing

Queuing is a method of buffering traffic so that the traffic does not overflow the allocated bandwidth on a WAN. To provide service guarantees, enable queuing at any node that has the potential for congestion.

When you enable queuing, follow these recommendations:

- Reserve at least 25% of the bandwidth of a link for the default best effort class.
- Limit the amount of strict-priority queuing to 33% of the capacity of a link.
- Whenever a Scavenger queuing class is enabled, assign it to a minimal amount of bandwidth.
- To ensure consistent per-hop behavior (PHB), configure consistent queuing policies in the campus, WAN, and VPN, according to platform capabilities.
- Enable WRED on all TCP flows, if supported. DSCP-based WRED is recommended.

Trust Boundaries

The Cisco IPICS QoS infrastructure is defined by using a trust boundary. For detailed information about trust boundary concepts, refer to Cisco Unified Communications SRND Based on Cisco Unified CallManager 4.x, which is available at this URL:


A trust boundary can include LMRs, and Cisco Unified IP Phones. IP precedence should be marked for Cisco Unified IP Phones, with a suggested value of 5 for voice traffic (such as RTP) and 3 for voice signaling (such as SIP or SCCP).

For a LMR PTT client, an LMR gateway marks the traffic coming from E&M ports to IP precedence 5 as follows:

```
voice-port 1/0/0
  voice class permanent 1
  connection trunk 111
  operation 4-wire
!
dial-peer voice 111 voip
  destination-pattern 111
  session protocol multicast
  session target ipv4:239.111.0.111:21000
  ip precedence 5
!
```

Cisco IPICS traffic that flows from an LMR or Cisco Unified IP Phone aggregates on an access switch, and QoS configuration is applied on this switch. Once marked, these values for IP precedence are honored throughout the network.

If one of the Cisco IPICS trusted endpoint is located in the PSTN, these endpoints are connected through a voice gateway. Cisco voice gateways can set IP precedence and DSCP values for voice control and bearer traffic to 3 (AF31/SC3) and 5 (EF/CS5) respectively.

VoIP bearer traffic is placed in a strict-priority queue, when possible. The boundary nodes police at the ingress level to rate-limit the VoIP traffic to avoid potential bandwidth exhaustion and the possibility of DoS attack through priority queues.

Figure 5-2 shows a trust boundary.
Figure 5-2  Trust Boundary

1 Trusted IP Phone PTT Endpoint
2 Trusted Mobile Client Endpoint

The following example shows access layer QoS configuration for a Cisco Catalyst 3550:

```
CAT3550(config)#mls qos map policed-dscp 0 24 46 to 8
! Excess traffic marked 0 or CS3 or EF will be remarked to CS1
CAT3550(config)#
CAT3550(config)#class-map match-all IPICS-VOICE
CAT3550(config-cmap)#  match access-group name IPICS-VOICE
CAT3550(config)#policy-map IPICS-PTTC
CAT3550(config-pmap)#class IPICS-VOICE
CAT3550(config-pmap-c)# set ip dscp 46
! VoIP is marked to DSCP EF
CAT3550(config-pmap-c)# police 128000 8000 exceed-action policed-dscp-transmit
! Out-of-profile IPICS VoIP (G711) is marked down to Scavenger (CS1)
CAT3550(config-pmap-c)#class IPICS-SIGNALING
CAT3550(config-pmap-c)# set ip dscp 24
! Signalling is marked to DSCP CS3
CAT3550(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
! Out-of-profile Signalling is marked down to Scavenger (CS1)
CAT3550(config-pmap-c)#class class-default
CAT3550(config-pmap-c)# set ip dscp 0
CAT3550(config-pmap-c)# police 50000 8000 exceed-action policed-dscp-transmit
! Out-of-profile data traffic is marked down to Scavenger (CS1) 50000 (Depends on per customer design and requirements)
CAT3550(config-pmap-c)# exit
CAT3550(config-pmap)#exit
CAT3550(config)#
CAT3550(config)#interface range FastEthernet0/1 - 48
CAT3550(config-if)# service-policy input IPICS-PTTC
! Attaching the policy map IPICS-PTTC to the interface range
CAT3550(config-if)#exit
CAT3550(config)#
CAT3550(config)#ip access-list extended IPICS-VOICE
! Extended ACL for the IPICS Address/Port ranges
CAT3550(config-ext-nacl)#
permit udp 233.0.0.0 0.255.255.255 233.0.0.0 0.255.255.255 range 21000 65534
permit udp 233.0.0.0 0.255.255.255 239.0.0.0 0.255.255.255 range 21000 65534
permit udp 239.0.0.0 0.255.255.255 233.0.0.0 0.255.255.255 range 21000 65534
```
permit udp 239.0.0.0 0.255.255.255 239.0.0.0 0.255.255.255 range 21000 65534
CAT3550(config-ext-nacl)# ip access-list extended IPICS-SIGNALING
! Extended ACL for the remote IDC clients
CAT3550(config-ext-nacl)# permit udp <RMS IP Address> <Any > eq 5060
! Extended ACL for the PSTN clients
CAT3550(config-ext-nacl)# permit udp <VoiceGW IP Address> <Any > eq 5060
CAT3550(config-ext-nacl)# permit tcp <VoiceGW IP Address> <Any > eq 1720
CAT3550(config-ext-nacl)# end
CAT3550#

VPN in Deployment Scenarios

A Cisco IPICS deployment can include a VPN implementation for mobile clients.

For the mobile client, audio cannot be transmitted bidirectionally on a 3G network because certain providers block the audio on their data networks. Implementing a VPN tunnel between the Cisco IPICS server and the mobile client allows bidirectional transmission of audio. (Bidirectional audio quality depends on the service provider.)

In addition, if a IPICS server typically resides in an enterprise network, the mobile client must be able to reach it over a public network. There are two methods by which the mobile client can reach the Cisco IPICS server over a wireless network or a 3G network. For a wireless connection, ensure that the wireless network can access the CISCO IPICS Server. If this connectivity is not available, the mobile client should be able to use its own VPN client and create a tunnel to the Cisco IPICS server. For a 3G network connection, a VPN client is required on the mobile client to contact the Cisco IPICS server.

To allow the mobile client to contact the Cisco IPCS server, the server must have its domain name resolve to an IP address. The mobile client must be able to contact a DNS server that is supplied by a service provider or by the VPN configuration.

For related information about VPNs, see the following documentation:

- Cisco AnyConnect Secure Mobility Solution Guide:
  AnyConnect_Secure_Mobility_SolutionGuide.pdf

- “General VPN Setup” chapter in Cisco ASA 5500 Series Configuration Guide using ASDM:
  vpn_gen.html

Port Utilization

This section describes the ports that can be used in a Cisco IPICS deployment. You can use this information to determine how best to define the QOS or firewall settings at a port level, if required. In the event that modifications to the port ranges are required, the details regarding how to facilitate that change are included.

Table 5-4 describes the default ports that are used by Cisco IPICS components.
Guidelines for Using IP Multicast Addresses with Cisco IPICS

When you use multicast communications with Cisco IPICS be aware of the following guidelines:

- This address range is part of the Administratively Scoped Block, as specified by RFC 3171, and is intended for use in a local domain. As such, this address range is less likely to cause an addressing conflict in an existing multicast domain.

- Although RFC 3171 permits the use of IP multicast addresses that span the 224.0.0.0 through 239.255.255.255 range, where the first octet contains 224, 232, 233, 238, or 239 and subsequent octets contain 0 through 255, be aware that Cisco enforces the use of the 239.192.0.0 to 239.251.255.255 range to ensure proper use and desired results.

- For more information, refer to RFC 3171 - Internet Assigned Numbers Authority (IANA) Guidelines for IPv4 Multicast Address Assignment and RFC 2365 - Administratively Scoped IP Multicast.

The following section provide related information:

- Guidelines for Using IP Multicast Addresses with Cisco IPICS, page 5-24
- QOS Policy Considerations, page 5-25

### Table 5-4 Default Ports used by Cisco IPICS Components

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Device</th>
<th>Destination Port</th>
<th>Remote Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>Cisco IPICS Administration</td>
<td>TCP 80</td>
<td>Cisco IPICS server</td>
</tr>
<tr>
<td></td>
<td>Console</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Unified IP Phone</td>
<td>TCP 80</td>
<td>Cisco Unified Communications Manager, Cisco Unified Communications Manager Express</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Cisco IPICS Administration</td>
<td>TCP 443</td>
<td>Cisco IPICS server</td>
</tr>
<tr>
<td></td>
<td>Console</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIP</td>
<td>Policy Engine</td>
<td>UDP 5060</td>
<td>UMS / policy engine SIP provider</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCP 5060 and 5061</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>UDP 5060, 5061, and 4000</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>20480</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mobile client</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>UMS</td>
</tr>
<tr>
<td>RTP/RTCP</td>
<td>Policy Engine</td>
<td>UDP 32768-61000</td>
<td>Cisco Unified Communications Manager, Cisco Unified Communications Manager Express</td>
</tr>
<tr>
<td>ICMP (PING)</td>
<td>IUMS</td>
<td>ICMP</td>
<td>Cisco IPICS server</td>
</tr>
<tr>
<td>IGMP</td>
<td>UMS</td>
<td>ICMP</td>
<td>Multicast group</td>
</tr>
<tr>
<td>SSH</td>
<td>Cisco IPICS server</td>
<td>TCP 22</td>
<td>UMS</td>
</tr>
</tbody>
</table>
QOS Policy Considerations

When defining QOS policies that will be assigned to a UDP port range, using Source Host and Destination Host addresses of ANY allows the QOS policy to be properly set based on the mobile client UDP port range. In this case, UDP ports that are assigned by the UMS are not considered, which helps to simplify the QOS policies.

Securing the Cisco IPICS Infrastructure

The following sections provide information about providing system security for Cisco IPICS:

- Secure Socket Layer, page 5-25
- Firewalls and Access Control Lists, page 5-25
- Other Security Recommendations, page 5-25

Secure Socket Layer

Cisco IPICS uses Secure Socket Layer (SSL) to encrypt communications with the Cisco IPICS server. The browser with which you access the Cisco IPICS Administration Console uses HTTPS. To enforce SSL, you must install a certificate on the Cisco IPICS server. You can use a self-signed certificate or, to impose additional security, you can purchase and set up a digitally-signed certificate. In addition, the RMS control uses SSH as a client.

For additional information, refer to the “Installing Third Party Certificates on the Cisco IPICS Server” section in Cisco IPICS Server Installation and Upgrade Guide, Release 4.0(2).

Firewalls and Access Control Lists

Use a firewall and access control lists (ACLs) in front of the Cisco IPICS server and other Cisco IPICS components to add an extra layer of security. For example, you can use a firewall or an ACL to allow only call control and management packets to reach the Cisco IPICS server, and block unnecessary traffic such as Telnet or TFTP traffic. You can use ACLs to allow only the source addresses that are supposed to access your network.

When you use a firewall, it must support state-full inspection of voice signaling protocol. Cisco IPICS uses UDP ports 21000–65534, and a firewall must only open the ports needed to support for this application. In addition, make sure that the firewall supports application layer gateway (ALG) capabilities. ALG inspects signaling packets to discover what UDP port an RTP stream is going to use and dynamically opens a pinhole for that UDP port.

Other Security Recommendations

For additional security in a Cisco IPICS network, follow these recommendations:

- Use Terminal Access Controller Access-Control System+ (TACACS+) and Remote Authentication Dial In User Service (RADIUS) to provide highly secure access in your network.
- Do not rely only on VLANs for separation; also provide layer 3 filtering at the access layer of your network.
Use VLANs and IP filters between your voice and data network.

Use out of band management switches and routers with SSH, HTTPS, out-of-band (OOB), permit lists, and so on to control who is accessing your network devices.

Disable unused switch ports on the LAN switches and place them in an unused VLAN so that they are not misused.

Use spanning tree (STP) attack mitigation tools such as Bridge Protocol Data Unit (BPDU) Guard and Root Guard.

