Fax, Modem, and Text Support over IP Configuration Guide, Cisco IOS Release 15M&T

Last Modified: 2015-07-31

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

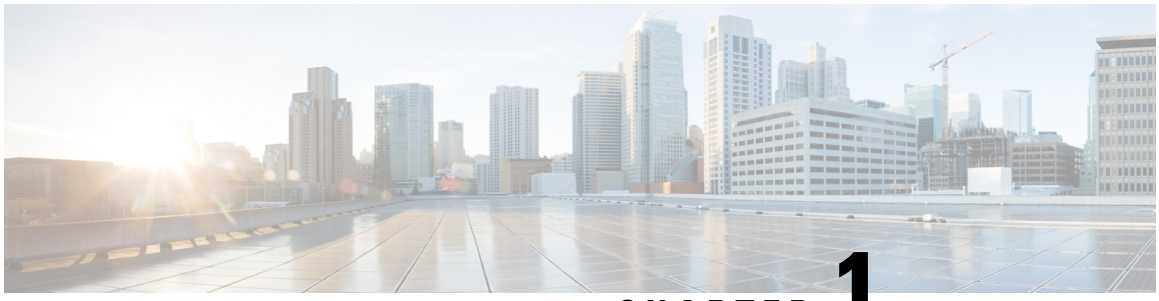
All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com go trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2015 Cisco Systems, Inc. All rights reserved.

CONTENTS



CHAPTER 1

Fax and Modem Services over IP Overview

Fax and Modem Services over IP Overview

This application guide includes descriptions and configuration instructions for fax and modem transmission capabilities on Cisco Voice over IP (VoIP) networks. It is written for developers and network administrators who are installing, configuring, and maintaining fax and modem applications on Cisco voice gateways.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Cisco IOS Fax Services over IP

Fax Transmission in the PSTN

Facsimile (fax) transmission is the sending of an image, drawing, or document over a distance by converting it into coded electrical signals at the originating end, passing the signals from the originator to the receiver over a transmission medium, and converting the signals into a replica of the original at the receiving end.

When sending a fax, a fax machine uses a scanner to convert the paper image into digital bits, a single-chip microprocessor called a digital signal processor (DSP) to reduce the number of bits, and a modem to convert the bits into an analog signal for transmission over an analog dial-up phone line.

When receiving a fax, the fax machine uses its modem and printer to convert the incoming bits into black and white images on paper.

The information conveyed in a fax transmission consists of both protocol (control information, capabilities, identification) and document content . The document content consists primarily of the document image plus additional metadata that accompanies the image. The means by which an image of a document is encoded within the fax content is the image data representation .

When a fax has been sent successfully, the sender receives a confirmati*on* that indicates that the fax content was delivered. This confirmation is an internal signal and is not normally visible to the sending user, although some error messages are visible to allow a page to be resent.

The ability to send the representation of a page to a remote location developed over a number of years. The first images were sent over wires as early as 1843, but modern fax machines did not start appearing in offices until the 1960s. At that time, a single-page letter took about six minutes to send over public phone lines using the new Group 1 standard for transmission that was introduced by the International Telegraph and Telephone Consultative Committee (CCITT) in 1968. The Group 2 standard, introduced in 1976, reduced the time to send a page to three minutes, but still could not provide transmission at a dense enough resolution for the clear reproduction of small print. In 1980, the Group 3 standard was introduced. The Group 3 standard improved fax scanning resolution and introduced digital transmission techniques to enable transmission rates of 14400 bits per second (bps). Group 3 fax machines are the most common today by far. Group 4 is a standard for digital phone lines such as ISDN, and it operates at 64 kbps. Each standard specifies special tones that identify calls as fax calls and enable handshaking to define fax capabilities at both ends of the call. All of the fax standards have evolved with a goal of sending more data faster over the public switched telephone network (PSTN).

The PSTN is composed of switched time-division multiplexing (TDM) circuits, which are either single lines or trunks. A line connects a single telephony device to a switch, whereas a trunk connects a switch to a switch. The network provides exclusive and full use of a circuit between two endpoints and is full-duplex (simultaneous transmission in both directions), unless the call is data. Trunks are one of the following types:

- Analog trunks, in which nearly all the audio is sent as an analog signal.
- Digital trunks that carry bit streams encoded by the G.711 codec and sent at 64 kbps. The bit streams are also called pulse code modulation (PCM) streams.

Both circuit types have sufficient audio clarity, or dynamic range, to pass the tones required to send fax traffic across PSTN circuits.

Fax traffic consists of digital data modulated onto high-frequency carrier tones. There are various ways to modulate this information, such as Amplitude Modulation (AM), Frequency Modulation (FM) or Frequency Shift Keying (FSK), and Phase Modulation (PM) or Phase Shift Keying (PSK). In order to get higher bit rates (more information) across the same carrier circuit, these modulation techniques are often combined into forms of modulation called Quadrature Amplitude Modulation (QAM) or Trellis-Coded modulation.

Data Transmission Standards

The international standards that define data transmission techniques are used by both fax and modem transmission devices. The main difference between them is that modem payload originates as digital data, whereas fax payload is a paper image that has been encoded into a digital data stream. Another key difference is the initial handshaking that determines the facsimile or data capabilities of each party in the transmission.

There are standards that apply to both fax and modem machines and standards that apply to only fax machines, defining methods by which faxes are encoded and sent.

The traditional facsimile transmission standard, also called Group 3 (G3) fax, describes implementations of ITU-T T.30 and T.4. All Cisco IOS fax applications use T.30 and T.4 standards to interface with the PSTN or fax device.

For a comprehensive list of fax and modem standards, see the Standards, on page 23,

Fax Transmission Phases

The T.30 specification is over 150 pages long, but a summary of its contents is provided in the following sections to provide some familiarity with the handshaking between calling and called parties and the basic procedures involved during fax transmission. The table below lists the five phases in a fax transmission.

Table 1: T.30 Fax Transmission Phases

Phase	Description
Phase A Establishing a Voice Call, on page 3	The calling party picks up a handset or prepares a fax and then dials a destination phone or fax machine.
Phase B Identifying Facilities and Capabilities, on page 3	Facilities and capabilities are identified and negotiated between the calling and called parties.
Phase C Transmitting Content, on page 4	The message or page is sent.
Phase D Signaling End of Transmission and Confirmation, on page 4	The end of transmission and confirmation are signaled between the calling and called parties.
Phase E Releasing the Call, on page 4	The call is released when a phone or fax machine hangs up.

Phase A Establishing a Voice Call

The call originator prepares a fax and dials a destination number. The destination fax device picks up the call. The originator and the destination are now connected in a voice call, but to transition to fax transmission one party must signal that it is a fax device. Either device can send its signal first, using one of the following methods:

- The calling device sends a Calling Tone (CNG) to the destination device. The CNG identifies the calling device as a fax machine. The CNG is a repeating 1100-Hz tone that is on for 0.5 seconds and then off for 3 seconds.
- The called device sends a Called Station Identifier (CED) tone, which identifies the called device as a fax machine. CED is a 2100-Hz tone that is on for 2.6 to 4 seconds.

Once these messages have been exchanged, the transaction can move to phase B.

Phase B Identifying Facilities and Capabilities

The following sequence of events identifies facilities and capabilities for fax transmission:

1. The called device sends a Digital Information Signal (DIS), which describes the called fax machine's reception facilities, such as maximum page length, scan line time, image resolution, and error correction mode. Many standard facilities are contained in the DIS message, and they are defined in the T.30 specification.
2. The calling device examines the DIS message and in response sends a Digital Command Signal (DCS) that tells the called device which facilities to select for the reception of the fax transmission.
3. The called device may also choose to send the following optional messages:
4. Called Subscriber Identification (CSI) provides some detail as to the identity of the called device.

5. Non-Standard Facilities (NSF) informs the calling device that the called device may have some extra features that can be utilized during the fax transmission.
6. The calling device can then choose to send a Transmitting Subscriber Identification (TSI) message. Also, in response to an NSF message, the calling device can send a Non-Standard facilities Setup (NSS) message to select extra reception parameters on the called device.
7. The calling device now sends the Training Check (TCF) message, which includes a stream of 0s for about 1.5 seconds through the HS modulation that was agreed upon during the DIS-DCS handshake. The called device then responds with a Failure To Train (FTT) if the modulation speed is not acceptable or with a Confirmation to Receive (CFR) if the modulation speed is acceptable. Training is a process that verifies the communication path.
8. Once the training has been completed and the modulation speed is agreed upon, the fax devices move to phase C and start the transmission of T.4 page data using HS modulation.

Phase C Transmitting Content

Phase C is referred to as the In-message Procedure. During this phase, high-speed T.4 page data is sent one line at a time. Each burst of line data is followed by an End Of Line (EOL) message. Because the EOL information is sent as T.4 data, it would not necessarily be seen in a T.30 trace. When the sending device has finished sending pages or wishes to return back to control mode, it sends 6 EOLs in a series that constitutes a Return To Control (RTC) message. The RTC message indicates the end of phase C, and the call progresses to phase D.

