Unified Communications on Cisco Integrated Services Routers

The following sections describe Unified Communications (UC) application services that are supported on Cisco 3900 series and Cisco 2900 series integrated services routers (ISRs).

Modules and Interface Cards

Cisco 3900 series and Cisco 2900 series ISRs support Unified Communications (UC) modules and interface cards in the following slots:

- Next-generation packet voice/data module (PVDM3)
- Service module (SM)
- Enhanced high-speed WAN interface card (EHWIC)

Note The PVDM3 slot and the SM slot are not backwards compatible with legacy modules. Legacy modules require an adapter for installation in these slots.

For a list of supported UC modules and interface cards see *Module Support on Cisco Integrated Services Routers Generation 2*.

Call Control

The Cisco 3900 series and Cisco 2900 series ISRs support the following types of call control applications and Cisco Voice solutions:

- Cisco Unified Communications Manager Express, page 170
- Unified Survivable Remote Site Telephony, page 171
- Cisco Unified SIP Proxy (CUSP), page 172
- Gatekeeper, page 172

Cisco Unified Communications Manager Express

Cisco Unified Communications Manager Express (CME) is a feature-rich entry-level IP telephony solution that is integrated directly into Cisco IOS software. Cisco Unified CME allows small business customers and autonomous small enterprise branch offices to deploy voice, data, and IP telephony on a single platform for small offices, thereby streamlining operations and lowering network costs.

Cisco Unified CME is ideal for customers who have data connectivity requirements and also have a need for a telephony solution in the same office. Whether offered through a service provider's managed services offering or purchased directly by a corporation, Cisco Unified CME offers most of the core telephony features required in the small office, and also many advanced features not available with traditional telephony solutions. The ability to deliver IP telephony and data routing by using a single converged solution allows customers to optimize their operations and maintenance costs, resulting in a very cost-effective solution that meets office needs.

A Cisco Unified CME system is extremely flexible because it is modular. A Cisco Unified CME system consists of a router that serves as a gateway and one or more VLANs that connect IP phones and phone devices to the router.

See Cisco Unified Communications Manager Express (CME) Overview at:
http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmeover.html.

Unified Survivable Remote Site Telephony

Cisco Unified Survivable Remote Site Telephony (SRST) enables Cisco routers to provide call-handling support for Cisco IP phones when they lose connection to Cisco Unified Communications Manager (CUCM) installations, or when the WAN connection is down. In a centralized deployment, under normal conditions, Cisco IP phones are controlled by the Cisco Unified Communications Manager located at a central site like the headquarters of an enterprise. When connection to CUCM breaks, for example as result of a failure in the network, Unified SRST automatically detects the failure and auto configures the router for providing backup call processing functionality.

During a WAN failure, the router allows all the phones to re-register to the remote site router in SRST mode, allowing all inbound and outbound dialing to be routed off to the PSTN (on a backup Foreign Exchange Office (FXO), BRI or Primary Rate Interface (PRI) connection).

Unified SRST provides redundancy for both Cisco IP as well as Analog phones to ensure that the telephone system remains operational during network failures. Both Skinny Client Control Protocol (SCCP) and session initiation protocol (SIP) based Cisco IP phones are supported with the Unified SRST.

When the WAN link or connection to the Cisco Unified Communications Manager is restored, call handling reverts back to the Cisco Unified Communications Manager automatically without need for any human intervention.

For general Unified SRST information, see *Cisco Unified SRST System Administrator Guide*.

- For information on how the H.323 and Media Gateway Control Protocol (MGCP) call control protocols relate to SRST, see *Cisco Unified SRST System Administrator Guide:*
  - For H.323, see *H.323 Gateways and SRST* at Cisco.com.
  - For MGCP, see *MGCP Gateways and SRST* at Cisco.com.
- Configurations of major SRST features are provided in the following chapters of the *Cisco Unified SRST System Administrator Guide*:
  - “Setting up the Network”
  - “Setting up Cisco Unified IP Phones”
  - “Setting up Call Handling”
  - “Configuring Additional Call Features”
  - “Setting up Secure SRST”
  - “Integrating Voice Mail with Cisco Unified SRST”

For SIP-specific SRST information, see *Cisco Unified SIP SRST System Administrator Guide*. To configure SIP SRST features, see the *Cisco Unified SIP SRST 4.1* chapter.