Disperse critical resources to provide redundancy.

Provide limited and controlled access to power switches.

Use IDS Host software on the Cisco IPICS server and other network servers to ensure security of voice applications.

Cisco IPICS Network Management System

When you plan for managing and monitoring a Cisco IPICS network, define the parameters that can be operatively monitored in the Cisco IPICS environment. You can use the outputs from these parameters to establish a set of alarms for spontaneous problems, and to establish a proactive, early warning system.

As you develop a management and monitoring policy for your network, take these actions:

- For each component in the network, define the parameters that must monitored on the component
- Select the network management and monitoring tools that are appropriate for monitoring the parameters that you defined

Managing the Overall Network

The Cisco Multicast Manager (CMM) is a web-based network management application that is designed to aid in the monitoring and troubleshooting of multicast networks. Cisco Multicast Manager includes the following features and benefits:

- Early warning of problems in multicast networks
- In-depth troubleshooting and analysis capabilities
- On demand, real time and historical reporting capabilities
- Optimization of network utilization and enhancement of services delivery over multicast enabled networks

CMM can monitor all multicast-capable devices that are running Cisco IOS, including Layer 2 switches. For more detailed information about CMM, refer to this URL:


If you use Cisco Unified IP Phones as PTT clients in your Cisco IPICS network, you can use various IP Telephony (IPT) management tools to manage these devices. For example, you can use Enterprise IPT management solution, which uses OpenView Gateway Statistics Utility (GSU) Reporting Solution and CiscoWorks IP Telephony Environment Monitor (ITEM) solution to provide real-time, detailed fault analysis specifically designed for Cisco IPT devices. This tool evaluates the health of IPT implementations and provides alerting and notification of problems and areas that should be addressed...
to help minimize IPT service interruption. IPT management solution also identifies the underutilized or imbalanced gateway resources, and provides historical trending and forecasting of capacity requirements.

Other items to monitor in a Cisco IPICS network in include the following:

- Cisco IPICS server health
- Cisco IPICS services health
- IP gateway health
- Cisco Unified Communications Manager functionality
- QoS monitoring
- L2/L3 switches and applications
Understanding Dial Peers

Dial peers identify call source and destination endpoints and define the characteristics that are applied to each call leg in a call connection. Understanding the principles behind dial peers can increase your understanding of how Cisco IPICS works.

This chapter includes these topics:

- **Dial Peer Call Legs, page 6-1**
- **Inbound and Outbound Dial Peers, page 6-2**
- **Destination Pattern, page 6-3**
- **Session Target, page 6-3**
- **Configuring Dial Peers for Call Legs, page 6-3**
- **Matching Inbound and Outbound Dial Peers, page 6-4**

## Dial Peer Call Legs

A traditional voice call over the PSTN uses a dedicated 64 KB circuit end-to-end. In contrast, a voice call over the packet network is made up of discrete segments, or call legs. A call leg is a logical connection between two routers or between a router and a telephony device. A voice call comprises four call legs, two from the perspective of the originating router and two from the perspective of the terminating router, as shown in Figure 6-1.

![Figure 6-1 Dial Peer Call Legs](image)

A dial peer is associated with each call leg. Attributes that are defined in a dial peer and applied to the call leg include codec, quality of service (QoS), and Voice Activation Detection (VAD). To complete a voice call, you must configure a dial peer for each of the four call legs in the call connection.

Depending on the call leg, a call is routed by using one of these dial peer types:
Inbound and Outbound Dial Peers

Dial peers are used for inbound and outbound call legs. It is important to understand that these terms are defined from the perspective of the router. An inbound call leg originates when an incoming call comes in to the router. An outbound call leg originates when an outgoing call is placed from the router. Figure 6-2 illustrates call legs from the perspective of the originating router. Figure 6-3 illustrates call legs from the perspective of the terminating router.

- POTS (Plain Old Telephone Service)–Dial peer that defines the characteristics of a traditional telephony network connection. POTS dial peers map a dialed string to a specific voice port on the local router, normally the voice port connecting the router to the local PSTN, private branch exchange (PBX), or telephone.
- Voice-network—Dial peer that defines the characteristics of a packet network connection. Voice-network dial peers map a dialed string to a remote network device, such as the destination router that is connected to the remote telephony device.

The specific type of voice-network dial peer depends on the packet network technology:
- VoIP (Voice over IP)—Points to the IP address of the destination router that terminates the call
- VoFR (Voice over Frame Relay)—Points to the data-link connection identifier (DLCI) of the interface from which the call exits the router
- VoATM (Voice over ATM)—Points to the ATM virtual circuit for the interface from which the call exits the router

POTS and voice-network dial peers are needed to establish either voice connections over a packet network or a unicast connection trunk.
For inbound calls from a POTS interface that are destined for the packet network, the router matches a POTS dial peer for the inbound call leg and a voice-network dial peer, such as VoIP or VoFR, for the outbound leg. For inbound calls from the packet network, the router matches a POTS dial peer to terminate the call and a voice-network dial peer to apply features such as codec or QoS.

The following examples show basic configurations for POTS and VoIP dial peers:

```plaintext
dial-peer voice 1 pots
    destination-pattern 555....
    port 1/0:1

dial-peer voice 2 voip
    destination-pattern 555....
    session target ipv4:192.168.1.1
```

The router selects a dial peer for a call leg by matching the string that is defined by using the answer-address, destination-pattern, or incoming called-number command in the dial peer configuration. For Cisco IPICS, the destination-pattern is used in the dial peer configurations.

### Destination Pattern

Cisco IPICS configurations use the destination pattern, which associates a string with a specific device. You configure a destination pattern in a dial peer by using the destination-pattern command. If the string matches the destination pattern, the call is routed according to the voice port in POTS dial peers, or the session target in voice-network dial peers. For outbound voice-network dial peers, the destination pattern may also determine the dialed digits that the router collects and then forwards to the remote telephony interface. You must configure a destination pattern for each POTS and voice-network dial peer that you define on the router.

### Session Target

The session target is the network address of the remote router to which you want to send a call once a local voice-network dial peer is matched. It is configured in voice-network dial peers by using the session target command. For outbound dial peers, the destination pattern is the telephone number of the remote voice device that you want to reach. The session target represents the path to the remote router that is connected to that voice device.

Establishing voice communication over a packet network is similar to configuring a static route; you are establishing a specific voice connection between two defined endpoints. Call legs define the discrete segments that lie between two points in the call connection. A voice call over the packet network comprises four call legs, two on the originating router and two on the terminating router. A dial peer is associated with each of these four call legs.

### Configuring Dial Peers for Call Legs

When a voice call comes into the router, the router must match dial peers to route the call. For inbound calls from a POTS interface that are being sent over the packet network, the router matches a POTS dial peer for the inbound call leg and a voice-network dial peer for the outbound call leg. For calls coming into the router from the packet network, the router matches an outbound POTS dial peer to terminate the call and an inbound voice-network dial peer for features such as codec, VAD, and QoS.
Matching Inbound and Outbound Dial Peers

To match inbound call legs to dial peers, the router uses three information elements in the call setup message and four configurable dial peer attributes. The call setup elements are:

- Called number or dialed number identification service (DNIS)—Set of numbers representing the destination
- Calling number or automatic number identification (ANI)—Set of numbers representing the origin
- Voice port—Voice port carrying the call.

The configurable dial peer attributes are:

- Incoming called-number—String representing the called number or DNIS. It is configured by using the `incoming called-number dial-peer configuration` command in POTS and VoIP dial peers.
- Answer address—String representing the calling number or ANI. It is configured by using the `answer-address dial-peer configuration` command in POTS or VoIP dial peers and is used only for inbound calls from the IP network.
- Destination pattern—String representing the calling number or ANI. It is configured by using the `destination-pattern dial-peer configuration` command in POTS or voice-network dial peers.
- Port—Voice port through which calls to this dial peer are placed.

The router selects an inbound dial peer by matching the information elements in the setup message with the dial peer attributes. The router attempts to match these items in the following order:

1. Called number with incoming called-number.
2. Calling number with answer-address.
3. Calling number with destination-pattern.
4. Incoming voice port with configured voice port.

The router must match only one of these conditions to select a dial peer. It is not necessary for all the attributes to be configured in the dial peer or that every attribute match the call setup information. The router stops searching as soon as one dial peer is matched and the call is routed according to the configured dial peer attributes. Even if there are other dial peers that would match, only the first match is used.

The router selects an outbound dial peer based on the dial string. If the dial string matches a configured dial peer, the router places the call by using the configured attributes in the matching dial peer.
This chapter provides information about how Cisco IPICS uses licensable features. It also provides information about resource usage and system sizing. Use this information to help plan your Cisco IPICS deployment.

This chapter includes these topics:

- Resource and License Usage, page 7-1
- UMS Usage, page 7-1
- Additional Planning and Sizing Guidelines, page 7-2
- Dial Port Licensing Details, page 7-2

### Resource and License Usage

To properly design a Cisco IPICS deployment, it is important to understand how resources are licensed and used. The Cisco IPICS license determines the number of concurrent land mobile radio (LMR) ports, multicast ports, IP phone users, dial users, and ops views that are available for your system. The total number of LMR and multicast ports, IP phone, dial users, and ops views cannot exceed the number that is specified in the license or licenses that you purchased. See the “Managing Licenses” section in “Chapter 2 Performing Cisco IPICS System Administrator Tasks” in *Cisco IPICS Server Administration Guide, Release 4.7(1)*.

### UMS Usage

A single UMS license is used in the following situations:

- For each channel in an active VTG
- For each instance of an active VTG that is accessed by a dial-in or dial-out user, regardless of the number of users who are connected to the VTG
- For each mobile client
Additional Planning and Sizing Guidelines

Each channel that is associated with a mobile client user ID consumes one UMS resource when a user logs in with that ID. For example, if a user ID has 10 associated channels, 10 UMS resources are used when a user logs in with this ID. If a mobile client user has several associated channels but does not require all of these channels when logging in from the Remote location, you can conserve system resources by creating an alternate login ID for the user. Configure this alternate login ID with only the resources that the user needs when connecting to Cisco IPICS, and instruct the user to log in with this alternate ID when connecting from a mobile client.

Dial Port Licensing Details

A Cisco IPICS license for the policy engine includes licenses for the purchased number of Cisco IPICS dial ports. These licenses determine the total number of dial users (incoming and outgoing) who can be connected simultaneously.

Dial port usage can be partitioned per ops view. This way, a Cisco IPICS administrator can limit the number of Cisco IPICS dial port licenses in groups that are segmented by ops views.

Dial ports from the available dial pool are used by the currently executing policy notification or invite actions. If there are fewer dial ports available than what is needed, other policy actions will wait for a dial port to become available.

The recipient of a call must authenticate properly for the call to succeed. Otherwise, the call is considered unsuccessful and the system moves on to the next number that is configured in the dial preferences for the recipient. If you want the system to retry the same number, enter the same number again as a dial preference. The system attempts one call to each number in the dial preferences. It stops attempting calls when the recipient authenticates properly or when the system has tried all numbers.

Dial pool configurations are made in the Administration Console Ops View window. For detailed information, refer to the “Configuring and Managing Cisco IPICS Operational Views” chapter in Cisco IPICS Server Administration Guide, Release 4.0(2).
This chapter describes Cisco IPICS deployment models. You can use these models as guides when you design your Cisco IPICS deployment.

This chapter includes these topics:

- Single Site Model, page 8-1
- Multiple Site Model, page 8-2

## Single Site Model

The Cisco IPICS single site model represents a deployment in a single multicast domain. Cisco IPICS components are located at one multicast-enabled site or campus, with no Cisco IPICS multicast services provided over an IP WAN. The single site model typically is deployed over a LAN or metropolitan area network (MAN), either of which carries the multicast voice traffic within the site. Calls from beyond the LAN or MAN connect to the Cisco IPICS domain via a SIP-based unicast call.

The single site model has the following design characteristics:

- Cisco IPICS server
- UMS
- Cisco Unified IP Phones
- LMR gateways (optional)
- Multicast-enabled network using PIM Sparse mode.