Note If the fax machines decide during phase B to use Error Correction Mode (ECM), the format of the data sent during phase C may be different. With ECM, the T.4 page data is grouped into high-level data link control (HDLC) frames rather than being sent in a raw stream. This means that if the HDLC blocks of T.4 page data are not received error-free, a Partial Page Request (PPR) message can be sent, listing the frames that were not received and asking for them to be resent. The details of the transmission differences during phase C with ECM enabled are explained in Annex A of the T.30 specification.

Phase D Signaling End of Transmission and Confirmation

After the T.4 transmission and the subsequent return to control mode, the sending device must send one of the following signals:

- Partial Page Signal (PPS)--Devices that send faxes with ECM can send a PPS, which must be acknowledged by a Message Confirmation (MCF) signal from the receiving device.
- End Of Procedure (EOP)--This signal indicates that transmission of pages is complete and that there are no more pages to send. The EOP must be acknowledged with an MCF from the receiving device, after which the devices can move to phase E.

Phase E Releasing the Call

Following the fax transmission and the postmessage transactions, either the calling device or the called device can send a Disconnect (DCN) message, at which point the devices tear down the call, and the telephony call control layer releases the circuit. DCN messages do not require a response from the opposite device.

Fax Transmission over IP Networks

An IP, or packet-switched, network enables data to be sent in packets to remote locations. The data is assembled by a packet assembler/disassembler (PAD) into individual packets of data, involving a process of segmentation or subdivision of larger sets of data as specified by the native protocol of the sending device. Each packet has a unique identifier that makes it independent and has its own destination address. Because the packet is unique and independent, it can traverse the network in a stream of packets and use different routes. This fact has some implications for fax transmissions that use data packets rather than using an analog signal over a circuit-switched network.

Differences from Fax Transmission in the PSTN

Individual packets that are part of the same data transmission may follow different physical paths of varying lengths. They can also experience varying levels of propagation delay (latency) and delay that is caused by being held in packet buffers awaiting the availability of a subsequent circuit. The packets can also arrive in an order different from the order in which they entered the network. The destination node of the network uses the identifiers and addresses in the packet sequencing information to reassemble the packets into the correct sequence.

Fax transmissions are designed to operate across a 64-kbps, PCM-encoded voice circuit, but in packet networks the 64-kbps stream is often compressed into a much smaller data rate by passing it through a digital signal processor (DSP). The codecs normally used to compress a voice stream in DSPs are designed to compress and decompress human speech, not fax or modem tones. For this reason, faxes and modems are rarely used in a VoIP network without some kind of relay or pass-through mechanism in place.

Fax Services over IP Networks

There are two conceptual methods of carrying virtually real-time fax-machine-to-fax-machine communication across packet networks:

- Fax relay, in which the T.30 fax from the PSTN is demodulated at the sending gateway. The demodulated fax content is enveloped into packets, sent over the network, and remodulated into T.30 fax at the receiving end.
- Fax pass-through, in which modulated fax information from the PSTN is passed in-band end-to-end over a voice speech path in an IP network. The following two pass-through techniques are possible:
  - The configured voice codec is used for the fax transmission. This technique works only when the configured codec is G.711 with no voice activity detection (VAD) and no echo cancellation (EC), or when the configured codec is a clear-channel codec or G.726/32. Low bit-rate codecs cannot be used for fax transmissions.
  - The gateway dynamically changes the codec from the codec configured for voice to G.711 with no VAD and no EC for the duration of the fax session. This method is specifically referred to as codec upspeed or fax pass-through with upspeed.

In addition to the methods for real-time fax transmission, a method called store-and-forward fax breaks the fax process into distinct sending and receiving processes and allows fax messages to be stored between those processes. store-and-forward fax is based on the ITU-T T.37 standard, and it also enables fax transmissions to be received from or delivered to computers rather than fax machines.

Cisco Fax Services

Some of the methods described in this section have different characteristics depending on the call control protocol used by the network, which may be H.323, Session Initiation Protocol (SIP), or Media Gateway Control Protocol (MGCP). Where the characteristics are different, they are noted.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn . You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

This section describes the following aspects of the fax services available on Cisco IOS gateways:

Concepts Related to Cisco Fax Services

The following concepts are useful in understanding how fax transmission methods are implemented on Cisco IP networks:

Voice Gateways and Dial Peers

A Cisco voice gateway provides an interface between the IP network and the public switched telephone network (PSTN) or telephony (fax) device. When a call comes into the IP network over a gateway, that gateway is called an originating gateway (OGW). Similarly, a gateway over which a call passes out of the IP network is called a terminating gateway (TGW).

A traditional voice call over the PSTN uses a dedicated 64-kbps circuit end to end. In contrast, a voice call over the packet network contains several 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, inbound into and outbound from both the OGW and the TGW.

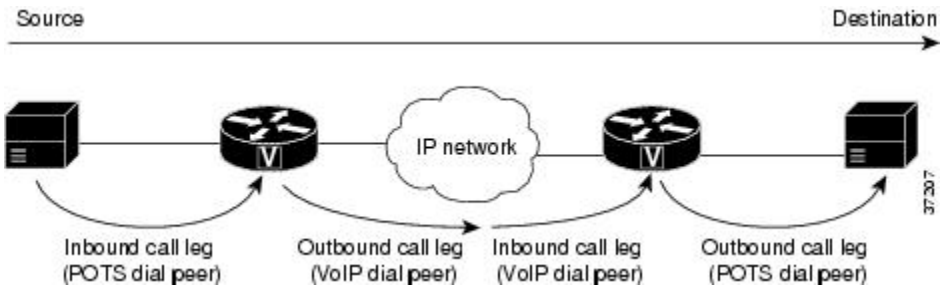
Dial peers are software constructs that sort calls, route calls, and define characteristics applied to each call leg in the call connection, based on call source and destination endpoints. Dial peers are used for both inbound and outbound call legs. It is important to remember that these terms are defined from the perspective of the router. An inbound call leg is created by any call that comes in to a router, regardless of whether the router is an OGW or a TGW. An outbound call leg is created by any call that leaves a router, regardless of whether the router is an OGW or a TGW, as shown in the figure below.

Different types of dial peers handle different kinds of call legs. The following types of dial peers are used for fax over Cisco IP networks:

- Plain old telephone service (POTS) dial peers handle call legs between a voice gateway and the PSTN or a telephony device.
- Voice over IP (VoIP) dial peers handle call legs between a voice gateway and the IP network.
- Multimedia Mail over IP (MMoIP) dial peers handle call legs between a voice gateway and a Simple Mail Transfer Protocol (SMTP) server or Extended SMTP (ESMTP) server.

Note For more information on voice gateways and dial peers, see Dial Peer Configuration on Voice Gateway Routers.

Figure 1: Call Legs and Dial Peers on Cisco IP Networks



TCL IVR

Tool Command Language (TCL) is used for scripts that direct interactive voice response (IVR) applications, which are used in Cisco voice networks for various purposes. IVR applications typically involve the real-time gathering of data from callers by means of digit collection and voice prompts. For example, you might have a debit card application that asks a user to enter a personal identification number (PIN) and then collects and verifies the digits that the user enters.

A gateway can have several IVR applications to accommodate different gateway services, and you can customize IVR applications to present different interfaces to various callers. IVR applications are used to implement the following fax services:

- T.37 Store-and-Forward Fax, on page 16
- Fax Detection IVR Application, on page 17
- Fax Rollover IVR Application, on page 18

TCL scripts are provided on the Cisco Software Center website. You download them to a location that is accessible to the voice gateway that is running the fax application and then configure the gateway with the name and location of the script.

Note For more information on TCL IVR, see the *Cisco IOS TCL and VoiceXML Application Guide*.

QoS

Quality of service (QoS) refers to the ability of a network--whether the network is a complex network, small corporate network, Internet service provider (ISP), or enterprise network--to provide better service to selected network traffic over various technologies, including Frame Relay, ATM, Ethernet and 802.1 networks, and SONET, as well as IP-routed networks that may use any or all of these underlying technologies.

The primary goals of QoS are to provide better and more predictable network service by providing dedicated bandwidth, controlled jitter and latency, and improved loss characteristics. QoS achieves these goals by providing tools for managing network congestion, shaping network traffic, using expensive wide-area links more efficiently, and setting traffic policies across the network.

QoS for fax transmissions means assuring that echo cancellation (EC) and voice activity detection (VAD), which are normally enabled for voice calls, are turned off as soon as a call is identified as a fax call. If EC and VAD are enabled, they can interfere with the successful reception of fax traffic.

The advantages of carrying fax over packet networks are reduced cost and saved bandwidth and are associated with QoS issues that are unique to packet networks. A major issue in the implementation of fax over IP networks is the problem of inaccurate timing of messages caused by delay through the network.

The delay of fax packets through a packet network causes the precise timing that is required for many portions of the fax protocol to be skewed and can result in the loss of the call. The fax-over-packet protocol in the interworking function must compensate for the loss of a fixed timing of messages over the packet network so that the T.30 protocol operates without error. Error Correction Mode (ECM) is enabled in the T.30 protocol.