Cisco Unified SIP Proxy (CUSP)

The Cisco Unified SIP Proxy (CUSP) is a high-performance, highly available Session Initiation Protocol (SIP) server for centralized routing and SIP signaling normalization. By forwarding requests between call-control domains, the Cisco Unified SIP Proxy provides the means for routing sessions within enterprise and service provider networks.

To configure CUSP features, see *Configuring Cisco Unified SIP Proxy Version 1.1.3 for an Enterprise Network* at:
http://www.cisco.com/en/US/docs/voice_ip_comm/cusp/rel1_1_3/configuration/guide/cuspgd113.html

Gatekeeper

An H.323 Gatekeeper is an optional node in an H.323 network that manages endpoints (such as H.323 terminals, gateways, and Multipoint Control Units (MCUs), as well as Cisco Unified Communications Manager Express and Cisco Unified Communications Manager clusters). An H.323 Gatekeeper provides these endpoints with call routing and call admission control functions. The endpoints communicate with the Gatekeeper using the H.323 Registration Admission Status (RAS) protocol.

The H.323 Gatekeeper is a special Cisco IOS software image that runs on the Cisco ISR platforms and the AS5350XM and AS5400XM Universal Gateway platforms. The Cisco IOS H.323 Gatekeeper is an application that acts as the point of control for a variety of voice and video components that can be attached to an IP network such as IP telephony devices, IP-PSTN gateways, H.323 video conferencing endpoints, and H.323 multipoint control units while facilitating buildout of large-scale multimedia service networks.

To configure Gatekeeper features, see *Configuring H.323 Gatekeepers and Proxies* at:
http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_h323_configuration_guide/old_archives_h323/5gkconf.html.

Call Control Protocols

The Cisco 3900 series and Cisco 2900 series ISRs support the following type of call control protocols:

- Trunk-side Protocols, page 172
- Line-side Protocols, page 173

Trunk-side Protocols

The Cisco 3900 series and Cisco 2900 series ISRs support the following trunk-side call control protocols:

- Session Initiation Protocol (SIP), page 173
- Media Gateway Control Protocol (MGCP), page 173
- H.323, page 173

Session Initiation Protocol (SIP)

Session Initiation Protocol (SIP) is a peer-to-peer, multimedia signaling protocol developed in the IETF (IETF RFC 3261). Session Initiation Protocol is ASCII-based. It resembles HTTP, and it reuses existing IP protocols (such as DNS and SDP) to provide media setup and tear down. See *Cisco IOS SIP Configuration Guide* for more information.

For router configuration information under SIP, see *Basic SIP Configuration* chapter of the *Cisco IOS SIP Configuration Guide*.

Voice gateways provide voice security through SIP enhancements within the Cisco IOS Firewall. SIP inspect functionality (SIP packet inspection and detection of pin-hole openings) is provided, as well as protocol conformance and application security. The user is given more granular control on the policies and security checks applied to SIP traffic, and capability to filter out unwanted messages. For more information, see "Cisco IOS Firewall: SIP Enhancements: ALG and AIC" at Cisco.com.

Media Gateway Control Protocol (MGCP)

Media Gateway Control Protocol (MGCP) RFC 2705 defines a centralized architecture for creating multimedia applications, including Voice over IP (VoIP). See *Cisco IOS MGCP and Related Protocols Configuration Guide* for more information.

ISRs are configured primarily as residential gateways (RGWs) under MGCP. For residential gateway configuration information, see the *Configuring an RGW* section of the *Basic MGCP Configuration* chapter of *Cisco IOS MGCP and Related Protocols Configuration Guide*.

H.323

H.323 is an umbrella recommendation from the International Telecommunication Union (ITU) that defines the protocols to provide voice and video communication sessions on a packet network. The H.323 standard addresses call signaling and control, multimedia transport and control, and bandwidth control for point-to-point and multi-point sessions. See *Cisco IOS H.323 Configuration Guide* for more information about H.323.