Figure 8-1 illustrates the Cisco IPICS single site model.
Benefits of the Single Site Model

A single infrastructure for a converged network solution provides significant cost benefits, and it enables Cisco IPICS to take advantage of the IP-based applications in an enterprise. In addition, a single site deployment allows a site to be completely self-contained. There is no dependency on an IP WAN, and a WAN failure or insufficient bandwidth will not cause loss of Cisco IPICS service or functionality.

Best Practices for the Single Site Model

When you implement a Cisco IPICS single site model, follow these guidelines:

- Provide a highly available, fault-tolerant infrastructure. A sound infrastructure is important for the installation of Cisco IPICS and makes it easier to change to a multiple site deployment, if you choose to do so.
- Use the G.711 codec for all local endpoints. This practice eliminates the consumption of DSP resources for transcoding.
- Implement the recommended network infrastructure for high availability, connectivity options for phones (inline power), QoS mechanisms, multicast, and security. (For more information, see Chapter 5, “Cisco IPICS Infrastructure Considerations.”)

Multiple Site Model

The Cisco IPICS multiple site model consists of a single Cisco IPICS server that provides services for two or more sites and that uses the IP WAN to transport multicast IP voice traffic between the sites. The IP WAN also carries call control signaling between the central site and the remote sites.

Multicast may be enabled between sites, but it is not required. Multiple sites connected by a multicast-enabled WAN are in effect a topologically different case of the single site model, because there is only one multicast domain. The main difference between multiple site model deployments is whether the connecting core network is a service provider network that employs Multiprotocol Label Switching (MPLS). If it is, MPLS with multicast VPNs is deployed to produce a single multicast domain between
Multiple sites with no native multicast support between sites can either employ Multicast over Generic Routing Encapsulation (GRE). IPSec VPNs can also be configured between sites to secure inter-site traffic.

Figure 8-2 illustrates a typical Cisco IPICS multiple site deployment, with a Cisco IPICS server at the central site and an IP WAN to connect all the sites.

Figure 8-2  Multiple Site Model

In the multiple site model, connectivity options for the IP WAN include the following:

- Leased lines
- Frame Relay
- Asynchronous Transfer Mode (ATM)
- ATM and Frame Relay Service Inter-Working (SIW)
- MPLS Virtual Private Network
- Voice and Video Enabled IP Security Protocol (IPSec) VPN (V3PN)

Routers that reside at the edges of the WAN require quality of service (QoS) mechanisms, such as priority queuing and traffic shaping, to protect the voice traffic from the data traffic across the WAN, where bandwidth is typically scarce.

This section includes these topics:

- MPLS with Multicast VPNs, page 8-3
- Multicast Islands, page 8-10
- VPN Termination for Mobile Clients, page 8-15

**MPLS with Multicast VPNs**

MPLS does not support native multicast in an MPLS VPN. This section discusses a technique for enabling multicast across an MPLS core. This section assumes that the unicast MPLS core and the VPN have been configured and are operating properly, and it assumes that you are familiar with IP multicast and MPLS. For additional information about these topics, refer to the documentation at this URL: http://www.cisco.com/en/US/products/ps6552/products_ios_technology_home.html
**Figure 8-3** illustrates the topology that is discussed in this section.

**MPLS Terminology**

The following terms apply to MPLS:

- **Customer Edge Router (CE)**—Router at the edge of a network and that has interfaces to at least one Provider Edge (PE) router.

- **Data Multicast Distribution Tree (MDT)**—Tree created dynamically by the existence of active sources in the network and that is sent to active receivers located behind separate PE routers. Data MDT connects only to PE routers that are attached to CE routers with active sources or receivers of traffic from active sources or that are directly attached to active sources or receivers of traffic.

- **Default-MDT**—Tree created by the multicast virtual private network (MVPN) configuration. The Default-MDT is used for customer Control Plane and low rate Data Plane traffic. It uses Routing and Forwarding (MVRFs) to connect all of the PE routers in a particular multicast domain (MD). One Default-MD exists in every MD whether there is any active source in the respective customer network.

- **LEAF**—Describes the recipient of multicast data. The source is thought of as the route and the destination is the leaf.

- **Multicast domain (MD)**—Collection of MVRFs that can exchange multicast traffic

- **Multicast Virtual Route Forwarding (MVRF)**—Used by a PE router to determine how to forward multicast traffic across an MPLS core.

- **Provider Router (P)**—Router in the core of the provider network that has interfaces only to other P routers and other PE routers

- **Provider Edge Router (PE)**—Router at the edge of the provider network that has interfaces to other P and PE routers and to at least one CE router

- **PIM-SSM**—PIM Source Specific Multicast
MVPN Basic Concepts

The following basic concepts are key to understanding MVPN:

- A service provider has an IP network with its own unique IP multicast domain (P-Network).
- The MVPN customer has an IP network with its own unique IP multicast domain (C-Network).
- The Service Provider MVPN network forwards the customer IP multicast data to remote customer sites. To do so, the service provider encapsulates customer traffic (C-packets) inside P-packets at the service provider PE. The encapsulated P-packet is then forwarded to remote PE sites as native multicast inside the P-Network.
- During the process of forwarding encapsulated P-packets, the P-Network has no knowledge of the C-Network traffic. The PE is the device that participates in both networks. (There may be more than one Customer Network per PE.)

VPN Multicast Routing

A PE router in an MVPN network has several routing tables. There is one global unicast/multicast routing table and a unicast/multicast routing table for each directly connected MVRF.

Multicast domains are based on the principle of encapsulating multicast packets from a VPN in multicast packets to be routed in the core. As multicast is used in the core network, PIM must be configured in the core. PIM-SM, PIM-SSM, and PIM-BIDIR are supported inside the provider core for MVPN. PIM-SM or PIM-SSM is the recommended PIM option in the provider core, because PIM-BIDIR is not supported on all platforms. PIM-SM, PIM-SSM, PIM-BIDIR and PIM-DENSE-MODE are supported inside the MVPN. MVPN leverages Multicast Distribution Trees (MDTs). An MDT is sourced by a PE router and has a multicast destination address. PE routers that have sites for the same MVPN source to a default MDT and join to receive traffic on it.

In addition, a Default-MDT is a tree that is always-on and that transports PIM control-traffic, dense-mode traffic, and rp-tree (*,G) traffic. All PE routers configured with the same default-MDT receive this traffic.

Data MDTs are trees that are created on demand and that will only be joined by the PE routers that have interested receivers for the traffic. Data MDTs can be created either by a traffic rate threshold or a source-group pair. Default-MDTs must have the same group address for all VPN Routing and Forwarding (VRFs) that make up a MVPN. Data MDTs may have the same group address if PIM-SSM is used. If PIM-SM is used, they must have a different group address, because providing the same one could result in the PE router receiving unwanted traffic.

Configuring the Provider Network for MVPN

This section provides an example of how to configure a provider network for MVPN.

The steps required to enable a MVPN in the provider network refer to the topology illustrated in Figure 8-3 on page 8-4. In these steps, the customer VPN is called “ipics.”

**Procedure**

**Step 1** Choose the PIM mode for the provider network.

Cisco recommends PIM-SSM as the protocol in the core. No additional source-discovery BGP configuration is required with the source-discovery attribute. A route distinguisher (RD) type is used to advertise the source of the MDT with the MDT group address. PIM-SM has been the most widely
deployed multicast protocol and has been used for both sparsely and densely populated application requirements. PIM SSM is based upon PIM SM. Without the initial Shared Tree and the subsequent cutover to the Shortest Path Tree, either PIM SSM or PIM SM is suitable for the default MDT.

When bidirectional PIM support becomes available on all relevant hardware, it will be the recommendation for the default MDT. For the Data MDT, either PIM SM or PIM SSM is suitable. PIM SSM is simpler to deploy than PIM SM. It does not require a Rendezvous point, and the Provider network is a known and stable group of multicast devices. Cisco recommends the use of PIM SSM for Provider core deployment. This configuration example uses PIM-SSM in the core.

Step 2  Choose the VPN group addresses used inside the provider network:

The default PIM-SSM range is 232/8. However, this address range is designed for global use in the Internet. For use within a private domain, you should use an address outside of this administratively scoped multicast range (as recommended in RFC2365). Using a private address range makes it simpler to filter on boundary routers. Cisco recommends using 239.232/16, because addresses in this range are easily recognizable as both private addresses and SSM addresses by using 232 in the second octet. In the design discussed in this document, the range is divided for default-MDT and data MDT. (Data MDT is discussed elsewhere in the “VPN Multicast Routing” section on page 8-5. Default-MDTs uses 239.232.0.0-239.232.0.255 and Data MDTs uses 239.232.1.0-239.232.1.255. This address range provides support for up to 255 MVRFs per PE router.

Step 3  Configure the provider network for PIM-SSM.

The following commands enable a basic PIM-SSM service.

- On all P and PE routers, configure these commands globally:

  ```
  ip multicast-routing
  ip pim ssm range multicast_ssm_range
  ip access-list standard multicast_ssm_range
  permit 239.232.0.0 0.0.1.255
  ```

- On all P interfaces and PE interfaces that face the core, configure this command:

  ```
  ip pim sparse-mode
  ```

- On each PE router, configure this command on the loopback interface that is used to source the BGP session:

  ```
  ip pim sparse-mode
  ```

Step 4  Configure the MDT on the VRF.

- To configure multicast routing on the VRF, configure these commands on all PE routers for the VRF ipics:

  ```
  ip vrf ipics
  mdt default 239.232.0.0
  ```

- To enable multicast routing for the VRF, configure this command:

  ```
  ip multicast-routing vrf ipics
  ```

Step 5  Configure the PIM mode inside the VPN.

The PIM mode inside the VPN depends on what type of PIM the VPN customer is using. Cisco provides automatic discovery of the group-mode used inside the VPN via auto-rp or bootstrap router (BSR), which requires no additional configuration. Optionally, a provider may choose to provide the RP for the customer by configuring the PE router as an RP inside the VPN. In the topology discussed in this section, the VPN customer provides the RP service and the PE routers will automatically learn the group-to-rendezvous point (RP) via auto-rp.
Configure all PE-CE interfaces for sparse-dense-mode, which ensures that either auto-rp or BSR messages are received and forwarded, and which allows the PE to learn the group-to-rendezvous point (RP) inside the VPN. To do so, configure the following on all customer facing interfaces:

```
ip pim sparse-mode
```

### Verifying the Provider Network for MVPN

After you complete the configuration as described in the “Configuring the Provider Network for MVPN” section on page 8-5, use the following procedure to verify that the configuration is correct:

#### Procedure

**Step 1** Verify BGP updates.

BGP provides for source discovery when SSM is used, which is known as a BGP-MDT update. To verify that all BGP-MDT updates have been received correctly on the PE routers, take either of these actions:

- Use the `show ip pim mdt bgp` command:

  ```
  PE1#show ip pim mdt bgp
  Peer (Route Distinguisher + IPv4)           Next Hop
  MDT group 239.232.0.0
  2:65019:1:10.32.73.248  10.32.73.248 (PE-2 Loopback)
  2:65019:1:10.32.73.250  10.32.73.250 (PE-3 Loopback)
  ```

  2:65019:1 indicates the RD-type (2) and RD (65019:1) that is associated with this update.

- The remaining output is the address that is used to source the BGP session.