An end-to-end fax over IP call is susceptible to the following sources of delay:

- Network delay--Network delay is caused by the physical medium and protocols that are used to send fax data and by buffers that are used to remove packet jitter on the receiving end. This delay is a function of the capacity of the links in the network and the processing that occurs as the packets transit the network. The jitter buffers add delay when they remove the packet delay variation of each packet as it transits the packet network. This delay can be a significant part of the overall delay because packet delay variations can be as high as 70 to 100 milliseconds in some Frame Relay networks, and even higher in IP networks.
- Processing delay--Processing delay is caused by the process of demodulating and collecting digital fax information into a packet for transmission over the packet network. Encoding delay, which is one type of processing delay, is a function of both the processor execution time and the amount of data collected before a packet is sent to the network.

Delay issues are compounded by the need to remove jitter, which is the variable interpacket arrival time that is caused by conditions in the network that a packet traverses. An approach to removing the jitter is to collect packets and hold them long enough so that even the slowest packets arrive in time to be played in the correct sequence. This approach, however, causes additional delay. In most fax over IP methods, a time stamp is incorporated in the packet to ensure that packet data is played out at the proper instant.

The T.30 standard provides for ECM that allows a fax page to be broken into HDLC-like frames that allow transmission errors to be detected. ECM works by sending a fax page in a series of blocks. After receiving the complete page data, the receiving fax identifies any frames with errors. The sending fax then retransmits those frames. This process is repeated until all frames have been received without errors.

If a receiving fax machine is not able to receive an error-free page, the fax transmission may fail, and one of the fax machines may disconnect. If a network has packet-loss levels greater than 3 to 5 percent, fax transmissions consistently fail when ECM is enabled. Fax relay packet loss concealment disables ECM so that fax calls with up to 9 percent packet loss succeed and calls with packet loss of 5 to 7 percent succeed with acceptable quality.

Fax Pass-Through and Fax Pass-Through with Upspeed

Fax pass-through is the simplest technique for sending fax over IP networks, but it is not the default, nor is it the most desirable method of supporting fax over IP. T.38 fax relay provides a more reliable and error-free method of sending faxes over an IP network, but some third-party H.323 and SIP implementations do not support T.38 fax relay. These same implementations often support fax pass-through.

Fax pass-through is the state of the channel after the fax upspeed process has occurred. In fax pass-through mode, gateways do not distinguish a fax call from a voice call. Fax communication between the two fax machines is carried in its entirety in-band over a voice call. When using fax pass-through with upspeed, the gateways are to some extent aware of the fax call. Although relay mechanisms are not employed, with upspeed the gateways do recognize a CED fax tone and automatically change the voice codec to G.711 if necessary (thus the designation *upspeed*) and turn off echo cancellation (EC) and voice activity detection (VAD) for the duration of the call.

Fax pass-through is also known as Voice Band Data (VBD) by the International Telecommunication Union (ITU). VBD refers to the transport of fax or modem signals over a voice channel through a packet network with an encoding appropriate for fax or modem signals. The minimum set of coders for VBD mode is G.711 u-law and a-law with VAD disabled.

Once a terminating gateway (TGW) detects a CED tone from a called fax machine, the TGW exchanges the voice codec that was negotiated during the voice call setup for a G.711 codec and turns off EC and VAD. This switchover is communicated to the originating gateway (OGW), which allows the fax machines to transfer modem signals as though they were traversing the PSTN. If the voice codec that was configured and negotiated for the VoIP call is G.711 when the CED tone is detected, there is no need to make any changes to the session other than turning off EC and VAD.

Before pass-through features were introduced (in Cisco IOS Release 12.1(3)T for the Cisco AS5300, and later for other Cisco IOS gateway platforms), fax pass-through was achieved by manually configuring a dial peer that only matched fax calls to set the codec parameters to G.711 with no EC and no VAD (or to clear-channel codec). Control of fax pass-through is achieved through named signaling events (NSEs) that are sent in the RTP stream.

NSEs are a Cisco-proprietary version of IETF-standard named telephony events (NTEs), which are specially marked data packets used to digitally convey telephony signaling tones and events. NSEs use different event values than NTEs and are generally sent with RTP payload type 100, whereas NTEs use payload type 101. NSEs and NTEs provide a more reliable way to communicate tones and events by using a single packet rather than a series of in-band packets that can be corrupted or partially lost.

Fax pass-through and fax pass-through with upspeed use peer-to-peer NSEs within the Real-Time Transport Protocol (RTP) stream or bearer stream to coordinate codec switchover and the disabling of EC and VAD. Redundant packets can be sent to improve reliability when the probability of packet loss is high.

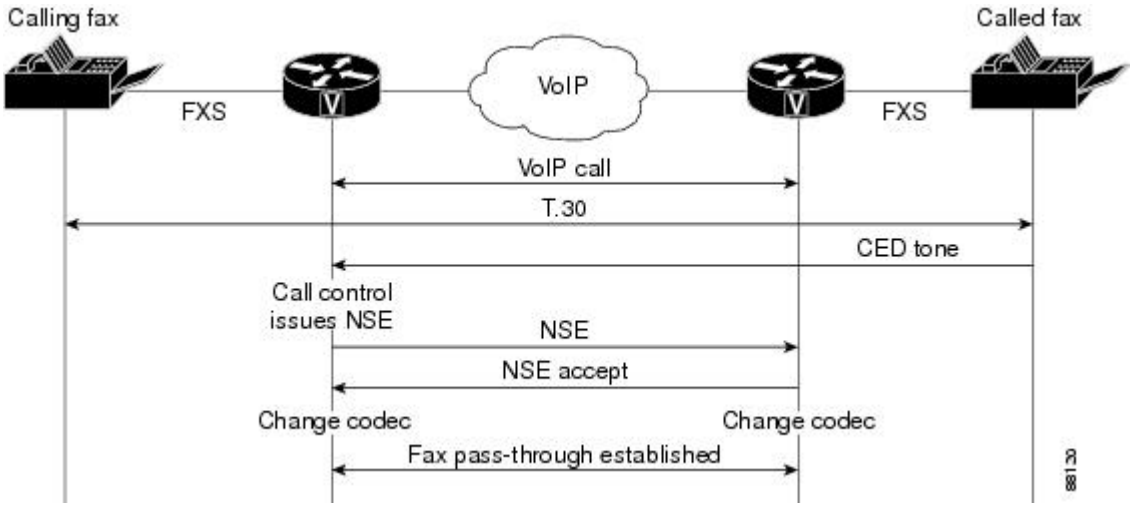
When a DSP is put into voice mode at the beginning of a VoIP call, the DSP is informed by the call control stack whether the control protocol can support pass-through or not. If pass-through is supported, the following events occur:

1. For the duration of the call, the DSP listens for the 2100-Hz CED tone to detect a fax or modem on the line.
2. If the CED tone is heard, an internal event is generated to alert the call control stack that a fax or modem changeover is required.
3. The call control stack on the OGW instructs the DSP to send an NSE to the TGW, informing the TGW of the request to carry out a codec change.
4. If the TGW supports NSEs, it responds to the OGW instruction and loads the new codec. The fax machines are able to communicate on an end-to-end basis with no further intervention by the voice gateways.

For configuration instructions, see Chapter 1, "Configuring Fax Pass-Through."

Fax pass-through call flow is shown in the figure below.

Figure 2: Fax Pass-Through and Fax Upspeed Call Flow



Cisco Fax Relay

Cisco fax relay is the oldest method of supporting fax on Cisco IOS gateways and has been supported since Cisco IOS Release 11.3. Cisco fax relay uses Real-Time Transport Protocol (RTP) as the method of transport. In Cisco fax relay mode, gateways terminate T.30 fax signaling by spoofing a virtual fax machine to the locally attached fax machine. The gateways use a Cisco-proprietary fax-relay RTP-based protocol to communicate between them.

Unlike fax pass-through, fax relay demodulates the fax modem bits at the local gateway, sends the information across the voice network using the fax relay protocol, and then remodulates the bits back into tones at the far gateway. The fax machines on either end are sending and receiving tones and are not aware that a demodulation/modulation fax relay process is occurring.

The default method for fax transmission on Cisco IOS gateways is Cisco fax relay. This is an RTP-based transmission method that uses proprietary signaling and encoding mechanisms. Cisco fax relay capability is widely available and has been in the Cisco IOS gateway software since Cisco IOS Release 11.3, which introduced DSPs to enable voice applications. The mechanism for Cisco fax relay is the same for calls that are controlled by SIP, MGCP, or H.323 call control protocols.

Before T.38 standards-based fax relay was introduced, no command-line interface (CLI) was required to enable Cisco fax relay. Today Cisco fax relay is still the default, but explicit CLI enables a choice between the fax relay methods.

Cisco fax relay is the default operation and, in the absence of any explicit CLI on the dial peer, is used when a fax transmission is detected. If voice calls are being completed successfully between two routers, fax calls should also work. Events that occur during a Cisco fax relay call fall into the following call phases:

For configuration information, see Chapter 1, "Configuring Cisco Fax Relay."