For router configuration information, see the *Configuring H.323 Gateways* chapter of *Cisco IOS H.323 Configuration Guide*.

Line-side Protocols

The Cisco 3900 series and Cisco 2900 series ISRs support the following line-side call control protocols:

- SCCP-Controlled Analog Ports with Supplementary Features, page 174
- Session Initiation Protocol (SIP), page 174

SCCP-Controlled Analog Ports with Supplementary Features

Voice gateway ISRs support the Cisco Skinny Client Control Protocol (SCCP), which supplies basic and supplementary features on analog voice ports that are controlled by Cisco Unified Communications Manager or by a Cisco Unified Communications Manager Express system. Supported features include:

- Audible message waiting indication
- Call forwarding options
- Call park/pickup options
- Call transfer
- Call waiting
- Caller ID
- 3-party conference calls
- Redial
- Speed dial options

For more information on the features supported and their configuration, see *SCCP Controlled Analog (FXS) Ports with Supplementary Features in Cisco IOS Gateways* at Cisco.com.

Session Initiation Protocol (SIP)

Session Initiation Protocol (SIP) is a peer-to-peer, multimedia signaling protocol developed in the IETF (IETF RFC 3261). Session Initiation Protocol is ASCII-based. It resembles HTTP, and it reuses existing IP protocols (such as DNS and SDP) to provide media setup and tear down. See *Cisco IOS SIP Configuration Guide* for more information.

For router configuration information under SIP, see the *Basic SIP Configuration* chapter of *Cisco IOS SIP Configuration Guide*.

Voice gateways provide voice security through SIP enhancements within the Cisco IOS Firewall. SIP inspect functionality (SIP packet inspection and detection of pin-hole openings) is provided, as well as protocol conformance and application security. The user is given more granular control on the policies and security checks applied to SIP traffic, and capability to filter out unwanted messages. For more information, see "Cisco IOS Firewall: SIP Enhancements: ALG and AIC" at Cisco.com.

Unified Communications Gateways

The Cisco 3900 series and Cisco 2900 series ISRs support the following Unified Communication gateways:

- TDM Gateways, page 175
- Cisco Unified Border Element, page 176
- Unified Messaging Gateway, page 176

TDM Gateways

The Cisco 3900 series and Cisco 2900 series ISRs support the following type of time-division multiplexing (TDM) gateways:

- Voice Gateways, page 175
- Video Gateway, page 175

Voice Gateways

Cisco IOS voice gateways connect TDM equipment such as private branch exchanges (PBXs) and the PSTN to VoIP packet networks. The Cisco ISR voice gateway routers support the widest range of packet telephony-based voice interfaces and signaling protocols within the industry, providing connectivity support for more than 90 percent of all PBXs and public-switched-telephone-network (PSTN) connection points. Signaling support includes T1/E1 Primary Rate Interface (PRI), T1 channel associated signaling (CAS), E1-R2, T1/E1 QSIG protocol, T1 Feature Group D (FGD), Basic Rate Interface (BRI), foreign exchange office (FXO), ear and mouth (E&M), and foreign exchange station (FXS). These voice gateway are highly scalable from just a few analog connections to up to 24 T1 or E1 interfaces.

The Cisco ISR series voice gateway routers can communicate with the Cisco Unified Communications Manager using Session Initiation Protocol (SIP), H.323, or Media Gateway Control Protocol (MGCP). The Cisco IOS voice gateway routers can also connect directly to other Cisco voice gateway routers using SIP or H.323 and to various other VoIP destinations and call agents.

For more information, see *ISDN Voice, Video and Data Call Switching with Router TDM Switching Features* at:
http://www.cisco.com/en/US/tech/tk652/tk653/technologies_tech_note09186a00804794c6.shtml.

For details about tuning voice ports, see *Cisco IOS Voice Port Configuration Guide, Release 12.4T* at Cisco.com at:
http://www.cisco.com/en/US/docs/ios/voice/voiceport/configuration/guide/12_4t/vp_12_4t_book.html.

Video Gateway

The Integrated Data, Voice, and Video Services for ISDN Interfaces feature allows multimedia communications between H.320 endpoints and H.323, SIP, or Skinny Client Control Protocol (SCCP) endpoints.