- Use the `show ip bgp vpnv4 all` command:

  ```
  PE1#show ip bgp vpnv4 all
  BGP table version is 204, local router ID is 10.32.73.247
  Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
  r RIB-failure, S Stale
  Origin codes: i - IGP, e - EGP, ? - incomplete
  Network           Next Hop          Metric LocPrf Weight Path
  Route Distinguisher: 65019:1 (default for vrf ipics)
  * i 10.32.72.48/28  10.32.73.248 0 100 0 ?
  ... (output omitted)
  Route Distinguisher: 2:65019:1
  * 10.32.73.247/32  0.0.0.0    0 ?
  * i 10.32.73.248/32 10.32.73.248 0 100 0 ?
  * i 10.32.73.250/32 10.32.73.250 0 100 0 ?
  ```

**Step 2** Verify the global mroute table

Use the `show ip mroute mdt-group-address` command to verify that there is a (Source, Group) entry for each PE router. Because PIM-SSM is used, the source is the loopback address used to source the BGP session and the Group is the MDT address configured. Without traffic, only default-MDT entries are visible.

```
PE1#show ip mroute 239.232.0.0
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
L - Local, P - Pruned, R - RP-bit set, F - Register flag,
T - SPT-bit set, J - Join SPT, M - MSDP created entry,
X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
  ```
U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel
Y - Joined MDT-data group, y - Sending to MDT-data group

Outgoing interface flags: H - Hardware switched
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(10.32.73.247, 239.232.0.0), 1w0d/00:03:26, flags: sTZ
Incoming interface: Loopback0, RPF nbr 0.0.0.0.0
Outgoing interface list:
  FastEthernet0/0, Forward/Sparse, 1w0d/00:02:47

(10.32.73.248, 239.232.0.0), 1w0d/00:02:56, flags: sTIZ
Incoming interface: FastEthernet0/0, RPF nbr 10.32.73.2
Outgoing interface list:
  MVRF ipics, Forward/Sparse, 1w0d/00:01:30

(10.32.73.250, 239.232.0.0), 1w0d/00:02:55, flags: sTIZ
Incoming interface: FastEthernet0/0, RPF nbr 10.32.73.2
Outgoing interface list:
  MVRF ipics, Forward/Sparse, 1w0d/00:01:29

Verify that the s flag is set on each (S,G) entry, which indicates that this group is used in ssm mode.
Verify that the z flag is set, which indicates that this PE router is a leaf of the multicast tunnel. When the
router is a leaf of a multicast tunnel, it has to do additional lookups to determine which MVRF to forward
this traffic to, as it is basically a receiver for this traffic. Verify the I flag is set for the remote PE(S,G)
entry. This flag indicates that the router understands it is joining an SSM group. It is as though an
IGMPv3 host had requested to join that particular channel.

Step 3
Verify PIM neighbors in the global table.

Use the `show ip pim neighbors` command on all PE and P routers to verify that the pim neighbors are
setup properly in the global table.

```
PE1#show ip pim neighbor
PIM Neighbor Table
Neighbor Address  Interface  Uptime/Expires  Ver  DR Prio/Mode
10.32.73.2 FastEthernet0/0 1w4d/00:01:21  v2  1 / DR
10.32.73.70 Serial0/2 1w4d/00:01:29  v2  1 / S
```

Step 4
Verify PIM neighbors inside the VPN

Use the `show ip pim vrf ipics neighbors` command on all PE routers to verify that the CE router is seen
as a PIM neighbor and that the remote-PE routers are seen as pim neighbors over the tunnel.

```
PE1#show ip pim vrf ipics neighbor
PIM Neighbor Table
Neighbor Address  Interface  Uptime/Expires  Ver  DR Prio/Mode
10.32.73.66 Serial0/0 1w3d/00:01:18  v2  1 / S
10.32.73.248 Tunnel0 3d17h/00:01:43  v2  1 / S
10.32.73.250 Tunnel0 1w0d/00:01:42  v2  1 / DR S
```

Step 5
Verify the VPN group-to-rendezvous point (RP).

The main customer site has been configured to use auto-rp within the VPN. VPN IPICS is using the
multicast range 239.192.21.64 - 79 for channels and VTGs.

```
ip pim send-rp-announce Loopback0 scope 16 group-list multicast_range
ip pim send-rp-discovery scope 16
ip access-list standard multicast_range
  permit 239.192.21.64 0.0.0.15
```
Use the `show ip pim vrf ipics rp mapping` command to verify that the PE router correctly learned the RP mapping information from the VPN.

```
PE1#show ip pim vrf ipics rp map
PIM Group-to-RP Mappings
Group(s) 239.192.21.64/28
   RP 10.32.72.248 (?), v2v1
      Info source: 10.32.73.62 (?), elected via Auto-RP
      Uptime: 1w3d, expires: 00:02:54
```

This output shows that the PE router has correctly learned the group-to-rendezvous point (RP), which is used inside the VPN. The default-MDT reaches all PE routers in the core of the provider network in which the multicast replication is performed. With only a default-MDT configured, traffic goes to all PE routers, regardless of whether they want to receive the traffic.

---

**Optimizing Traffic Forwarding: Data MDT**

Data MDT is designed to optimize traffic forwarding. Data MDT is a multicast tree that is constructed on demand. The conditions to create a data MDT are based upon traffic-load threshold measured in kbps or on an access-list that specifies certain sources inside the VPN. A data MDT is created only by the PE that has the source connected to its site. The data MDT conditions do not have to be configured. However, when there are no conditions set for each (S,G) inside the VPN, a data MDT is created. This data MDT requires resources from the router, so it is recommended that you not create one just because a source exists. A non-zero threshold is recommended, because this value requires an active source to trigger the creation of the Data MDT. The maximum number of multi-VPN Routing/Forwarding (MVRF) entries is 256.

To configure the data MDT under the VRF, use one of the ranges that is described in Step 2 in the “Configuring the Provider Network for MVPN” section on page 8-5. A maximum of 256 addresses is allowed per VRF. This limitation is an implementation choice, not a protocol limitation. Because SSM is used, the data MDT address-range may be the same on all PE routers for the same VPN. Use an inverse-mask to specify the number of addresses used for the data MDT, as shown in the following command:

```
ip vrf ipics
   mdt data 239.232.1.0 0.0.0.255 threshold 1
```

---

**Verifying Correct Data MDT Operation**

Data MDTs create mroute entries in the global table. There also are specific commands for verifying functionality of the sending and receiving PE router. To verify the data MDT operation, there must be multicast traffic between sites that exceeds the configured threshold. An easy way to test the data MDT is to statically join a multicast group in one site and then ping that group from another site, as shown in the following example:

```
CE1
   interface Loopback0
   ip address 10.32.72.248 255.255.255.255
   ip pim sparse-mode
   ip igmp join-group 239.192.21.68

CE2
   ping 239.192.21.68 size 500 repeat 100
```
To verify the data MDT operation, perform the following procedure:

**Step 1** Verify the sending PE router.

Use the `show ip pim vrf ipics mdt send` command on the sending PE router (PE2) to verify the setup of a data mdt.

```
PE2#show ip pim vrf ipics mdt send
MDT-data send list for VRF: ipics
   (source, group)       MDT-data group     ref_count
   (10.32.72.244, 239.192.21.68)  239.232.1.0     1
   (10.32.73.74, 239.192.21.68)  239.232.1.1     1
```

**Step 2** Verify the receiving PE router.

Use the `show ip pim vrf ipics mdt receive detail` command on the receiving PE (PE1) router to verify that this router is receiving on a data mdt.

```
PE1#show ip pim vrf ipics mdt receive
Joined MDT-data [group : source] for VRF: ipics
   [239.232.1.0 : 10.32.73.248] ref_count: 1
   [239.232.1.1 : 10.32.73.248] ref_count: 1
```

At this point, if everything is correctly configured, the sites in VPN IPICS can transfer multicast traffic by using the MPVN and all sites are now in the same multicast domain. Therefore, all channels and users on the Cisco IPICS server can be configured with the same location.

---

**Multicast Islands**

A multicast island is a site in which multicast is enabled. A multi-site deployment can consist of several multicast islands that connect to each other over unicast-only connections. See Figure 8-4.

*Figure 8-4  Multicast Islands*
Multicast over GRE

Multicast of GRE provides multicast support between islands. This section provides an overview of how to configure multicast over GRE. Figure 8-5 illustrates a Cisco IPICS deployment with multicast over GRE.

Figure 8-5  Multicast over a GRE Tunnel

A tunnel is configured between the gateway in Site 1 and the gateway in Site 2, which is sourced with their respective loopback0 interfaces. The `ip pim sparse-dense mode` command is configured on tunnel interfaces and multicast routing is enabled on the gateway routers. Sparse-dense mode configuration on the tunnel interfaces allows sparse-mode or dense-mode packets to be forwarded over the tunnel depending on the RP configuration for the group.

The following examples show the configuration that is required to implement multicast over GRE between Site 1 and Site 2. Use the same approach between Site 1 and Site 3, and between Sites 2 and Site 3

```
interface loopback 0
  ip address 1.1.1.1 255.255.255.255

interface Tunnel0
  ip address 192.168.3.1 255.255.255.252
  ip pim sparse-mode
  tunnel source Loopback0
  tunnel destination 2.2.2.2

Site 2

ip multicast-routing

interface loopback 0
  ip address 2.2.2.2 255.255.255.255

interface Tunnel0
  ip address 192.168.3.2 255.255.255.252
  ip pim sparse-mode
  tunnel source Loopback0
```
When you configure PIM sparse mode over a tunnel, make sure to follow these guidelines:

- For successful RPF verification of multicast traffic flowing over the shared tree (*,G) from the RP, configure the `ip mroute rp-address nexthop` command for the RP address, pointing to the tunnel interface.

  For example, assume that Site 1 has the RP (RP address 10.1.1.254). In this case, the mroute on the gateway in Site 2 would be the `ip mroute 10.1.1.254 255.255.255.255 tunnel 0` command, which ensures a successful RPF check for traffic flowing over the shared tree.

- For successful RPF verification of multicast (S,G) traffic flowing over the Shortest Path Tree (SPT), configure the `ip mroute source-address nexthop` command for the multicast sources, pointing to the tunnel interface on each gateway router.

  In this case, when SPT traffic flows over the tunnel interface, an `ip mroute 10.1.1.0 255.255.255.0 tunnel 0` command is configured on the Site 2 gateway and `ip mroute 10.1.2.0 255.255.255.0 tunnel 0` command is configured on the Site 1 gateway. This configuration ensures successful RPF verification for incoming multicast packets over the Tu0 interface.

### Bandwidth Considerations when using Multicast over GRE

Cisco IPICS can operate with either the G.711 or the G.729 codec. Table 8-1 lists the bandwidth requirements for a voice call over unicast connection trunks, based on the codec used, the payload size, and whether cRTP, VAD, or both are configured.

<table>
<thead>
<tr>
<th>Compression Technique</th>
<th>Payload Size (Bytes)</th>
<th>Full Rate Bandwidth (kbps)</th>
<th>Bandwidth with cRTP (kbps)</th>
<th>Bandwidth with VAD (kbps)</th>
<th>Bandwidth with cRTP and VAD (kbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.711</td>
<td>240</td>
<td>76</td>
<td>66</td>
<td>50</td>
<td>43</td>
</tr>
<tr>
<td>G.711</td>
<td>160</td>
<td>83</td>
<td>68</td>
<td>54</td>
<td>44</td>
</tr>
<tr>
<td>G.729</td>
<td>40</td>
<td>17.2</td>
<td>9.6</td>
<td>11.2</td>
<td>6.3</td>
</tr>
<tr>
<td>G.729</td>
<td>29</td>
<td>26.4</td>
<td>11.2</td>
<td>17.2</td>
<td>7.3</td>
</tr>
</tbody>
</table>

Bandwidth consumption across a tunnel depends on the number of active channels and VTG users that are communicating between the sites.

The following cases are examples how to calculate bandwidth use across a tunnel.

**Case 1: Active channel in Site 1 and Site 2.**

All users in Site 1 are using one channel, and all users in Site 2 are using another channel. No multicast voice flows across the tunnel.

**Case 2: Active channel has n users in site 1 and m users in site 2.**

In the following example, Call bandwidth is the bandwidth value from Table 5-2 on page 5-6.

\[
\text{Bandwidth 1} = \text{Call bandwidth} \times n \text{ (Flow from site 1 to site 2)}
\]

\[
\text{Bandwidth 2} = \text{Call bandwidth} \times m \text{ (Flow from site 2 to site 1)}
\]

\[
\text{Total bandwidth} = \text{Bandwidth 1} + \text{Bandwidth 2}
\]

(Call bandwidth is the value from Table 3-1.)
Depending on the number of active channels, the number of active users per channel, and whether the channel spans multiple sites, the bandwidth usage could be significant.