Cisco Fax Relay Fax Setup Phase

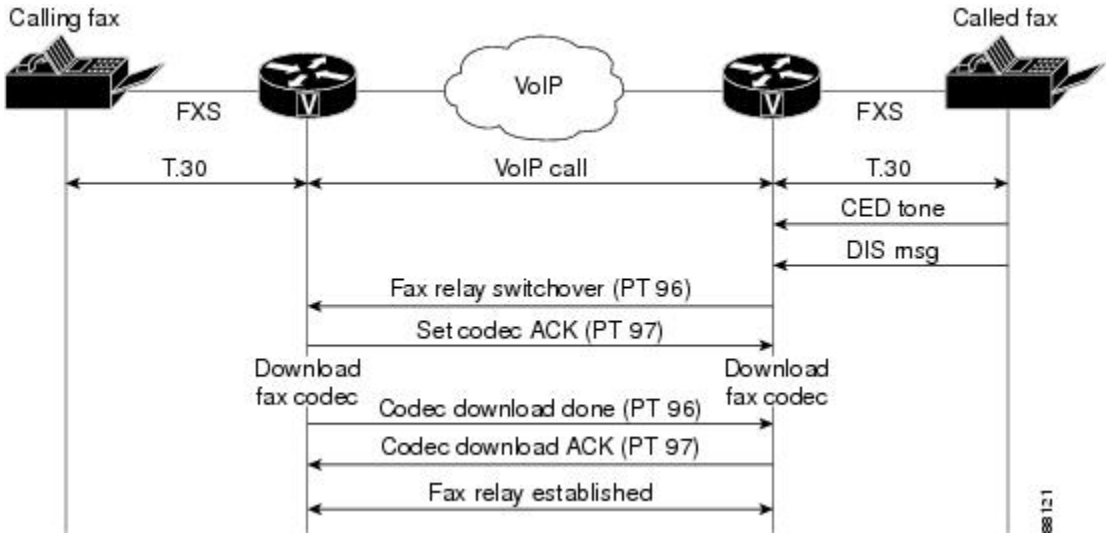
When a DSP is put into voice mode at the beginning of a VoIP call, the DSP is informed by the call control stack whether fax relay is supported and if it is supported, whether it is Cisco fax relay or T.38 fax relay. If Cisco fax relay is supported, the following events occur:

- Initially a VoIP call is established as if it were a normal speech call. Call control procedures are followed and the DSP is put into voice mode, after which human speech is expected to be received and processed.

- At any time during the life of the call, if a fax answer or calling tone (ANSam or CED) is heard, the DSP does not interfere with the speech processing. The ANSam or CED tone causes a switch to modem passthrough, if enabled, to allow the tone to pass cleanly to the remote fax.
- A normal fax machine, after generating a CED or hearing a CNG, sends a DIS message with the capabilities of the fax machine. The DSP in the Cisco IOS gateway attached to the fax machine that generated the DIS message (normally the TGW) detects the HDLC flag sequence at the start of the DIS message and initiates fax relay switchover. The DSP also triggers an internal event to notify the call control stack that fax switchover is required. The call control stack then instructs the DSP to change the RTP payload type to 96 and to send this payload type to the OGW.
- When the DSP on the OGW receives an RTP packet with payload type set to 96, it triggers an event to inform its own call control stack that a fax changeover has been requested by the remote gateway. The OGW then sends an RTP packet to the TGW with payload type 97 to indicate that the OGW has started the fax changeover. When the TGW receives the payload type 97 packet, the packet serves as an acknowledgement. The TGW starts the fax codec download and is ready for fax relay.
- Once the OGW has completed the codec download, it sends RTP packets with payload type 96 to the TGW. The TGW responds with an RTP packet with payload type 97, and fax relay can begin between the two gateways. As part of the fax codec download, other parameters such as VAD, jitter buffers, and echo cancellation are changed to suit the different characteristics of a fax call.

Cisco fax relay fax setup is shown in the figure below.

Figure 3: Cisco Fax Relay Fax Setup Call Flow



Cisco Fax Relay Data Transfer Phase

During fax relay operation, the T.30 analog fax signals are received from the PSTN or from a directly attached fax machine. The T.30 fax signals are demodulated by a DSP on the gateway and then packetized and sent across the VoIP network as data. The TGW decodes the data stream and remodulates the T.30 analog fax signals to be sent to the PSTN or to a destination fax machine.

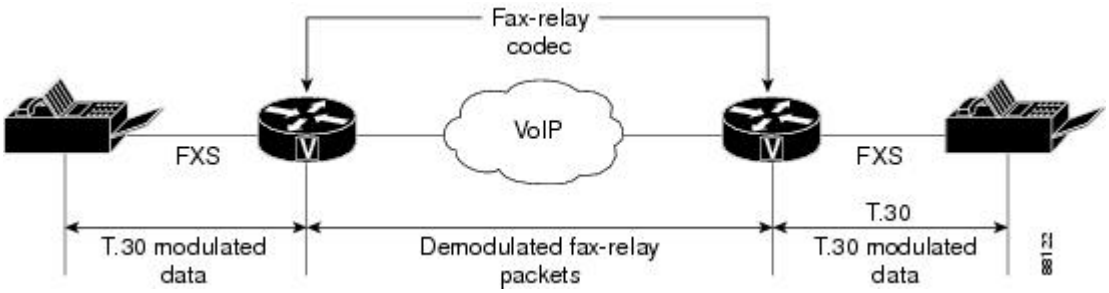
The messages that are demodulated and remodulated are predominantly the phase B, phase D, and phase E messages of a T.30 transaction. Most of the messages are passed across without any interference, but certain messages are modified according to the constraints of the VoIP network.

During phase B, fax machines interrogate each other's capabilities. They expect to communicate with each other across a 64-kbps PSTN circuit, and they attempt to make best use of the available bandwidth and circuit quality of a 64-kbps voice path. However, in a VoIP network, the fax machines do not have a 64-kbps PSTN circuit available. The bandwidth per call is probably less than 64 kbps, and the circuit is not considered a clear circuit.

Because transmission paths in VoIP networks are more limited than in the PSTN, Cisco IOS CLI is used to adjust fax settings on the VoIP dial peer. The adjusted fax settings restrict the facilities that are available to fax machines across the VoIP call leg and are also used to modify values in DIS and NSF messages that are received from fax machines.

The call flow of the Cisco fax relay data transfer phase is shown in the figure below.

Figure 4: Cisco Fax Relay Data Transfer Call Flow



T.38 Fax Relay

The T.38 fax relay feature provides an ITU-T standards-based method and protocols for fax relay. Data is packetized and encapsulated according to the T.38 standard. The encoding of the packet headers and the mechanism to switch from VoIP mode to fax relay mode are clearly defined in the specification. Annexes to the basic specification include details for operation under Session Initiation Protocol (SIP) and H.323 call control protocols.

T.38 fax relay provides an ITU-standard mechanism for a voice gateway to inform another voice gateway of the desire to change the media stream from a voice stream to a data stream. The desire to change the media stream is indicated by the call control protocol, and not through a change in the RTP payload or bearer information. Annexes to the T.38 specification define the switchover mechanism for the following call control protocols:

- H.323--T.38 Annex B
- SIP--T.38 Annex D

T.38 fax relay uses data redundancy to accommodate packet loss. During T.38 call establishment, voice gateways indicate the level of packet redundancy that they incorporate in their transmission of Facsimile User Datagram Packet Transport Layer packets (UDPTLs). The level of redundancy (the number of times that the packet is repeated) can be configured on Cisco IOS gateways.

There is work under way to implement T.38 fax switchover independently of the call control mechanisms. This is referred to as "bearer level signaling" and makes use of named signaling events (NSEs). The following sections address call-control-initiated switchover mechanisms:

For configuration information, see Chapter 1, "Configuring T.38 Fax Relay."

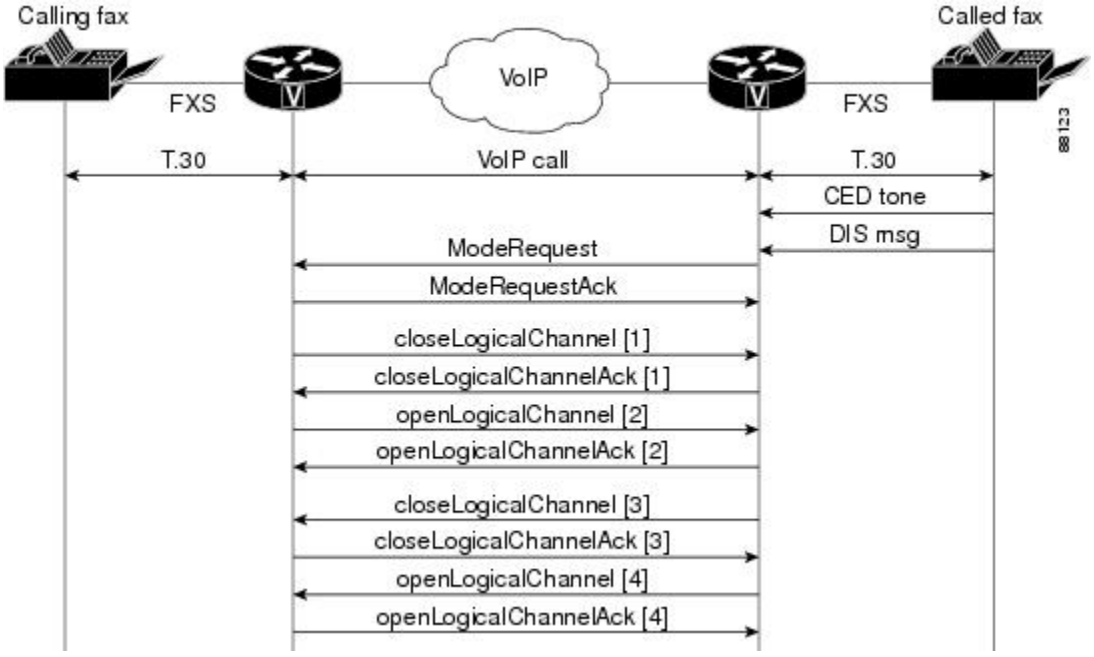
H.323 T.38 Fax Relay

The T.38 Annex B standard defines the mechanism that is used to switch over from voice mode to T.38 fax mode during a call. The ability to support T.38 must be indicated during the initial VoIP call setup. If the DSP on the gateway is capable of supporting T.38 mode, this information is indicated during the H.245 negotiation procedures as part of the regular H.323 VoIP call setup.