See *Integrating Data, Voice, and Video Services for ISDN Interfaces* at Cisco.com for details about setting up a Video gateway (http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/h320gw.html.)

See *Cisco IOS H.323 Configuration Guide, Release 12.4T* at Cisco.com for details about the H.323 protocol (http://www.cisco.com/en/US/docs/ios/voice/h323/configuration/guide/12_4t/vh_12_4t_book.html).

Cisco Unified Border Element

Cisco Unified Border Element (Cisco UBE) is a session border controller that provides the necessary services for interconnecting independent Unified Communications networks securely, flexibly, and reliably. Media packets can flow either through the gateway (thus hiding the networks from each other) or around the border element, if so configured. The Cisco UBE is typically used to connect enterprise networks to service provider SIP trunks, or to interconnect different nodes in an enterprise network where protocol or feature incompatibilities exist, or where extra secure demarcation between segments of the network is needed.

The Cisco Unified Border Element provides the following network-to-network interconnect capabilities:

- Session Management: Real-time session setup and tear-down services, call admission control, ensuring QoS, routing of calls if an error occurs, statistics, and billing.
- Interworking: H.323 and SIP protocol conversion; SIP normalization; DTMF conversion, transcoding, codec filtering
- Demarcation: Point of fault isolation, topology hiding, establishing and maintaining network borders, gathering statistics, and billing information on each network segment separately
- Security: Provides interworking between encrypted and non-encrypted network segment, SIP registration services, DOS protection, authentication services, and toll fraud protection on H.323 or SIP trunks.

See *Cisco Unified Border Element Configuration Guide* at Cisco.com for more information, http://www.cisco.com/en/US/docs/ios/voice/cube/configuration/guide/vb_book/vb_book.html.

Unified Messaging Gateway

The Cisco Unified Messaging Gateway provides an open and secure method of intelligently routing messages and exchanging subscriber and directory information within a unified messaging network. It acts as the central hub in a network of Cisco unified messaging solutions and third-party gateways that interface with older voicemail systems.

Unified Messaging Gateway is ideal for companies that need the following key features:

- Scales the unified messaging network as required for branch-office customers and larger distributed enterprises
- Simplifies configuration tasks and centralize voicemail system management
- Transparently integrates Cisco Unified Communications solutions into existing voicemail installations
- Integrates small to large-scale unified messaging deployments that consist of more than five Cisco Unity Express systems.
- Integrates up to 10,000 mixed Cisco Unity Express, Cisco Unity, and Cisco Unity Connection systems.

See *Cisco Unified Messaging Gateway 1.0 Command Reference* at Cisco.com for more information, http://www.cisco.com/en/US/docs/voice_ip_comm/umg/rel1_0/command/reference/UMG_1.0_CmdRef.html.

IP Media Services

The Cisco 3900 series and Cisco 2900 series ISRs support the following media services:

- Conferencing, Transcoding and Media Termination Point (MTP), page 177
- RSVP Agent, page 177
- Trusted Relay Point (TRP), page 177

Conferencing, Transcoding and Media Termination Point (MTP)

Cisco Enhanced Conferencing and Transcoding for Voice Gateway Routers provides conferencing and transcoding capabilities in Cisco IOS Software-based gateways using the onboard Cisco Packet Voice/Fax Digital Signal Processor Modules on the Cisco voice gateway routers. This capability is also supported on Cisco voice gateway router platforms using the Cisco IP Communications Voice/Fax Network Module and the Cisco IP Communications High-Density Digital Voice/Fax Network Module. This feature is delivered in Cisco IOS Software and operates in conjunction with Cisco CallManager.

See *Configuring Enhanced Conferencing and Transcoding for Voice Gateway Routers* at Cisco.com for configuration information, http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/interop/intcnf2.html.

RSVP Agent

The RSVP Agent feature implements a Resource Reservation Protocol (RSVP) agent on Cisco IOS voice gateways that support Cisco Unified Communications Manager Version 5.0.1. The RSVP agent enables Cisco Unified Communications Manager to provide resource reservation for voice and video media to ensure QoS and call admission control (CAC). Cisco Unified Communications Manager controls the RSVP agent through Skinny Client Control Protocol (SCCP). This signaling is independent of the signaling protocol used for the call so SCCP, SIP, H.323, and MGCP calls can all use the RSVP agent.