**IPSec VPNs**

IPSec VPNs can be implemented over multicast GRE tunnels. See Figure 8-6.

![Figure 8-6 IPSec over Multicast GRE Tunnels](image)

There are a number of ways to configure IPSec over GRE tunnels. Refer to the appropriate Cisco documentation.

**Multicast Singularities**

A multicast singularity is a restrictive case of the multicast island scenario. Between sites, multicast routing is not enabled. Within a site, multicast is enabled only on Cisco IPICS specific devices: UMS, LMR gateways, and Cisco Unified IP Phones. These Cisco IPICS devices reside in a multicast singularity, as shown in Figure 8-7.
The singularities can be connected by using multicast over GRE tunnels (as shown in Figure 8-8).
The configuration of a multicast over GRE tunnel is identical to the multicast island scenario except the tunnel must be configured between the routers and not the gateway routers because the gateway routers are not enabled for multicast.

The following rules apply to a multicast singularity:

1. All UMSs and LMR gateways must reside in a multicast singularity. That is, these devices must be on directly connected multicast enabled LANs.
2. All users within the multicast singularity can use a Cisco Unified IP Phone because they are in the multicast enabled zone.
3. Users outside the multicast singularity can use the mobile client.
4. Users outside the multicast singularity cannot use the Cisco Unified IP Phone because this device supports only multicast.

It would be possible to have multiple multicast singularities within the same site and the singularities could be connected with multicast over GRE tunnels. This solution depends on the policies of the organization.

**VPN Termination for Mobile Clients**

Cisco IPICS Mobile Clients expand the types of devices that can access the network and provide access to the network from virtually anywhere on the Internet.

For information about the ports and transport protocols that Cisco IPICS mobile clients, see Table 2-2 on page 2-24.
In a secure campus network, mobile clients work over WiFi. As the network expands and access shifts to 3G/4G and LTE, an additional level of protection is required. Cisco offers that protection by using the Cisco AnyConnect Mobile VPN Client and Cisco Adaptive Security Appliance (ASA) platforms to create a VPN tunnel between the endpoints and Cisco IPICS.

The VPN tunnel encapsulates and encrypts the traffic and provides the added advantage of overcoming issues with NAT traversal through the carrier network. A Cisco IPICS session that runs over a VPN tunnel is viewed by the service provider as a data call, not a voice call, because the tunneled payload is a data service running on the mobile client.
| **A** | **action** | A discrete function that is performed through a policy. Discrete functions include activate VTG, notification, VTG add participant, dial-out, and invite to VTG. |
| **activate VTG** | An action that activates a preconfigured VTG; can also specify a duration. At the end of the specified duration, the VTG is deactivated. If no duration is specified, the VTG must be manually deactivated by the dispatcher from the VTG Management drawer in the Cisco IPICS administration console. |
| **activated** | A state that indicates that the SIP (unicast) or multicast channel is fully operational. |
| **active virtual talk group** | A virtual talk group (VTG) becomes active when Cisco IPICS commits global resources, such as a multicast address and any necessary dial-in peers, so that the participants in the VTG can communicate with each other. |
| **Administration Console** | The graphical user interface (GUI) in the Cisco IPICS server software through which authorized Cisco IPICS users can manage and configure Cisco IPICS resources, events and VTGs. |
| **autonomous system** | A radio system under one administrative control; also known as a management domain. This system is usually mapped to an agency. |
| **B** | **backward compatibility** | The ability of newer radio equipment to operate within an older system infrastructure or to directly intercommunicate with an older radio unit. The term usually applies to digital radios that are also capable of analog signal transmission. |
| **bandwidth** | The difference between the highest and lowest frequencies that are available for network signals. The term also describes the rated throughput capacity of a specific network medium or protocol. Bandwidth specifies the frequency range that is necessary to convey a signal measured in units of hertz (Hz). For example, voice signals typically require approximately 7 kHz of bandwidth and data traffic typically requires approximately 50 kHz of bandwidth. |
| **base station** | A land station in the land mobile radio service. In the personal communication service, the common name for all the radio equipment that is located at one fixed location and used for serving one or several calls. |
call
Radio terminology that defines a call as beginning at the moment that you press the transmit key and concluding when you release the transmit key. The term “per call” implies that some form of control causes the radio to select a specific frequency before it transmits audio. Some radios may be configured to automatically return to a predefined RF channel when the call ends.

call delay
The delay that occurs when there is no idle channel or facility available to immediately process a call that arrives at an automatic switching device.

call setup time
The time that is required to establish a circuit-switched call between users or terminals.

carrier
A wave that is suitable for modulation by an information-bearing signal.

CAS
Channel associated signaling. The transmission of signaling information within the voice channel. CAS signaling often is referred to as robbed-bit signaling because user bandwidth is being robbed by the network for other purposes.

channel
A communication path that is wide enough to permit a single RF transmission. Multiple channels can be multiplexed over a single cable in certain environments. There are many different types of channels in Cisco IPICS, including direct dial, 2-way, VTGs, and radio channels. Channels can be dynamically or statically allocated. Channels may have one or more channel connections that define the source for the channel. See PTT channel.

channel capacity
The maximum possible information transfer rate through a channel, subject to specified constraints.

channel connection
One or more methods by which a content stream can be obtained. For instance, a particular channel may be found on several different multicast addresses in different locations and also on several different radios at different locations.

channel group
A logical grouping of channels

channel spacing
The distance from the center of one channel to the center of the next-adjacent-channel. Typically measured in kilohertz.

Cisco Unified Communications Manager (CallManager)
The software-based call-processing component of the Cisco IP telephony solution. Cisco Unified Communications Manager (CallManager) extends enterprise telephony features and functions to packet telephony network devices, such as Cisco Unified IP Phones, media processing devices, VoIP gateways, and multimedia applications.

Cisco IPICS
Cisco IP Interoperability and Collaboration System. The Cisco IPICS system provides an IP standards-based solution for voice interoperability by interconnecting voice channels, talk groups, and VTGs to bridge communications amongst disparate systems.

Cisco IPICS policy engine
Integrated with the Cisco IPICS server, this component enables telephony dial functionality and is responsible for the management and execution of policies and user notifications.

Cisco IPICS server
Provides the core functionality of the Cisco IPICS system. The Cisco IPICS server software runs on the Linux operating system on selected servers. The server software includes an incident management framework administration GUI that enables dynamic resource management for users, channels, and VTGs. The server also includes the Cisco IPICS policy engine, which enables telephony dial functionality and is responsible for the management and execution of policies and user notifications.
<table>
<thead>
<tr>
<th><strong>Cisco Unified IP Phone</strong></th>
<th>A full-featured telephone that provides voice communication over an IP network. A user can participate in a PTT channel or VTG by using a Cisco Unified IP Phone as a PTT device.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CLI</strong></td>
<td>command-line interface. An interface that allows the user to interact with the operating system by entering commands and optional arguments.</td>
</tr>
</tbody>
</table>
| **codec**                | coder-decoder.  
1. Integrated circuit device that typically uses pulse code modulation to transform analog signals into a digital bit stream and digital signals back into analog signals.  
2. In Voice over IP, Voice over Frame Relay, and Voice over ATM, a DSP software algorithm that is used to compress/decompress speech or audio signals. |
| **conference of conferences** | A conference that consists of two or more VTGs. |
| **conventional radio system** | A non-trunked system that is similar to telephone party-line in that the user determines availability by listening for an open channel. |
| **COR**                  | carrier operated relay. An electrical signal that is used to signal when a radio is receiving traffic. |
| **coverage**             | In radio communications, the geographical area that is within the range of, or that is covered by, a wireless radio system to enable service for radio communications. Also referred to as service delivery area. |
| **D**                    | delay time  
The sum of waiting time and service time in a queue. |
|                          | decrypt  
Cryptographically restore ciphertext to the plaintext form it had before encryption. |
|                          | decryption  
Reverse application of an encryption algorithm to encrypted data, thereby restoring that data to its original, unencrypted state. |
|                          | dial engine scripts  
Scripts that the Cisco IPICS dial engine executes to provide the telephony user interface (TUI) for interaction with incoming and outgoing phone calls. |
|                          | dial-in  
A phone call that is dialed in to the policy engine. |
|                          | dial-in floor control  
A feature that allows one dial-in user, at a time, to talk in a VTG or a channel. The telephony user interface provides this dial-in floor control feature to support dial-in users. It does not provide support for floor control for other PTT users. |
|                          | dial number  
The phone number that is used by the policy engine and the SIP provider and configured in the Dial Information pane in the Ops Views window. Dialing this number provides user access to the telephony user interface. |
|                          | dial out invite  
An action that invites selected user(s) to the selected VTG.  
A phone call that is dialed out by the policy engine to a phone user to invite the user in to a talk group. |
|                          | dial peer  
Addressable call endpoint. In Voice over IP, there are two kinds of dial peers: POTS and VoIP. |
**digit ID**
A numeric identifier that is chosen by a Cisco IPICS user and stored in the user profile. Cisco IPICS uses this ID and a numeric password to authenticate a Cisco Unified IP Phone user.

**digital modulation technique**
A technique for placing a digital data sequence on a carrier signal for subsequent transmission through a channel.

**discrete tone**
Any tone that is sent without any summed or added tone. For example, adding a function tone with a low level guard tone may impact the recognition of the function tone. Contrast with mixed tones.

**dispatcher**
The Cisco IPICS dispatcher is responsible for setting up the VTGs, activating the VTGs to begin conferences, and adding and/or removing participants in inactive VTG and active VTGs. The dispatcher also monitors the active VTGs and events, can mute and unmute IDC users, as necessary, and manages policies, which activate/deactivate VTGs based on specific criteria and designated intervals. Policy management activities include create/modify/delete policies, view policies, execute policies, and activate privileges.

**DS0**
digital service zero (0). Single timeslot on a DS1 (also known as T1) digital interface—that is, a 64-kbps, synchronous, full-duplex data channel, typically used for a single voice connection on a PBX.

**DTMF**
dual tone multi-frequency. The signal to the phone company that you generate when you press keys on a telephone keypad. With DTMF, each key that you press on your phone (0 through 9, ‘*’ and ‘#’) generates two tones of specific frequencies; one tone is generated from a high frequency group of tones and the other from a low frequency group. Voice gateways often strip these inband tones and present them out-of-band in SIP, H.323, or other messages.

**dynamic radio channel (dynamic control)**
The controls that are used to preset radio characteristics so that channels are available to clients.

**dynamic regrouping**
A trunking system feature that allows multiple radios to be placed upon a specific talk group without manual manipulation of the programming of the radios. Dynamic regrouping is initiated through a system control console and transmitted to the radio via the trunking systems control channel.

**E & M**
recEive and transMit (or ear and mouth). As the analog interface between a radio and the LMR gateway, the E&M interface provides voice signals from radio channels, which are then mapped to IP multicast or unicast. The E&M interface provides the most common form of analog trunking.

1. Trunking arrangement that is generally used for two-way switch-to-switch or switch-to-network connections. Cisco's analog E&M interface is an RJ-48 connector that allows connections to PBX trunk lines (tie lines). E&M also is available on E1 and T1 digital interfaces.

2. A type of signaling that is traditionally used in the telecommunications industry. Indicates the use of a handset that corresponds to the ear (receiving) and mouth (transmitting) component of a telephone.

**e-lead**
The ear portion of the E & M interface. The e-lead is the receive path of the LMR gateway.

**encipher**
To convert plain text into an unintelligible form by using a cipher.

**encode**
To modify information into the required transmission format.
encryption  
Application of a specific algorithm so as to alter the appearance of data and make it incomprehensible to unauthorized users.

event  
An active VTG in the Cisco IPICS solution.

F

FDM  
frequency-division multiplexing. Technique whereby information from multiple channels can be allocated bandwidth on a single wire based on frequency.