Once the VoIP call setup is completed, the DSP continues to listen for a fax tone. When a fax tone is heard, the DSP signals the receipt of fax tone to the call control layer, which then initiates fax changeover as specified in the T.38 Annex B procedures. The H.245 message flow shown in the figure below contains the following events:

1. The detecting TGW sends a ModeRequest message to the OGW, and the OGW responds with a ModeRequestAck.
2. The OGW sends a closeLogicalChannel message to close its VoIP UDP port, and the TGW responds with a closeLogicalChannelAck while it closes the VoIP port.
3. The OGW sends an openLogicalChannel message that indicates to which port to send the T.38 UDP information on the OGW, and the TGW responds with an openLogicalChannelAck.
4. The TGW sends a closeLogicalChannel message to close its VoIP UDP port, and the OGW responds with a closeLogicalChannelAck.
5. Finally the TGW sends an openLogicalChannel message that indicates to which port to send the T.38 UDP stream, and the OGW responds with an openLogicalChannelAck.
6. T.38-encoded UDP packets flow back and forth. At the end of the fax transmission, either gateway can initiate another ModeRequest message to return to VoIP mode.

Figure 5: H.323 T.38 Fax Relay Call Flow



SIP T.38 Fax Relay

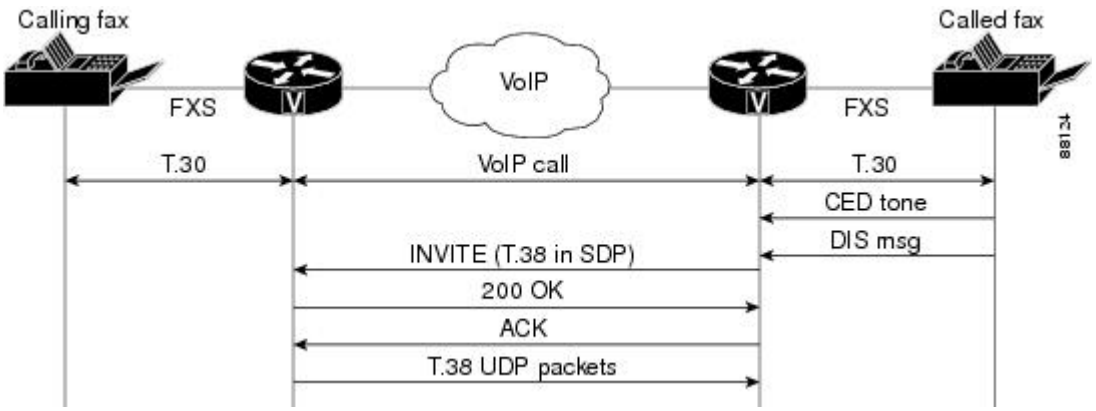
When the call control protocol is SIP, T.38 Annex D procedures are used for the changeover from VoIP to fax mode during a call. Initially, a normal VoIP call is established using SIP INVITEs. The DSP needs to be informed that it can support T.38 mode while it is put into voice mode. Then, during the call, when the DSP detects fax HDLC flags, it signals the detection of the flags to the call control layer, and the call control layer initiates a SIP INVITE mid-call to signal the desire to change the media stream.

Note For initial INVITE in SIP calls, Cisco UBE and voice gateways do not support having both fax (T.38) and audio capabilities together.

The SIP T.38 fax relay call flow shown in the figure below contains the following events:

1. The TGW detects a fax V.21 flag sequence and sends an INVITE with T.38 details in the SDP field to the OGW or to the SIP proxy server, depending on the network topology.
2. The OGW receives the INVITE message and sends back a 200 OK message.
3. The TGW acknowledges the 200 OK message and sends an ACK message direct to the OGW.
4. The OGW starts sending T.38 UDP packets instead of VoIP UDP packets across the same ports.
5. At the end of the fax transmission, another INVITE message can be sent to return to VoIP mode.

Figure 6: SIP T.38 Fax Relay Call Flow



MGCP T.38 Fax Relay

The MGCP T.38 fax relay feature conforms to ITU-T T.38, Procedures for Real-Time Group 3 Facsimile Communication over IP Networks, which determines procedures for real-time facsimile communication in various gateway control protocol (XGCP) applications.

MGCP T.38 fax relay provides two modes of implementation:

- Gateway-controlled mode--Gateways negotiate fax relay transmission by exchanging capability information in Session Description Protocol (SDP) messages. Transmission of SDP messages is transparent to the call agent. Gateway-controlled mode allows use of MGCP-based T.38 fax without the necessity of upgrading the call agent software to support the feature.

- Call-agent-controlled mode--Call agents use MGCP messaging to instruct gateways to process fax traffic. For MGCP T.38 fax relay, call agents can also instruct gateways to revert to gateway-controlled mode if the call agent is unable to handle the fax control messaging traffic; for example, in overloaded or congested networks.

MGCP-based T.38 fax relay enables interworking between the T.38 application that already exists on Cisco gateways and the MGCP applications on call agents.

MGCP-based T.38 fax relay has the following call flow:

1. A call is initially established as a voice call.
2. The gateways advertise capabilities in an SDP exchange during connection establishment.
3. If both gateways do not support T.38 fax relay, fax pass-through is used for fax transmission. If both gateways support T.38, they attempt to switch to T.38 upon fax tone detection. The existing audio channel is used for T.38 fax relay, and the existing connection port is reused to minimize delay. If failure occurs at some point during the switch to T.38, the call reverts to the original settings it had as a voice call. If this failure occurs, a fallback to fax pass-through is not supported.
4. Upon completion of the fax image transfer, the connection remains established and reverts to a voice call using the previously designated codec, unless the call agent instructs the gateways to do otherwise.

A fax relay MGCP event allows the gateway to notify the call agent of the status (start, stop, or failure) of T.38 processing for the connection. This event is sent in both call-agent-controlled and gateway-controlled mode.

Gateway-Controlled MGCP T.38 Fax Relay

In gateway-controlled mode, a call agent uses the fx: extension of the local connection option (LCO) to instruct a gateway about how to process a call. Gateways do not need instruction from the call agent to switch to T.38 mode. This mode is used if the call agent has not been upgraded to support T.38 and MGCP interworking, or if the call agent does not want to manage fax calls. Gateway-controlled mode can also be used to bypass the message delay overhead caused by call agent handling; for example, to meet time requirements for switchover to T.38 mode. If the call agent does not specify the mode to the gateway, the gateway defaults to gateway-controlled mode.

In gateway-controlled mode, the gateways exchange NSEs that do the following:

- Instruct the peer gateway to switch to T.38 for a fax transmission.
- Either acknowledge the switch and the readiness of the gateway to accept T.38 packets or indicate that the gateway cannot accept T.38 packets.

CA-Controlled MGCP T.38 Fax Relay

In call-agent (CA)-controlled mode, the call agent can instruct the gateway to switch to T.38 for a call. In Cisco IOS Release 12.3(1) and later releases, CA-controlled mode enables T.38 fax relay interworking between H.323 gateways and MGCP gateways and between two MGCP gateways under the control of a call agent. This feature supersedes previous methods for CA-controlled fax relay and introduces the following gateway capabilities to enable this functionality:

- Ability to accept the MGCP FXR package, to receive the fxr prefix in commands from the call agent, and to send the fxr prefix in notifications to the call agent.

- Ability to accept a new port when switching from voice to fax transmission during a call. This new ability allows successful T.38 CA-controlled fax between H.323 and MGCP gateways in those situations in which the H.323 gateway assigns a new port when changing a call from voice to fax. New ports are assigned in H.323 gateways using Cisco IOS images from Release 12.2(2)T to Release 12.2(7.5)T. Note that MGCP gateways in MGCP-to-MGCP fax calls simply reuse the same port. CA-controlled T.38 fax relay enables MGCP gateways to handle both situations, either switching to a new port or reusing the same port, as directed by the call agent.

T.37 Store-and-Forward Fax

The T.37 store-and-forward feature provides an ITU-T standards-based method for store-and-forward fax. The fax transmission process is divided into distinct sending and receiving phases with the potential to store the fax between sending and receiving, if necessary.

