

H.323 Overview

Last Updated: May 26, 2011

This chapter provides an overview of the ITU- H.323 standard for sending and receiving audio, video, and data on an IP-based internetwork.

Note For information about the full set of Cisco IOS voice features, see the entire Cisco IOS Voice Configuration Library--including library preface, glossary, and other documents--at h / en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vcl.htm

- Prerequisites for Configuring an H.323 Network, page 1
- Restrictions for Configuring an H.323 Network, page 2
- Information About H.323, page 4
- Additional References, page 13

Prerequisites for Configuring an H.323 Network

- Establish a working IP network. For information on IP configuration, see the references listed in the "Related Documents" section.
- Install the appropriate voice network module and voice-interface card for the Cisco router. For information on the module and card, see the Voice Network Module and Voice Interface Card Configuration Note that came with the voice network module.
- Configure your H.323 gateways, gatekeepers, and proxies. For information on VoIP configuration, see the resources in the "Related Documents" section.
- To ensure network security, configure a RADIUS authentication, authorization, and accounting (AAA) server. Configure the following information in your CiscoSecure AAA server:
  - In the /etc/raddb/clients file, ensure that the following information is provided:

```
#Client Name            Key
```

```
#---------------          --------------------------
                               testing123
```

Where is resolved to the IP address of the gatekeeper requesting authentication

- ◦ In the /etc/raddb/users file, ensure that the following information is provided:

```
                  Password = "thiswouldbethepassword"
User-Service-Type = Framed-User,
Login-Service = Telnet
```

Where is the h323-id of the gateway authenticating to gatekeeper .

- Configure an NTP server for your network.
- For gatekeeper-management statistics, do the following:
  - Configure the Simple Network Management Protocol (SNMP) agent in global configuration mode.
  - Update the MIB data files on your management workstations so that the management application knows what the new objects are.

Restrictions for Configuring an H.323 Network

This section describes the following restrictions:

- H.323 Version 2 Restrictions, page 2
- H.323 Signaling Enhancement Restrictions, page 2
- Source Call Signal Address and H.245 Empty Capabilities Set Restrictions, page 3
- Call Transfer Restrictions, page 3
- Ecosystem Gatekeeper Interoperability Restrictions, page 4
- H.323 Gatekeepers and Proxies Restrictions, page 4

H.323 Version 2 Restrictions

- All systems must be running either Cisco IOS Release 11.3(9)NA and later releases or Cisco IOS Release 12.0(3)T and later releases to interoperate with the Cisco H.323 Version 2 features. Earlier releases contain H.323 Version 1 software that does not support protocol messages that have an H.323 Version 2 protocol identifier. The earlier releases do not interoperate with Cisco H.323 Version 2 Phase 2 features.
- To use H.450 services (call transfer or call deflection), use Cisco IOS Release 12.1(1)T or later on the gatekeeper: H.450 on the gateways is incompatible with previous releases of the Cisco gatekeeper.
- If a Cisco AS5300 is used, the software requires the appropriate version of VCWare.
- The H.323 Version 2 Fast Connect feature is not explicitly configurable. It is assumed that the gateway is capable of sending and receiving fast-connect procedures unless its corresponding dial peer is configured for RSVP (in other words, the req-qos is set to a value other than the default of best-effort). In the latter case, traditional "slow" connect procedures are followed, and the endpoint neither attempts to initiate fast connect nor responds to a fast-connect request from its peer.

H.323 Signaling Enhancement Restrictions

- Supplementary voice services are not supported with ISDN and CAS over an H.323 network--except on the NET5 switch.
- Progress messages require a PI value, and only ITU-T standards are supported.
- Progress indicator 2 is not supported in progress messages for the DMS100 switch.
- TCL 2.0 for IVR supports the interworking signaling enhancements only on the Cisco AS5300. For IVR on other Cisco platforms, select TCL 1.0 as the session application. To use standard IVR applications with TCL 1.0, configure the application name as "session.t.old" by using the **call application voice** command. It is not necessary to do this if customized scripts are used.
- The Cisco AS5300 sends a connect message to the originating gateway after it receives a setup message only when it is configured for one of the following supported switch types:
  - 5ESS
  - NET5
  - NTT
  - QSIG
  - QSIGP
- For the SS7 interconnect for voice gateways solution, the following behavior applies to suspend and resume messages, which are supported on NET5 and NI2+ ISDN interfaces:
  - If the ISDN interface is NET5, the Cisco AS5300 sends a notify message with the notification indicator (NI) set to user-suspended or user-resumed.
  - If the ISDN interface is NI2+, the Cisco AS5300 sends a suspend or resume message to the Cisco SC2200.
  - If the Cisco SC2200 receives an ISUP suspend or resume message, it sends an NI2+ suspend or resume message to the Cisco AS5300.
  - Both the Cisco AS5300 and the Cisco SC2200 timers start when a suspend message is received. The Cisco AS5300 timer, T307, is configurable from 30 to 300 seconds. The Cisco SC2200 timer, T6, is not configurable and has a default of 120 seconds if the ISUP variant Q.761 is used.
- When the Cisco AS5300 and the Cisco SC2200 receive a resume message, the timers are stopped. If either of the timers expires, the call is released with a cause code of normal clearing.

Source Call Signal Address and H.245 Empty Capabilities Set Restrictions

- To use H.450 services (call transfer or call deflection), Cisco IOS Release 12.1(2)T of the gatekeeper must be used. H.450 on the gateways is incompatible with previous releases of the Cisco gatekeeper.
- If a Cisco AS5300 is used, the system requires the appropriate version of VCWare.

Call Transfer Restrictions

- Interactive Voice Response (IVR) must be configured on the router and supplementary services must be provided for processing. For information about configuring IVR and supplementary services, see Configuring Interactive Voice Response for Cisco Access Platforms.
- The "session" application must be specified properly for the dial-peers.
- Release 12.1(1)T (or later) of the Cisco H.323 Gatekeeper is required.
- The H.323 Call Redirection Enhancements feature does not provide the ability for a Cisco H.323 Gateway to initiate a call transfer request.

Ecosystem Gatekeeper Interoperability Restrictions

- The maximum number of alternate gatekeepers is eight (including static gatekeepers).
- During the retransmission of the GRQ or RRQ messages, the gateway responds only to the current gatekeeper (regardless of the state of the altGKisPermanent flag).
- The process of retransmission to an alternate gatekeeper can be time-consuming.

H.323 Gatekeepers and Proxies Restrictions

- Both the gateway H323_ID and the generalID in ClearTokens should be same.

Information About H.323



Note When you configure H.323 on a router, the ports on all its interfaces are open by default. This makes the router vulnerable to malicious attackers who can execute toll fraud across the gateway if the router has a public IP address and a public switched telephone network (PSTN) connection. To eliminate the threat, you should bind an interface to private IP address that is not accessible by untrusted hosts. In addition, you should protect any public or untrusted interface by configuring a firewall or an access control list (ACL) to prevent unwanted traffic from traversing the router.

- H.323 Standards, page 4
- Network Components, page 5
- Discovery and Registration, page 10
- Call Setup, page 10
- Call Termination, page 12
- Security, page 13

H.323 Standards

The table below lists H.323 standards and applicable Cisco VoIP features.

Table 1: H.323 Standards and Applicable Cisco VoIP Features

Standard	Applicable Cisco VoIP Features
H.323 Version 1	• Multimedia conferencing protocol which includes voice, video, and data conferencing for use over packet-switched networks • Provides a framework that uses others to describe the actual protocol ◦ H.245 conference-control protocol

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：https://d.book118.com/508137032013006023