FDMA  
frequency-division multiple access. A channel access method in which different conversations are separated onto different frequencies. FDMA is employed in narrowest bandwidth and multiple-licensed channel operations.

FLEXlm  
Cisco software that enforces licensing on certain systems; FLEXlm ensures that Cisco IPICS software will work only on the supported and licensed hardware.

floor control  
The standard mechanism for Push-to-Talk speaker arbitration.

frame  
A logical grouping of information sent as a data link layer unit over a transmission medium. Often refers to the header and the trailer, used for synchronization and error control, that surround the user data contained in the unit. The terms cell, datagram, message, packet, and segment also describe logical information groupings at various layers of the OSI reference model.

frequency  
For a periodic function, frequency represents the number of cycles or events per unit of time. Frequency is used in several different contexts. For example, transmission frequency (the band on which the radio sends signals) or the frequency of an audible signal measured in hertz (Hz). All tone control operations require audible tones that fall within a narrow band of a specific frequency and at a specific volume (amplitude).

frequency assignment  
Assignment that is given to a radio station to use a radio frequency or radio frequency channel under specified conditions.

frequency hopping  
The repeated switching of frequencies during radio transmission according to a specified algorithm, intended to minimize unauthorized interception or jamming of telecommunications.

frequency modulation  
Modulation technique in which signals of different frequencies represent different data values.

frequency sharing  
The assignment to or use of the same radio frequency by two or more stations that are separated geographically or that use the frequency at different times.

function tone  
A tone that follows the high level guard tone and causes the radio to perform a specific function, such as selecting a new transmit frequency. Function tones are often referred to as F1, F2, F3, and so on. See preamble and high level guard tone.
gateway

Device that performs an application-layer conversion of information from one protocol stack to another. In Cisco IPICS, the gateway component includes LMR gateways, which functionality is usually installed as an additional feature in a supported Cisco router. LMR gateways provide voice interoperability between radio and non-radio networks by bridging radio frequencies to IP multicast streams.

GRE

generic routing encapsulation. Tunneling protocol that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork. By connecting multiprotocol subnetworks in a single-protocol backbone environment, IP tunneling that uses GRE allows network expansion across a single-protocol backbone environment. GRE is generally used to route multicast traffic between routers.

guard tone

The most common guard tones are the high level guard tone (HLGT) and the low level guard tone (LLGT). The HLGT is used to alert the radio that a function tone follows. The LLGT is used as a hold tone or keying tone. See tone keyed.

H

H.323

Defines a common set of codecs, call setup and negotiating procedures, and basic data transport methods to allow dissimilar communication devices to communicate with each other by using a standardized communication protocol.

high-band frequency

Refers to the higher frequency levels in the VHF band, typically 138-222 MHz.

HLGT

high level guard done. Also known as awake tone. This tone is set at high volume and is usually the first tone in a preamble. It is used to alert the radio that another tone, usually a function tone, will follow. See guard tone.

Hoot 'n' Holler (Hootie)

A communications system where the loudest and most recent talker or talkers are mixed into one multicast output stream. Also known as hootie, these networks provide “always on” multiuser conferences without requiring that users dial in to a conference.

Cisco enables the Cisco Hoot 'n' Holler feature in specific Cisco IOS versions.

I

idle tone

The tone that a radio may deliver on the m-lead to signal the LMR gateway that there is no incoming traffic. When the idle tone is removed, the LMR gateway deems all signals to be valid voice traffic.

inband

Traffic that is sent inband is included in the same stream as the real-time traffic protocol (RTP). Inband signals can be encoded signals and RFC 2833 signals.

incident

An event that you create in the IDC and for which various users can coordinate responses by using the IDC.

incident VTG

A temporary talk group for an incident.
**informix linux group**

Members of this group have full permission to Cisco IPICS server folders, files, and scripts that are related to the Informix database application. Members of this group include the informix and ipicsdba users.

**informix user ID**

The Cisco IPICS Linux user that belongs to both the informix linux group, which includes full permission to the Cisco IPICS database server folders, files, and scripts, and the ipics linux group, which includes permission to Cisco IPICS application-related folders, files, and scripts. In addition, this user has full administrative permission to the Informix database instance. Cisco IPICS creates this Linux system user ID and generates the password during the software installation process. The password for this user ID never expires.

To access the informix user, log in to the Cisco IPICS server by using the root user ID; then, enter `su - informix` (superuser from root).

**interference**

The effect of unwanted energy due to one or a combination of emissions, radiation, or inductions upon reception in a radio communication system, manifested by any performance degradation, misinterpretation, or loss of information, which could be extracted in the absence of such unwanted energy.

**interoperability**

The capability of equipment manufactured by different vendors to communicate with each other successfully over a network.

**invitation policy**

A policy that can be invoked only through the telephony user interface and can include only the invite to VTG action. After joining a talk group, a user can access the breakout menu and invoke invitation policies. The talk group that this user has joined is the talk group that the invited users join.

**invite to VTG**

A version of the dial out invite action where users to be invited are preconfigured but the VTG that they are invited to depends on which VTG the invoker of the policy is dialed into.

**ipicsadmin user ID**

The Cisco IPICS Linux user that, as part of the ipics linux group, has full permission to the Cisco IPICS server folders, files, and scripts that are related to the Cisco IPICS application and database backup and restore operations. In addition, the ipicsadmin user has permission to read and write data from and/or to the Informix database. Cisco IPICS creates this Linux system user ID during the software installation process. The password for this user ID never expires.

To access the ipicsadmin user, log in to the Cisco IPICS server by using the root user ID; then, enter `su - ipicsadmin` (superuser from root).

**ipicsdba user ID**

The Cisco IPICS Linux user that belongs to both the informix linux group, which includes full permission to the Cisco IPICS database server folders, files, and scripts, and the ipics linux group, which includes permission to Cisco IPICS application-related folders, files, and scripts. In addition, the ipicsdba user has permission to read data, write data, create tables, and create databases in the Informix database instance. Cisco IPICS creates this Linux system user ID and generates the password during the software installation process. The password for this user ID never expires.

To access the ipicsdba user, log in to the Cisco IPICS server by using the root user ID; then, enter `su - ipicsdba` (superuser from root).

**ipics linux group**

Members of this group have full permission to Cisco IPICS server folders, files, and scripts that are related to the Cisco IPICS application and database backup and restore operations. Members of this group include the ipicsadmin, ipicsdba, and informix users.
ipics user ID

The Cisco IPICS application-level user ID that can perform all administration-related tasks via the Cisco IPICS Administration Console. Cisco IPICS creates this web-based user ID during the software installation process.

IPSec

IP Security. A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer. IPSec uses IKE to handle the negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPSec. IPSec can protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

K

keepalive

A message that is sent by one network device to inform another network device that the virtual circuit between the two devices is still active.

key

The parameter that defines an encryption code or method.

Key (a radio) causes the radio to transmit. See tone keyed.

kilohertz (kHz)

A unit of frequency that denotes one thousand Hz.

L

linear modulation

A radio frequency transmission technique that provides the physical transport layer of a radio system. This technology is compatible in digital and analog system environments and supports channel bandwidths of 5 kHz to 50 kHz.

LLGT

low level guard tone. This tone is used as a hold tone or keying tone. See guard tone.

LMR

Land Mobile Radio. A Land Mobile Radio (LMR) system is a collection of portable and stationary radio units that are designed to communicate with each other over predefined frequencies. They are deployed wherever organizations need to have instant communication between geographically dispersed and mobile personnel.

This term is often used interchangeably between a handheld or vehicle-mounted device and a stationary transmitter. Stationary devices are typically referred to as base stations.

Cisco IPICS leverages the Cisco Hoot ‘n’ Holler feature, which is enabled in specific Cisco IOS versions, to provide radio integration into the Cisco IPICS solution. LMR is integrated by providing an ear and mouth (E&M) interface to a radio or other PTT devices, such as Nextel phones. Configured as a voice port, this interface provides the appropriate electrical interface to the radio. You configure this voice port with a connection trunk entry that corresponds to a voip dial peer, which in turn associates the connection to a multicast address. This configuration allows you to configure a corresponding channel in Cisco IPICS, using the same multicast address, which enables Cisco IPICS to provide communication paths between the desired endpoints.

LMR gateway

Land Mobile Radio gateway. Refers to the router E&M interface that converts IP traffic from digital to analog for use by radios.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>location</td>
<td>In Cisco IPICS, location signifies reachability; meaning, channels or users who are associated with the same location can communicate with each other without additional network configuration. Location may refer to a physical or virtual location, as defined in the server.</td>
</tr>
<tr>
<td>low-band frequency</td>
<td>Lower frequency levels in the VHF band, typically 25–50 MHz.</td>
</tr>
<tr>
<td>M</td>
<td></td>
</tr>
<tr>
<td>megahertz (MHz)</td>
<td>A unit of frequency denoting one million Hz.</td>
</tr>
<tr>
<td>mixed tone</td>
<td>Two tones that are mixed together. DTMF is an example of a mixed tone. To be transmitted properly, tone signals must be mixed with the LLGT. See DTMF.</td>
</tr>
<tr>
<td>m-lead</td>
<td>The mouth portion of the E&amp;M interface. The m-lead is the transmit path of the LMR gateway.</td>
</tr>
<tr>
<td>modulation</td>
<td>The process, or result of the process, of varying a characteristic of a carrier in accordance with an information-bearing signal.</td>
</tr>
<tr>
<td>multicast</td>
<td>Single packets that are copied by the network and sent to a specific subset of network addresses. Multicast refers to communications that are sent between a single sender and multiple recipients on a network.</td>
</tr>
<tr>
<td>multicast address</td>
<td>A single address that may refer to multiple network devices.</td>
</tr>
<tr>
<td>multicast address/port</td>
<td>Cisco IPICS uses this type of connection to enable the IDC to directly tune in to the multicast channel. MULTICAST ADDRESS/PORT combinations are also used by gateways and UMS components.</td>
</tr>
<tr>
<td>multicast pool</td>
<td>Multicast IP addresses that are defined as part of a multicast pool. Cisco IPICS allocates a multicast address from this pool of resources when a dispatcher activates a VTG.</td>
</tr>
<tr>
<td>multiplexing</td>
<td>The combination of two or more information channels on to a common transmission medium. In electrical communications, the two basic forms of multiplexing are time-division multiplexing (TDM) and frequency-division multiplexing (FDM).</td>
</tr>
<tr>
<td>multipurpose policy</td>
<td>A policy that can include any of the supported actions; may be invoked through the telephony user interface or the Cisco IPICS administration console.</td>
</tr>
<tr>
<td>mutual aid channel</td>
<td>A national or regional channel that has been set aside for use only in mutual aid interoperability situations. Restrictions and guidelines governing usage usually apply.</td>
</tr>
<tr>
<td>N</td>
<td></td>
</tr>
<tr>
<td>narrowband channels</td>
<td>Channels that occupy less than 20 kHz.</td>
</tr>
<tr>
<td>National Public Safety Planning Advisory Committee</td>
<td>The committee that was established to conduct nationwide planning and allocation for the 821–824 MHz and 866–869 MHz bands.</td>
</tr>
</tbody>
</table>
**National Telecommunication and Information Administration**
The United States executive branch agency that serves as the principal advisor to the president on telecommunications and information policies and that is responsible for managing the federal government’s use of the radio spectrum.

**near end**
The device or devices that are physically connected to the Ethernet or an RS-232 link. Compare with far end, which refers to devices on the other side of the broadcast. A base station that is connected to an LMR gateway is a near end device while a handheld radio that receives over-the-air signals from the base station is a far end device.

**network**
An interconnection of communications entities.

**NAT**
Network Address Translation. Provides a mechanism for translating addresses that are not globally unique into globally routable addresses for connection to the Internet.

**not activated**
A VTG state that becomes effective when the Activate button is clicked a second time (to deactivate the channel) or if the connection terminates. No IDC buttons appear highlighted.