A store-and-forward fax gateway takes calls from G3 fax machines, converts them into e-mail messages, and sends them over an IP network. Another store-and-forward fax gateway at the terminating end of the network receives the e-mail message, converts it back into a fax message, and delivers it to a far-end G3 fax machine. The transmitting gateway is referred to as an on-ramp gateway, and the terminating gateway is referred to as an off-ramp gateway. With store-and-forward fax, you can do the following:

- Send and receive faxes to and from Group 3 fax devices.
- Receive faxes that are to be delivered as e-mail attachments.
- Create and send standard e-mail messages that are delivered as faxes to standard Group 3 fax devices.

Cisco fax gateways support the T.37 standard as independent on-ramp gateways, independent off-ramp gateways, or combined on-ramp and off-ramp gateways. The two phases, on-ramp fax and off-ramp fax, are often combined to provide fax throughput over an IP network. Advantages of T.37 store-and-forward fax include delivery at off-peak hours, sophisticated retry-on-busy algorithms, and the ability to broadcast a single fax to multiple receiving fax machines.

With store-and-forward fax, the on-ramp gateway receives a fax from a traditional PSTN-based Group 3 fax device and converts it into a Tagged Image File Format (TIFF) file attachment. The gateway creates a standard Multipurpose Internet Mail Extension (MIME) e-mail message and attaches the TIFF file to the e-mail. The gateway forwards the e-mail, now called a fax mail, and its attachment to the messaging infrastructure of a designated Simple Mail Transport Protocol (SMTP) server. The messaging infrastructure performs message routing, message storage, and transport, and can be custom store-and-forward SMTP software or a standard Internet mail transfer agent (MTA) such as UNIX sendmail or Netscape MailServer. The IETF standards for fax transmission are covered by RFC 2301 through 2306. TIFF-F describes the data format for compressed fax images.

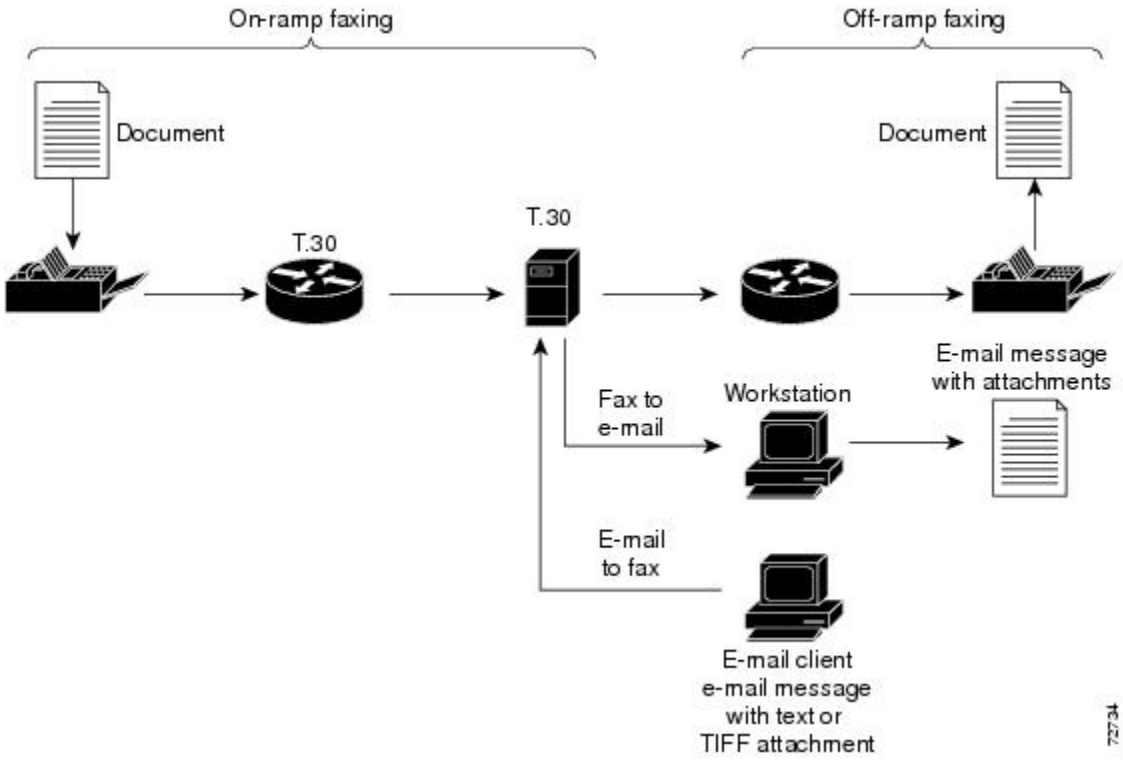
Many MTAs on the market work without modification with both the on-ramp and off-ramp features of store-and-forward fax. We recommend that you dedicate a mail server to fax mail and avoid the conflicting configuration requirements of traditional e-mail and fax-mail servers. Optimize each mail server for its individual functions--for example, fax messages should usually retry transmissions every 5 minutes whereas normal e-mail should retry every 30 minutes, and fax messages should give up after 3 to 4 hours whereas normal e-mail should not give up for 4 to 5 days.

After the fax mail is stored on the SMTP server, it can be delivered in two ways: either as an e-mail message with attachment when the recipient downloads e-mail messages or as a fax to a standard PSTN-based G3 fax device. In the latter case, the SMTP server mail delivery infrastructure delivers the fax mail to the off-ramp gateway, which converts the attached TIFF file back into standard fax format and then sends the information to a standard PSTN-based G3 fax device. The off-ramp gateway is also responsible for generating delivery status notifications (DSNs) and message disposition notifications (MDNs), as appropriate.

A topology for T.37 store-and-forward fax is shown in the figure below.

T.37 store-and-forward fax is implemented on Cisco gateways using TCL IVR applications. For configuration information, see Chapter 1, "Configuring T.37 Store-and-Forward Fax."

Figure 7: T.37 Store-and-Forward Fax Topology



IVR Applications for Fax

The following IVR applications have been developed for fax:

- T.37 store-and-forward fax--See the T.37 Store-and-Forward Fax, on page 16.

Fax Detection IVR Application

Fax detection supports the use of a single E.164 number for both voice mail and fax mail by providing the capability to detect through an interactive voice response interface whether an incoming call is voice or fax. Fax detection can be configured to use either the distinctive fax calling tones (CNG) or a manually dialed digit or both to distinguish fax calls from voice calls. Fax detection supports the following modes of operation:

- connect-first--The gateway connects incoming calls immediately to a voice-mail server, which plays a greeting, or audio prompt, based upon the number called. The gateway also listens for CNG throughout the duration of the call and connects the call to the configured fax application if CNG is detected.
- listen-first--The gateway listens for CNG for 9 seconds; an audio prompt can be played during this time. If CNG is detected, the call is connected to a fax application or server. If CNG is not detected, the call is connected to a voice application or server.

- default-voice--The gateway is configured to recognize a particular dual tone multifrequency (DTMF) tone to indicate voice calls and a different DTMF tone to indicate fax calls. If no DTMF tone is heard and no CNG tone is heard for 9 seconds, the call is treated as a voice call.
- default-fax--The gateway is configured to recognize a particular DTMF tone to indicate voice calls and a different DTMF tone to indicate fax calls. If no DTMF tone is heard and no CNG tone is heard for 9 seconds, the call is treated as a fax call.

For configuration information, see Chapter 1, "Configuring Fax Detection."

Fax Rollover IVR Application

The fax rollover IVR application provides a configured fallback to T.37 store-and-forward fax if a call attempts to use fax relay and fails. An OGW must be configured with fax relay, store-and-forward fax, and also with the fax rollover application. Then, if a fax relay attempt fails, the call is forwarded to an SMTP server by a mail transfer agent (MTA) using T.37-standard protocols for store-and-forward fax.

For configuration information, see Chapter 1, "Configuring Fax Rollover."

Information About Cisco IOS Modem Services over IP

Modem Passthrough over VoIP

When service providers and aggregators are implementing VoIP, they sometimes cannot separate data traffic from voice traffic. These carriers that aggregate voice traffic over VoIP infrastructures require service offerings to carry data as easily as voice.

Modem passthrough over VoIP provides for the transport of modem signals through a packet network by using pulse code modulation (PCM)-encoded packets.