Benefits of this feature include the following:

- Improves flexibility and scalability of bandwidth management in a meshed network by decentralizing call admission control
- Provides method of managing unpredictable bandwidth requirements of video media
- Enables RSVP across WAN for Cisco IP phones and other devices that do not support RSVP

See *Configuring the RSVP Agent* at Cisco.com for information, http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/interop/int_rsvp.html.

Trusted Relay Point (TRP)

The Cisco Unified Communications system can be deployed in a network virtualization environment. Cisco Unified Communications Manager enables the insertion of trusted relay points (TRPs). The insertion of TRPs into the media path constitutes a first step toward VoIP deployment within a virtual network.

See *Media Resource Management* at Cisco.com for more information, http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/7_0_1/ccmsys/a05media.html#wp1056492.

Packet Voice Data Module

The Next-Generation Packet Voice Data Module (PVDM3) digital signal processor (DSP) modules provide up to four times the density (per slot) of existing audio applications on Cisco voice gateway routers. One universal DSP image for these DSP modules provides resources for time-division multiplexing-to-Internet Protocol (TDM-to-IP) gateway functionality for digital and analog interfaces, audio transcoding, and audio conferencing.

This enhanced DSP architecture accommodates a new packet-processing engine for rich-media voice applications and supports the TDM voice framework used by the PVDM2 module. The PDVM3 has a Gigabit Ethernet interface with a Multi-Gigabit Fabric to increase IP throughput, and a DSP hardware-based health monitor provides DSP failure detection that is ten times faster than existing technology.

To configure PVDM3 features, see the "Configuring Next-Generation High-Density PVDM3 Modules" section on page 185.

Voice Security

The Cisco 3900 series and Cisco 2900 series ISRs support the following voice security services:

- UC Trusted Firewall, page 178
- Signaling and Media Authentication and Encryption, page 179
- Virtual Route Forward, page 179

UC Trusted Firewall

Cisco Unified Communications Trusted Firewall Control pushes intelligent services onto the network through a Trusted Relay Point (TRP). Firewall traversal is accomplished using Simple Session Traversal Utilities for NAT (STUN) on a TRP co-located with a Cisco Unified Communications Manager Express (Cisco Unified CME), Cisco Unified Border Element (CUBE), Media Termination Point (MTP), Transcoder, or Conference Bridge.

Firewall traversal for Unified Communications is often a difficult problem. Voice over IP (VoIP) protocols use many ports for a single communication session and most of these ports (those used for media, H.245 and so forth) are ephemeral. It is not possible to configure static rules for such ports, as they fall in a large range. Cisco Unified Trusted Firewall opens ports dynamically based on the conversation of trusted end-points.

By using UC Trusted Firewall in the network, following things can be achieved:

- Firewall can be made independent of protocol, because only TRP, which is controlled by Call Control needs to be enhanced for various protocols. Firewall does not need to change.
- Increase firewall performance while opening firewall ports in the media path dynamically when a VoIP call is made between two endpoints.
- Simplify the firewall policy configuration and integration of firewall policy generation with call control.
- Provide a solution without compromising on network security.

To configure UC Trusted Firewall features, see *Cisco Unified Communications Trusted Firewall Control* at:
http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/feature/guide/TrustedFirewallControll.html.

Signaling and Media Authentication and Encryption

The Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways feature provides support for Cisco Secure Survivable Remote Site Telephony (SRST) and voice security features that include authentication, integrity, and encryption of voice media and related call control signaling.

See *Media and Signaling Authentication and Encryption Feature on Cisco IOS MGCP Gateways* at Cisco.com for configuration information, http://www.cisco.com/en/US/docs/ios/12_3t/12_3t11/feature/guide/gtsecure.html.

The Media and Signaling Encryption (SRTP/TLS) on DSP Farm Conferencing feature provides secure conferencing capability for Cisco Unified Communications Manager (Unified CM) networks, including authentication, integrity and encryption of voice media and related call control signaling to and from the digital signal processor (DSP) farm.