**notification**
An action that notifies selected user(s) via email, SMS, pager, or phone. The necessary IDs and phone numbers are configured in the communication preferences for each user. Notifications that are sent via the phone require user authentication before the notification prompt is heard.

An email, SMS, pager, or phone call that is placed to a user for the purpose of sending a notification message.

**O**

**operator**
The Cisco IPICS operator is responsible for setting up and managing users, configuring access privileges, and assigning user roles and ops views.

**ops view**
operational view. A Cisco IPICS feature that provides the ability to organize users, user groups, channels, channel groups, VTGs, and policies into different user-definable views across multiple organizations or agencies that normally would not share resources. While ops views are maintained separately by the Cisco IPICS system administrator and/or ops view administrator, this functionality also allows multiple entities to use one Cisco IPICS server to enable resource sharing across multiple ops views, according to business need.

**ops view administrator**
The ops view administrator capabilities include managing and monitoring the activity logs that are filtered by ops views and accessible in the Administration Console (*Administration > Activity Log Management*) window.

**OTAR**
over-the-air re-keying. Provides the ability to update or modify over radio frequency the encryption keys that are programmed in a mobile or portable radio.

**P**

**packet**
A logical grouping of information that includes a header that contains control information. Usually also includes user data.
packet switching: The process of routing and transferring data by using addressed packets so that a channel is occupied during the transmission of the packet only. Upon completion of the transmission, the channel is made available for the transfer of other traffic.

PIM: Protocol Independent Multicast. Multicast routing architecture that allows the addition of IP multicast routing on existing IP networks. PIM is unicast routing protocol independent and can be operated in two modes: PIM dense mode and PIM sparse mode.

PIM dense mode: One of the two PIM operational modes. PIM dense mode is data-driven and resembles typical multicast routing protocols. Packets are forwarded on all outgoing interfaces until pruning and truncation occurs. In dense mode, receivers are densely populated, and it is assumed that the downstream networks want to receive and will probably use the datagrams that are forwarded to them. The cost of using dense mode is its default flooding behavior. Sometimes called dense mode PIM or PIM DM.

PIM sparse mode: One of the two PIM operational modes. PIM sparse mode tries to constrain data distribution so that a minimal number of routers in the network receive it. Packets are sent only if they are explicitly requested at the RP (rendezvous point). In sparse mode, receivers are widely distributed, and the assumption is that downstream networks will not necessarily use the datagrams that are sent to them. The cost of using sparse mode is its reliance on the periodic refreshing of explicit join messages and its need for RPs. Sometimes called sparse mode PIM or PIM SM.

policy: Policies include one or more actions that execute sequentially and can be manually activated via the Cisco IPICS administration console or the telephony user interface. Cisco IPICS provides support for multiple policy types.

policy execution status: An indicator of policy execution success or failure. The Cisco IPICS administration console provides a status for each action under a policy.

portalization: A web programming paradigm for customizing the interface and functionality of a client application.

preamble: The sequence of tones that precede a transmission. The preamble generally includes the HLGT and the function tone.

protocol: A set of unique rules that specify a sequence of actions that are necessary to perform a communications function.

PTT: Push-to-talk. A signal to a radio transmitter that causes the transmission of radio frequency energy. The action that keys a radio or causes the radio to transmit. On the Cisco router, the e-lead, or key tone, is used to signal the radio to transmit.

PTT channel: A channel consists of a single unidirectional or bidirectional path for sending and/or receiving signals. In the Cisco IPICS solution, a channel represents one LMR gateway port that maps to a conventional radio physical radio frequency (RF) channel.

PTT channel button: The button on the IDC that you click with your mouse, or push, and hold to talk. You can use the latch functionality on this button to talk on one or more channels at the same time.

PTT channel group: A logical grouping of available PTT channels that can be used for categorization.
QoS

Quality of service. A measurement of performance for a transmission system, including transmission quality and service availability.

Queue

Represents a set of items that are arranged in sequence. Queues are used to store events occurring at random times and to service them according to a prescribed discipline that may be fixed or adaptive.

Queuing delay

In a radio communication system, the queuing delay specifies the time between the completion of signaling by the call originator and the arrival of a permission to transmit to the call originator.

R

Radio channel

Represents an assigned band of frequencies sufficient for radio communication. The bandwidth of a radio channel depends upon the type of transmission and its frequency tolerance.

Radio control service

The logical element in the Cisco IPICS system that can tune a radio to the desired channel without manual intervention. Refers to a serial control entity.

Radio equipment

Any equipment or interconnected system or subsystem of equipment (both transmission and reception) that is used to communicate over a distance by modulating and radiating electromagnetic waves in space without artificial guide. This equipment does not include microwave, satellite, or cellular telephone equipment.

Remote connection

Cisco IPICS uses this type of connection to provide SIP-based trunking into the UMS component, which is directly tuned into the multicast channel.

RF

Radio frequency. Any frequency within the electromagnetic spectrum that is normally associated with radio wave propagation. RF generally refers to wireless communications with frequencies below 300 GHz.

RFC 2833

The Internet Engineering Task Force (IETF) specification that describes how to carry DTMF signaling, other tone signals, and telephony events in RTP packets. Using RFC 2833 a packet can be compactly composed to play a series of tones, including DTMF, in a specific sequence that includes specified durations and volume levels.

RF repeater

An analog device that amplifies an input signal regardless of its nature (analog or digital). Also, a digital device that amplifies, reshapes, retimes, or performs a combination of any of these functions on a digital input signal for retransmission.

Root user ID

The Cisco IPICS Linux user that has access to all files in the Cisco IPICS server. Strong passwords are enforced and Linux operating system password expiration rules apply to this user ID.

RTP

Real-Time Transport Protocol. Commonly used with IP networks to provide end-to-end network transport functions for applications that transmit real-time data, such as audio, video, or simulation data, over multicast or unicast network services.

RTCP

Real-time Transport Control Protocol. The standard for notifying senders and receivers of important events or transmission statistics. The most common forms of RTCP are the sender report and the receiver report.
scanning  A subscriber unit feature that automatically allows a radio to change channels or talk groups to enable a user to listen to conversations that are occurring on different channels or talk groups.

script prompts  The audio prompts that the dial engine scripts play out during execution and which callers hear when they are interacting with the telephony user interface.

secure channel  A channel that is connected to a radio that provides secure (encrypted or scrambled) communications on the Common Air Interface (CAI) side of the radio. (The level of security that is configured in the data network determines the security of the communications between the LMR gateway and a network attached device, such as an IDC or Cisco Unified IP Phone.)

An attribute that is set in the server to indicate that a channel is secure. A PTT channel that is configured as secure cannot be combined with unsecure channels in a VTG.

serial controlled radio  A type of control for a radio that uses out-of-band signaling (usually RS-232). See radio control service.

signal  The detectable transmitted energy that carries information from a transmitter to a receiver.

speaker arbitration  The procedure that is used to determine the active audio stream in a Push-to-Talk system.

spectrum  The usable radio frequencies in the electromagnetic distribution. The following frequencies have been allocated to the public safety community:

- High HF 25–29.99 MHz
- Low VHF 30–50 MHz
- High VHF 150–174 MHz
- Low UHF 406.1–420/450–470 MHz
- UHF TV Sharing 470–512 MHz
- 700 MHz 764–776/794–806 MHz
- 800 MHz 806–824/851–869 MHz

spoken names  The recorded names that are used for entities, such as channels, channel groups, VTGs, users, user groups, ops views, and policies. The names can be recorded through the policy engine or externally-recorded .wav files that can be uploaded into the system.

squelch  An electric circuit that stops input to a radio receiver when the signal being received is too weak to be anything but noise.

statically configured tone control  Every stream of data that flows to the LMR gateway can be applied with a preamble and/or guard tone by using a static configuration in the LMR gateway. When traffic is sent on a multicast address, the radio automatically switches (because of the preamble) to the specific radio channel that is requested by the tone control sequence.

stored VTG  Also referred to as inactive VTG.

subchannel  A channel that shares the same multicast address as another channel or channels. These multiple source streams (channels) may be present on a single radio channel.

subscriber unit  A mobile or portable radio unit that is used in a radio system.
The Cisco IPICS system administrator is responsible for installing and setting up Cisco IPICS resources, such as servers, routers, multicast addresses, locations, and PTT channels. The system administrator also creates ops views, manages the Cisco IPICS licenses, and monitors the status of the system and its users via the activity log files.

The design principles, physical structure, and functional organization of a land mobile radio system. Architectures may include single site, multi-site, simulcast, multicast, or voting receiver systems.

T1
Digital WAN carrier facility. T1 transmits DS-1-formatted data at 1.544 Mbps through the telephone-switching network, using alternate mark inversion (AMI) or binary 8 zero suppression (B8ZS) coding.

T1 loopback
Allows mapping from multicast to unicast so that unicast phone calls can be patched into an LMR or into other multicast audio streams. A loopback is composed of two of the available T1 interfaces.

talk group
A VTG or a channel.

A subgroup of radio users who share a common functional responsibility and, under normal circumstances, only coordinate actions among themselves and do not require radio interface with other subgroups.

TCP
Transmission Control Protocol. A connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.

time division multiple access
Type of multiplexing where two or more channels of information are transmitted over the same link by allocating a different time interval (“slot” or “slice”) for the transmission of each channel; that is, the channels take turns to use the link.

A device capable of sending, receiving, or sending and receiving information over a communications channel.

The number of bits, characters, or blocks passing through a data communications system, or a portion of that system.

A joint effort between government and industry to develop voice and data technical standards for the next generation of public safety radios.

The process of using inband tone sequences to change the behavior of a radio end point. An inband tone can be used to control functions, such as modifying (retuning) the radio frequency (RF channel), changing the transmit power level, and monitoring a channel. The most basic form of tone control (tone keyed) is used to key the radio. With the Cisco IPICS solution, the radio that is being controlled is directly connected to the LMR gateway E&M leads.

A specific form of a function tone. The tone that is used to signal the radio to select a frequency. These audible tone frequencies are generated in the router and combined in a specific sequence to perform a tone control function.

A tone keyed radio requires the presence of a specific tone on the incoming analog (e-lead) port. Without this tone, the radio cannot transmit. The tone is generally used to prevent spurious transmission that may occur because of injected noise.
tone signaling

Any form of over-the-air audible signals that are intended to terminate at the far end. Examples include alerting tones, DTMF tones, and paging tones.

trigger

A time-based event that invokes a policy on a scheduled basis, without manual intervention.

trunk

A physical and logical connection between two switches across which network traffic travels. In telephony, a trunk is a phone line between two central offices (COs) or between a CO and a PBX.

trunked (system)

Systems with full feature sets in which all aspects of radio operation, including RF channel selection and access, are centrally managed.

trunked radio system

Integrates multiple channel pairs into a single system. When a user wants to transmit a message, the trunked system automatically selects a currently unused channel pair and assigns it to the user, decreasing the probability of having to wait for a free channel.

tune (a radio)

To change the current send and receive frequencies on a radio. This task is usually accomplished via a preset with some form of radio control.

U

user

The Cisco IPICS user may set up personal login information and specify communication preferences that are used to configure audio devices. By using a predefined user ID and profile, the user can participate in PTT channels and VTGs by using supported Cisco Unified IP Phone models, the Cisco Mobile Client, or the Public Switched Telephone Network (PSTN) via the telephony dial functionality of the Cisco IPICS IP policy engine. Users may have one or more Cisco IPICS roles, such as system administrator, ops view administrator, operator or dispatcher.

UMS

The Unified Media Service (UMS) is a highly available, software-based media engine that performs several core functions in a Cisco IPICS deployment.

unicast

Specifies point-to-point transmission, or a message sent to a single network destination.