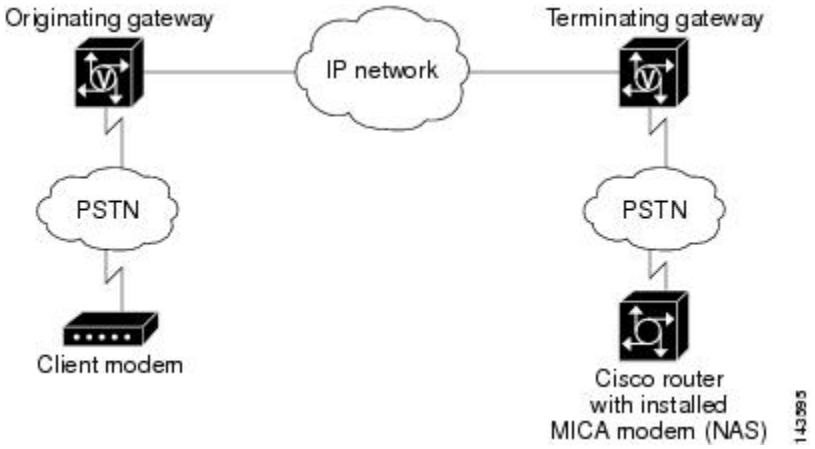
Modem passthrough performs the following functions:

- Suppressing processing functions like compression, echo cancellation, high-pass filter, and voice activity detection (VAD)
- Issuing redundant packets to protect against random packet drops
- Providing static jitter buffers of 200 milliseconds (ms) to protect against clock skew
- Differentiating modem signals from voice and fax signals, indicating the detection of the modem signal across the connection, and placing the connection in a state that transports the signal across the network with the least distortion
- Maintaining a modem connection reliably across the packet network for a long duration under normal network conditions

On detection of the modem answer tone, the gateways switch into modem passthrough mode. With modem passthrough, the modem traffic is carried between the two gateways in real-time transport protocol (RTP) packets, using an uncompressed or lightly compressed voice codec--G.711 u-law, G.711 a-law, or Voice Band Data (VBD). Packet redundancy may be used to mitigate the effects of packet loss in the IP network. Even so, modem passthrough remains susceptible to packet loss, jitter, and latency in the IP network.

The figure below illustrates the connection from the client modem to a modem ISDN channel aggregation (MICA) technologies modem network access server (NAS).

Figure 8: Modem Passthrough in an IP Network



Voice Band Data

The modem passthrough feature is also known as Voice Band Data (VBD) by the International Telecommunication Union (ITU). VBD refers to the transport of modem signals over a voice channel through a packet network with an encoding appropriate for modem signals. The minimum set of coders for VBD mode is G.711 ulaw and alaw.

For VBD mode of operation, the path between the originating and answering gateway remains in a voice configuration. The modem signals are encoded using an appropriate speech codec suitable for the task, and samples are transported across a packet network. Currently G.711 is supported.

Some system requirements for the use of VBD follow:

- Use a voice codec that passes voice band modulated signals with minimal distortion.
- Have end-to-end constant latency.
- Disable Voice Activity Detection (VAD) and Comfort Noise Generation (CNG) during the data transfer phase.
- Disable any DC removal filters that may be integral with the speech encoder used.
- Be capable of tone detection, including mid-call dual tone multifrequency (DTMF), as well insertion of tones, announcements, and voice prompts.

Note To use VBD, you should consider the appropriate application of echo cancellers on a VBD channel.

Passthrough Switchover

When the gateways detect a data modem, both the originating gateway and the terminating gateway switch to modem passthrough mode. This switchover includes the following:

- Switching to the G.711 codec
- Disabling the high pass filter

- Disabling Voice Activity Detection (VAD)
- Using special jitter buffer management algorithms
- On detection of modem phase reversal tone, disabling the echo canceler

At the end of the modem or fax call, the voice ports revert to the previous configuration and the DSPs switch back to the original voice codec.

Note The gateway detects modems operating at speeds up to V.90.

Controlled Redundancy

Packet loss is a persistent issue in voice applications. The disruption of speech, which is characteristic of packet loss, can be somewhat resolved with controlled redundancy and the RTP (RFC 2198). Controlled redundancy reconstructs missing information at the receiver end from the redundant data that arrives in the transmitted packets.

Some of the requirements for a controlled redundancy are as follows:

- The packets have to carry a primary encoding and one redundant encoding.
- Because the use of variable size encodings is desirable, each encoded block in the packet must have a length indicator.
- The RTP header provides a time-stamp field that corresponds to the time of creation of the encoded data and redundant blocks of data correspond to different time intervals than the primary data. So each block of redundant encoding requires its own time stamp.

You can enable redundancy so that the modem and fax passthrough switchover causes the gateway to transmit redundant packets and redundancy can be enabled in one or both of the gateways. When only one gateway is configured, the other gateway receives the packets correctly, but does not produce redundant packets. When redundancy is enabled, 10-ms sample-sized packets are sent. When redundancy is disabled, 20-ms sample-sized packets are sent.

Note The current Cisco implementation of RFC 2198 reflects a redundant encoding of 1X or 1 repeat of the original packet. This means that any loss scenario in which two or more consecutive packets are dropped would cause a loss of data translated into a retrain, Failure To Train (FTT), or call drop, etc. in modem and fax passthrough.

Clock Slip Buffer Management

When the gateways detect a data modem, both the originating gateway and the terminating gateway switch from dynamic and adaptive buffers to static de-jitter buffers. The use of a static de-jitter buffer is required for modem passthrough because the adaptation process in a dynamic de-jitter buffer causes a retrain on the modem connection. When the modem call is concluded, the voice ports revert to dynamic jitter buffers.

In addition, the modem passthrough data management algorithm is designed to handle and compensate for clocking differences in the PSTN between the originating and terminating gateways. This additional clock-slip monitoring prevents issues that show up in long duration modem calls.

Modem Relay over VoIP

The Modem Relay feature provides support for modem connections across traditional time-division multiplexing (TDM) networks. Modem relay demodulates a modem signal at one voice gateway and passes it as packet data to another voice gateway where the signal is remodulated and sent to a receiving modem. On detection of the modem answer tone, the gateways switch into modem passthrough mode and then, if the call menu (CM) signal is detected, the two gateways switch into modem relay mode.

Differences Between Modem Passthrough and Modem Relay

There are two ways to transport modem traffic over VoIP networks:

- With modem passthrough, the modem traffic is carried between the two gateways in RTP packets, using an uncompressed voice codec--G.711 u-law or a-law. Although modem passthrough remains susceptible to packet loss, jitter, and latency in the IP network, packet redundancy may be used to mitigate the effects of packet loss in the IP network.
- With modem relay, the modem signals are demodulated at one gateway, converted to digital form, and carried in Simple Packet Relay Transport (SPRT) protocol (which is a protocol running over User Datagram Protocol (UDP)) packets to the other gateway, where the modem signal is recreated and remodulated, and passed to the receiving modem.

In this implementation, the call starts out as a voice call, then switches into modem passthrough mode, and then into modem relay mode.

Modem Tone Detection and Signaling

This implementation of modem relay supports V.34 modulation and the V.42 error correction and link layer protocol with maximum transfer rates of up to 33.6 kbps. It forces higher-rate modems to train down to the supported rates. Signaling support includes the Session Initiation Protocol (SIP), MGCP/SGCP, and H.323:

- For MGCP and SIP, during the call setup, the gateways negotiate the following:
  - To use or not use modem relay mode
  - To use or not use gateway exchange identification
  - The value of the payload type for NSE packets
- For H.323, the gateways negotiate the following:
  - To use or not use modem relay mode
  - To use or not use gateway exchange identification

Benifits of Modem Relay

Modem relay on VoIP offers the following benefits:

- Modem tone detection
- Packetized modem signal transmission over the WAN
- Significant reduction of dropped packet, latency, and jitter effects on modem sessions
- Reduction of bandwidth used (as compared to modem passthrough)

Packet Redundancy

You can enable payload redundancy so that the modem relay VoIP switchover causes the gateway to send redundant packets. Redundancy can be enabled in one or both of the gateways. When only a single gateway is configured for redundancy, the other gateway receives the packets correctly, but does not produce redundant packets. When redundancy is enabled, 10-ms sample-sized packets are sent. When redundancy is disabled, 20-ms sample-sized packets are sent.

Note By default, modem relay over VoIP capability and redundancy are disabled.

Clock Slip Buffer Management

When the gateways detect a data modem, both the originating and the terminating gateways switch from dynamic jitter buffers to static jitter buffers of 200-ms depth. The switch from dynamic to static is designed to compensate for Public Switched Telephone Network (PSTN) clocking differences at the originating and terminating gateways. When the modem call is concluded, the voice ports revert to dynamic jitter buffers.

Additional References

Developer Support

Developers using this guide may be interested in joining the Cisco Developer Support Program. This program was created to provide you with a consistent level of support that you can depend on while leveraging Cisco interfaces in your development projects.

The Developer Support Program provides formalized support for Cisco Systems interfaces to enable developers, customers, and partners in the Cisco Technology Developer program to accelerate their delivery of compatible solutions.

The Developer Support Engineers are an extension of the product technology engineering teams. They have direct access to the resources necessary to provide expert support in a timely manner.

Note Cisco Technical Assistance Center (TAC) support does not include Cisco Developer Support and is limited to Cisco product installation/configuration and Cisco-developed applications. A signed Developer Support Agreement is required to participate in this program. For more details on how to obtain a Developer Support agreement go to http://www.cisco.com/go/developersupport under "Ordering" or contact developer-support@cisco.com.