See *Media and Signaling Encryption (SRTP/TLS) on DSP Conferencing Farm* at Cisco.com for configuration information, http://www.cisco.com/en/US/docs/ios/12_4t/12_4t15/itsdsp.html.

See *SIP: SIP Support for SRTP* at Cisco.com for configuration information, http://www.cisco.com/en/US/docs/ios/12_4t/12_4t15/srtpstub.html#wp1008975.

Virtual Route Forward

Virtual Route Forward (VRF) is the technique to create multiple virtual networks within a single network entity. In a single network component, we can create multiple VRFs to create the isolation among each other. In our regular deployment of Unified Communication, we create different VLANs for voice and data to separate traffics. This is Layer-2 virtualization. In conjunction with VAN support, Cisco UC also supports Layer-3 virtualization through VRF for both voice and data.

In a typical UC deployment, hard phones are typically in Voice Segments and PCs are in Data Segments. PCs are inherently un-trusted devices in the network. Mechanisms based on’s rely on port numbers and there is no way to ensure only ‘trusted’ media enters UC Segment. VRF implementations in ISR can create single voice network and multiple data networks, which consolidate voice communication into one logically partitioned network to separate voice and data communication on a converged multi-media network.

To configure Virtual Route Forward features, see *Virtual Route Forwarding Design Guide* at: http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/vrf/design/guide/vrfDesignGuide.html.

Applications and Application Interfaces (APIs)

The Cisco 3900 series and Cisco 2900 series ISRs support the following applications and application interfaces:

- Cisco Unity Express, page 180
- Voice XML, page 180
- Hoot-n-Holler, page 181
- Hoot-n-Holler, page 181
- Cisco Application Extension Platform, page 181
- APIs, page 181

Cisco Unity Express

Cisco Unity Express provides integrated messaging, voicemail, Automated Attendant services, and optional interactive voice response (IVR) for the small and medium-sized office or branch office. The application is delivered on either a network module or advanced integration module, both of which are supported on a variety of voice-enabled integrated services routers.

This application is ideal for companies that need the following:

- Integrated messaging, voicemail, Automated Attendant, or interactive-voice-response (IVR) services at the branch or small office to support local users
- Up to 250 users per site
- Networking of multiple Cisco Unity Express systems for easy management of messages across sites

The application features follow:

- Affordable messaging, greeting services for increased customer service, and rich employee communications.
- Intuitive telephone prompts and a web-based interface provide fast, convenient voicemail, and Automated Attendant administration.
- Cisco Unity Express can view, sort, search, and play back voice messages using the display of a Cisco Unified IP Phone or your e-mail client.
- Scalable solution from 4 to 16 concurrent voicemail or Automated Attendant calls and 12 to 250 mailboxes.
- Deployable with Cisco Unified Communications Manager Express, Cisco Unified Communications Manager, Cisco Unity, and Cisco Unity Connection systems.

See the Unity Express Configuration guides at Cisco.com for more information, http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guides_list.html.

Voice XML

Cisco IOS unified communications routers provide many rich voice capabilities, including Voice Extensible Markup Language (VoiceXML) browser services. VoiceXML is an open-standard markup language used to create voice-enabled Web browsers and interactive-voice-response (IVR) applications. Available on a wide range of Cisco IOS Software voice gateways, these services are used in conjunction with a VoiceXML application service such as Cisco Unified Customer Voice Portal (CVP). Other VoiceXML applications can also use the Cisco IOS routers as a VoiceXML browser to provide IVR services to callers.

To configure a Voice XML gateway on the Cisco 3900 series or Cisco 2900 series Integrated Services Router see:
http://www.cisco.com/en/US/docs/ios/voice/ivr/configuration/guide/ivrapp01.html#wp1010676.

Cisco IOS voice features having to do with Cisco IOS Tcl IVR and VoiceXML for developers and network administrators who are installing, configuring, and maintaining a Tcl or VoiceXML application on a Cisco voice gateway are provided at:

http://www.cisco.com/en/US/docs/ios/voice/ivr/configuration/guide/Roadmap.html#wp1008602.