V

VAD

Voice Activity Detection. When VAD is enabled on a voice port or on a dial peer, only audible speech is transmitted over the network. When VAD is enabled on Cisco IPICS, the IDC only sends voice traffic when it detects your voice.

virtual channel

A virtual channel is similar to a channel but a radio system may not be attached. By creating a virtual channel, participants who do not use physical handheld radios to call into a VTG become enabled by using the IDC application or a supported Cisco Unified IP Phone model.

voice interoperability

Voice interoperability enables disparate equipment and networks to successfully communicate with each other.
VoIP  Voice over Internet Protocol. By digitalizing and packetizing voice streams, VoIP provides the capability to carry voice calls over an IP network with POTS-like functionality, reliability, and voice quality.

VOX  Voice-operated transmit. A keying relay that is actuated by sound or voice energy above a certain threshold and sensed by a connected acousto-electric transducer. VOX uses voice energy to key a transmitter, eliminating the need for push-to-talk operation.

VTG  virtual talk group. A VTG can contain any combination of channels, channel groups, users, and user groups. A VTG can also contain other VTGs.

VTG add participant  An action that adds selected participant(s) to the selected VTG.

W

wavelength  The representation of a signal as a plot of amplitude versus time.

wideband channel  Channels that occupy more than 20 kHz.
INDEX

A
access control list (ACL)  5-10, 5-25
aggressive VAD  5-8
Android devices  2-16
Assured Forwarding  5-20
assured forwarding 31 (AF31)  5-9
Asynchronous Transfer Mode (ATM)  8-3
Asynchronous Transfer Mode Peak Cell Rate (ATM PCR)  5-4
ATM and Frame Relay Service Inter-Working (SIW)  8-3

B
bandwidth
  codec affect on  5-5
  consumption  5-5, 5-6
  issues  5-4
  leased lines  5-19
  modifying consumption  5-6
  multicast over GRE  8-12
  over-provisioning  5-11
  planning  5-4
  point-to-point lines  5-19
  provisioning  5-2
  usage  5-5, 5-6
  voice payload  5-7
  bidirectional PIM  5-2, 5-3, 5-16
  broadcast queue  5-13
  buffering  5-11
  burst  5-4, 5-11

C
cabling, for VIC2-2E/M interface card  4-2
call leg  6-1, 6-3
Carrier Operated Relay  4-10
Carrier Operated Relay (COR)  5-8
carrier operated relay (COR)  4-7
Carrier Operated Squelch  4-10
Carrier Operated Squelch (COS)  4-7, 5-8
Cisco Instant Connect  2-16
Cisco IOS
  configuration for LMR gateway  4-6
  queuing techniques  5-10
Cisco IPICS
  codec  5-4
  components
    Cisco Instant Connect MIDlet  1-3
    Cisco IPICS server  1-3
    Cisco Unified IP Phone gateway  1-4
    LMR gateway  1-3
    mobile client  1-3
    networking components  1-4
    overview  1-2
    UMS  1-3
  deployment models  8-1
  markets  1-1
  mobile client, using DNS with  2-16
  multiple site model  8-2
  overview  1-1
  single site model  8-1
  UMS configuration for mixing  2-3
  WAN deployment issues  5-2
  Cisco Multicast Manager (CMM)  5-26
Cisco Unified Communications Manager
  configuration overview 2-21
  using with Cisco Unified IP Phone 2-20
Cisco Unified Communications Manager Express
  configuration 2-21
  using with Cisco Unified IP Phone 2-20
Cisco Unified IP Phone
  Cisco Communications Manager Express configuration for 2-21
  Cisco Unified Communications Manager Express configuration for 2-21
  configuring for Cisco IPICS 2-20
  overview 1-4
  services 2-20
Class-Based Weighted Fair Queuing (CBWFQ) 5-10
codec
  bandwidth use 5-5
  choosing 5-4
  considerations 5-4
delay 5-4
  G.711 5-4
  G.729a 5-4
  types in Cisco IPICS 5-4
  voice quality 5-5
Committed Information Rate (CIR) 5-4, 5-11, 5-12
compressed RTP (cRTP) 5-6
cRTP 5-7
Customer Edge Router (CE) 8-4

destination pattern 6-3
inbound 6-2
inbound call leg 6-4
matching inbound call leg 6-4
matching outbound call leg 6-4
outbound 6-2
outbound call leg 6-4
POTS 6-2
session target 6-3
VoATM (Voice over ATM) 6-2
VoFR (Voice over Frame Relay) 6-2
voice-network 6-2
Voice over IP (VoIP) 6-2
dial pool 7-2
dial port, usage 7-2
digital signal processor (DSP) 5-7, 5-8
discard eligible (DE) 5-11, 5-20
DNS
  mobile client 2-16
  DNS, configuration for mobile client 2-16
DS0
  channel optimization 4-11
  resources not required 2-7
DSCP per-hop behaviors (Fibs) 5-20
DSP
  channel optimization 4-11
  signal detection 5-8
dspfarm 4-11
duplicate packets 2-7

E
E&M interface card
  cabling 4-2
  overview 4-2
ear and mouth (E&M)
  analog signaling types 4-4
  interface 4-1
  interface card 4-3
Index

Solution Reference Network Design (SRND) for Cisco IPICS Release 4.7

port 5-13
Type III interface 4-5
Type II interface 4-4
Type V interface 4-5
egress policing 5-20
egress shaping 5-20
endpoints
  communication between 2-2
duplicate packets 2-7
expedited forwarding (EF) 5-9

F
firewall 5-25
Frame Relay
  broadcast queue 5-13
  Committed Information Rate (CIR) in 5-12
  connection with E&M port 5-13
  in WAN 8-3
  IP RTP Priority 5-10
  LLQ 5-10
  QoS 5-11
Frame Relay Traffic Shaping (FRTS) 5-12
FRF.12 fragmentation and reassembly technique 5-19

G
G.711 5-4, 8-2
G.729a 5-4
GRE tunnel 8-11

H
High-Level Data Link Control (HDLC) 5-19
Hoot ‘n’ Holler 4-1, 5-8

I
Internet Group Management Protocol (IGMP) 2-4
interoperability and collaboration 1-1
IP
  precedence 5-9
  RTP Priority 5-9, 5-10
IPSec VPN 8-13

J
jitter 5-2, 5-9, 5-11, 5-12

L
land mobile radio
  See LMR
LEAF 8-4
leased line 8-3
licenses, for Cisco IPICS 7-1
Link Fragmentation and Interleaving (LFI) 5-19
LMR
  audio connection to Cisco IPICS 4-1
  channel 2-3
  communication with endpoints 2-3
  gateway
    Cisco IOS configuration for 4-6
      radio interface 4-1
    integration with Cisco IPICS 4-1
    interface with Cisco IPICS 4-1
    recording multicast traffic 4-12
    use with Cisco Hoot ‘n’ Holler 4-1
  location, with UMS 3-2
  loopback
    interface 5-16
    voice port 2-2
  Low-Latency Queuing (LLQ) 5-9, 5-10, 5-12
Mixing
 audio 2-4
 channels in VTG 2-2
 DSP function 5-8
 voice streams 2-4, 5-8
 Mobile client 2-16
 DNS, using with 2-16
 overview 1-3

 MPLS
 in multiple site model 8-2
 VPN 8-3
 with multicast VPN 8-3
 multicast 5-6, 8-2
 address
 for VTG communication 2-2
 guidelines for using 5-24
 bandwidth 8-12
 bidirectional PIM 5-16
 call flow to unicast 2-11
 domain 8-2, 8-4, 8-5
 GRE tunnel 8-15
 island
 overview 8-10
 topology 8-10
 over GRE 8-11
 singularity
 GRE tunnel 8-14
 overview 8-13
 Multicast Virtual Route Forwarding (MVRF) 8-4
 multicast VPN (MVPN) 8-5
 provider network configuration for 8-5
 provider network verification 8-7
 routing 8-5
 Multilink Point-to-Point Protocol (MLPPP) 5-19
 multiple site model
 connectivity options 8-3
 overview 8-2

 Multilink Point-to-Point Protocol (MLPPP) 5-19
 Multilink Point-to-Point Protocol (MLPPP) 5-19
 Multiple site model
 connectivity options 8-3
 overview 8-2

 Multiprotocol Label Switching
 See MPLS

 Network
 management 5-26
 security in 5-25
 networking components, overview 1-4

 Over-detection 5-8
 Over-provisioning 5-11

 Packet
 buffering 5-11
 delay 5-9
 discard-eligible (DE) 5-11
 drop 5-11
 errors 5-2
 loss 5-2, 5-9, 5-12
 packet rate 5-13
 Permanent Virtual Circuit (PVC) 5-3
 PIM-SSM 8-4
 point-to-point connection 5-19
 Point-to-Point Protocol (PPP) 5-19
 policing 5-20
 Protocol Independent Multicast (PIM)
 bidirectional 5-2, 5-3
 dense mode (DM) 5-2
 overview 5-2
 sparse mode (SM) 5-2
 Provider Edge Router (PE) 8-4, 8-5
 Provider Router (P) 8-4
Q

QoS
  at WAN edge 5-20
  factors affecting 5-9
  in enterprise 5-21
  in Frame Relay network 5-11
  in LAN 5-20
  in multiple site model 8-3
  overview 5-8, 5-9
  policing 5-20
  queuing 5-21
  recommendations for networks 5-9
  trust boundary 5-21
  WAN, use in 5-2
  with point-to-point connections 5-19

Quality of Service
  See QoS
  queuing
    overview 5-21
    techniques 5-9, 5-10, 5-12

R

RADIUS 5-25
  Real-time Transport Protocol (RTP) 5-6
  recording
    multicast LMR traffic 4-12
    Tap Cisco IOS configuration 4-12
  remote user, UMS function with 3-4
  rendezvous point (RP) 5-2, 5-16
  Reverse Path Forwarding (RPF) 5-3
  RMS
    DS0 resources 2-7
    mixing 2-3, 2-4
    RTP, header compression 5-7

S

Secure Socket Layer (SSL) 5-25
  security
    access control list (ACL) 5-25
    firewall 5-25
    for Cisco IPICS 5-25
    RADIUS 5-25
    recommendations 5-25
    Secure Socket Layer (SSL) 5-25
    spanning tree (STP) attack mitigation 5-26
    TACACS+ 5-25
  serialization 5-9
  service access point (SAP) broadcast 5-13
  session target 6-3
  shared tree
    bidirectional 5-2
    forwarding traffic 5-3
    in PIM SIM 5-2
    unidirectional 5-2
  single site model
    benefits 8-2
    best practices 8-2
    design characteristics 8-1
    overview 8-1
    topology 8-2
  SIP
    provider for policy engine 1-3
    signaling flow 2-10
    spanning tree (STP) attack mitigation 5-26
    sparse mode (SM) 5-2
    Sustained Cell Rate 5-4

T

TACACS+ 5-25
  Time to Live (TTL) 2-12
  topology
    MPLS with multicast VPN 8-4
multicast island 8-10
multiple site model 8-3
single site model 8-2
trust boundary 5-21

U

UDP port 5-10

UMS
conserving resources 7-2
in Cisco IPICS deployment 3-2
in WAN that is not multicast enabled 5-6
license 7-1
locations, instances for 3-2
overview 1-3, 3-1
remote user, function with 3-4
resource allocation 3-3
resource consumption 2-8
scaling 3-3
under-detection 5-8
unicast
connection set up 2-10
in WAN that is not multicast enabled 5-6
Unified Media Service
See UMS

V

Virtual Private Network (VPN) 8-3
virtual talk group
See VTG
voice
packet 5-7
payload 5-7
quality 5-5, 5-8, 5-9, 5-12

voice activation detection (VAD)
aggressive 5-8
conventional 5-8

enabling 5-8
overview 5-7
use with LMR 4-7, 4-8

Voice and Video Enabled IP Security Protocol (IPSec) 8-3
VoIP bearer traffic 5-21
VoIP traffic, transmission rate 5-5
VPN
in deployment scenarios 5-23
multicast routing 8-5
with MLPS 8-3
VTG
about 2-2
communication between channels 2-2
creation 2-2
members 2-2
mixing of channels 2-2
multicast address 2-2
restricting access 2-9

W

Weighted-Fair Queuing (WFQ) 5-10
wireless network
configuration example 2-18
overview 2-18