Hoot-n-Holler

Cisco Hoot-n-Holler network solution uses Cisco IOS Multicast and Cisco IOS Voice-over-IP technologies. The Cisco IP-based Hoot network uses bandwidth when it is in use; when it is not, the same bandwidth can be used to carry other traffic. The IP backbone interoperates with existing Hoot & Holler end-station equipment, such as microphones, turrets, Hoot phones, or squawk boxes, as well as bridges and mixers, for a seamless transition. Brokerage houses can adapt this solution to eliminate costly private telco circuits and reap significant operational cost savings—up to millions of dollars per year—for a rapid return on investment.

See *Cisco Hoot and Holler over IP* at Cisco.com for information, http://www.cisco.com/en/US/docs/ios/12_2/voice/configuration/guide/vvfhhip.html

See *Cisco IOS Multicast for Hoot & Holler Networks* at Cisco.com for information, http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns70/networking_solutions_white_paper09186a00800a3e6c.shtml

Cisco Application Extension Platform

Cisco Application Extension Platform (AXP) is an open network platform for application development, integration and hosting. It is a service module on the Cisco Integrated Services Router (ISR). AXP realizes the "Network as a Platform" vision of Cisco while bringing collaborative partnerships and accelerating innovation. Cisco AXP offers the following features:

- Linux-based integration environment to develop applications that run on routers.
- Certified libraries to implement C, Python, Perl, and Java applications (http web server and SSH are also supported).
- Service APIs for integrating applications into the network.
- Multiple applications can run in their own virtual instance with the ability to segment and guarantee CPU, memory, and disk resources.

See *Cisco Application eXtension Platform Quick Start Guide* at Cisco.com for Getting Started information, http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/ax/1.0/quick/guide/axpqs.html.

See *Cisco Application eXtension Platform Developer Guide* at Cisco.com for developers information, http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/ax/1.0/developer/guide/axpdev.html.

APIs

The Cisco 3900 series and Cisco 2900 series ISRs support the following application interfaces:

- TAPI, page 182
- AXL, page 182
- Gatekeeper Transaction Message Protocol (GKTMP), page 182

TAPI

The standard Cisco Unified TAPI provides an unchanging programming interface for different implementations. The goal of Cisco in implementing TAPI for the Cisco Unified Communications Manager platform remains to conform as closely as possible to the TAPI specification, while providing extensions that enhance TAPI and expose the advanced features of Cisco Unified Communications Manager to applications.

See *Basic TAPI Implementation* at Cisco.com for information, http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/tapi_dev/7_0_1/tpdevch4.html

AXL

The AXL API provides a mechanism for inserting, retrieving, updating, and removing data from the Cisco Unified Communications Manager database by using an eXtensible Markup Language (XML) Simple Object Access Protocol (SOAP) interface. This approach allows a programmer to access the database by using XML and receive the data in XML form, instead of by using a binary library or DLL.

The AXL API methods, known as requests, use a combination of HTTPS and SOAP. SOAP is an XML remote procedure call (RPC) protocol. The server receives the XML structures and executes the request. If the request completes successfully, the system returns the appropriate AXL response. All responses are named identically to the associated requests, except that the word "Response" is appended.

See *Cisco Unified Communications Manager XML Developers Guide Release 7.0(1)* at Cisco.com for information,
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/devguide/7_0_1/ccmdvCh1.html.

Gatekeeper Transaction Message Protocol (GKTMP)

The Cisco Gatekeeper Transaction Message Protocol (GKTMP) and application programming interface (API) is available for your use.

See *GKTMP Commands (GK API Guide Version 4.4* at Cisco.com for the latest Gatekeeper API inputs and outputs, http://www.cisco.com/en/US/docs/ios/12_3/gktmpv4_3/guide/gk_cli.html.

Online Insertion and Removal

Online insertion and removal (OIR) is a feature that allows you to replace modules without turning off the router and without affecting the operation of other interfaces. OIR of a module provides uninterrupted operation to network users, maintains routing information, and ensures session preservation.

For instructions on inserting, removing, and replacing the module, see the hardware installation guide for your router at Cisco.com.