Related Documents

Related Topic	Document Title
Cisco IOS command references	• *Cisco IOS Debug Command Reference* • *Cisco IOS Voice Command Reference*

Related Topic	Document Title
Cisco IOS security features, including authentication, authorization, and accounting (AAA)	*Cisco IOS Security Configuration Guide*
Cisco IOS voice troubleshooting information	*Cisco IOS Voice Troubleshooting and Monitoring Guide*
Cisco MGCP configuration information	*Cisco IOS MGCP and Related Protocols Configuration Guide*
Cisco SIP configuration information	*Cisco IOS SIP Configuration Guide*
Network configuration	*Cisco IOS IP Application Services Configuration Guide*

Standards

Standards[1]	Title
ITU-T T.4	*Standardization of Group 3 facsimile terminals for document transmission*
ITU-T T.30	*Procedures for document facsimile transmission in the general switched telephone network*
ITU-T.37	Procedures for the Transfer of Facsimile Data via Store-and-Forward on the Internet, June 1998
ITU-T.38	Procedures for Real-Time Group 3 Facsimile Communication over IP Networks, June 1998
ITU-T.38	Procedures for Real-Time Group 3 Facsimile Communication over IP Networks, Amendment 1, April 1999
ITU-T.38	Revised Annex B of Recommendation T.38, November 1998
ITU-T.38	Revised Annex D of Recommendation T.38, November 1998
Fax Standards	
T.4	Defines the encoding of printed information (content) into a digital stream ready for modulation.
T.30	Defines the handshaking protocol and capabilities exchange that takes place during fax transmission.
T.30 Annex A	Defines Error Correction Mode (ECM) facilities.
Fax and Modem Standards	
V.8	Part of the capabilities exchange during the modem and fax answering procedures.
V.17	High speed data transmission, used for high transfer rates of High Speed (HS) fax page data (9600 to 14400 bps).

Standards[1]	Title
V.21	Low Speed (LS) data transmission, used for the fax control information (300 baud).
V.22bis	Medium speed data transmission, used for low transfer rates of High Speed (HS) fax page data (1200 to 2400 bps).
V.25	Modem and fax machine answering procedures.
V.27	High speed data transmission, used for medium transfer rates of High Speed (HS) fax page data (2400 to 4800 bps).
V.29	High speed data transmission, used for medium transfer rates of High Speed (HS) fax page data (4800 to 9600 bps).
V.34	Very high speed modems--A modem operating at rates of up to 33,600 bps for use on the PSTN and on leased point-to-point 2-wire telephone-type circuits.
V.90	A digital modem and analog modem pair for use on the PSTN at data rates of up to 56,000 bps downstream and up to 33,600 bps upstream.

[1] Not all supported standards are listed.

MIBs

MIBs[2]	MIBs Link
• CISCO-CALL-APPLICATION-MIB • CISCO-CAS-IF-MIB • CISCO-DSP-MGMT-MIB • CISCO-ISDN-MIB • CISCO-MMAIL-DIAL-CONTROL-MIB • CISCO-VOICE-DNIS-MIB • CISCO-VOICE-IF-MIB • CISCO-VOICE-NUMBER-EXPANSION-MIB • DIAL-CONTROL=MIB • EXPRESSION-MIB • IF-MIB(MIB II)	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

[2] Not all supported MIBs are listed.

RFCs

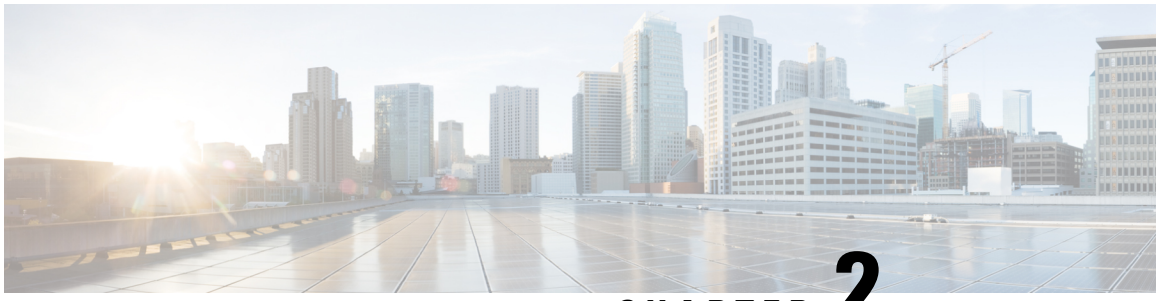
RFCs[3]	Title
RFC 821	>*Simple Mail Transfer Protocol*
RFC 822	>*Standard for the Format of ARPA Internet Text Messages*
RFC 1123	>*Requirements for Internet Hosts--Application and Support*
RFC 1652	>*SMTP Service Extension for 8 bit-MIME Transport*
RFC 1869	*SMTP Service Extensions*
RFC 1891	>*SMTP Service Extension for Delivery Status Notifications*
RFC 1892	>*The Multipart/Report Content Type for the Reporting of Mail System Administrative Messages*
RFC 1893	>*Enhanced Mail System Status Codes*
RFC 1894	>*An Extensible Message Format for Delivery Status Notifications*
RFC 1896	>*The Text/Enriched MIME Content-Type*
RFC 2034	>*SMTP Service Extension for Returning Enhanced Error Codes*
RFC 2045	>*Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies*
RFC 2046	>*Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types*
RFC 2047	>*MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text*
RFC 2197	>*SMTP Service Extension for Command Pipelining*
RFC 2198	RTP Payload for Redundant Audio Data
RFC 2298	>*An Extensible Message Format for Message Disposition Notifications*
RFC 2301	>*File Format for Internet Fax*

RFCs[3]	Title
RFC 2302	Tagged >*Image File Format (TIFF)--Image/TIFF MIME Sub-Type Registration*
RFC 2303	>*Minimal PSTN Address Format in Internet Mail*
RFC 2304	>*Minimal Fax Address Format in Internet Mail*
RFC 2305	>*A Simple Mode of Fax Using Internet Mail*
RFC 2306	*Tag Image File Format (TIFF)--Profile for Facsimile*
RFC 2326	Real Time Streaming Protocol (RTSP)
RFC 2327	SDP: Session Description Protocol
RFC 2532	>*Extended Facsimile Using Internet Mail*
RFC 2543	SIP: Session Initiation Protocol
RFC 2705	Media Gateway Control Protocol
RFC 2821	*Simple Mail Transfer Protocol*
RFC 2833	RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
RFC 2865	*Remote Authentication Dial In User Service (RADIUS)*
RFC 2866	*RADIUS Accounting*

[3] Not all supported RFCs are listed.

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport



CHAPTER 2

Configuring Modem Passthrough

Configuring Modem Passthrough

Modem Passthrough over VoIP provides the transport of modem signals through a packet network by using pulse code modulation (PCM) encoded packets. This chapter describes the configuration for modem passthrough.

Your software release may not support all the features documented in this chapter. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn . An account on Cisco.com is not required.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring Modem Passthrough

Before configuring modem passthrough, perform the following tasks:

- Establish a working VoIP-enabled network.
- Verify network suitability to pass modem traffic. The key characteristics of the network are packet loss, delay, and jitter. These characteristics can be determined by using the Service Assurance Agent (SAA) feature of Cisco IOS software.
- Configure clock sourcing on the T1 controller on the voice gateway that connects to the PSTN. For modem passthrough to operate correctly, the gateway clock must be synced with the PSTN clock. See the following example configuration:

```
!
controller T1 0
 framing esf
 linecode b8zs
 clock source line
 channel-group 1 timeslots 1-24 speed 64
 !
```

Note Configure clock sourcing for all interfaces connected to the PSTN.

Restrictions for Configuring Modem Passthrough

Restrictions for configuring modem passthrough are as follows:

- The **modem passthrough protocol** and **fax protocol**commands cannot be configured at the same time. If you enter either one of these commands when the other is already configured, the command-line interface returns an error message. The error message serves as a confirmation notice because the **modem passthrough protocol** command is internally treated the same as the **fax protocol pass-through** command by the Cisco IOS software. For example, no other mode of fax protocol (for example, fax protocol T.38) can operate if the **modem passthrough protocol** command is configured.
- Even though the **modem passthrough protocol** and **fax protocol pass-through** commands are treated the same internally, be aware that if you change the configuration from the **modem passthrough protocol**command to the **modem passthrough nse**command, the configured **fax protocol pass-through** command is not automatically reset to the default. If default settings are required for the **fax protocol**command, you have to specifically configure the **fax protocol** command.

Information About Modem Passthrough

Modem Passthrough Functions

Modem passthrough over VoIP performs the following functions:

- Represses processing functions like compression, echo cancellation, high-pass filter, and voice activity detection (VAD).
- Issues redundant packets to protect against random packet drops.
- Provides static jitter buffers of 200 milliseconds to protect against clock skew.
- Discriminates modem signals from voice and fax signals, indicating the detection of the modem signal across the connection, and placing the connection in a state that transports the signal across the network with the least amount of distortion.
- Reliably maintains a modem connection across the packet network for a long duration under normal network conditions.

Passthrough Rollover

When the gateway detects a data modem, both the originating gateway and the terminating gateway roll over to G.711. The roll over to G.711 disables the high-pass filter, disables echo cancellation, and disables VAD. At the end of the modem call, the voice ports revert to the prior configuration and the digital signal processor (DSP) goes back to the state before the rollover.

Note The gateway can detect modems at speeds up to V.90.

Payload Redundancy

Payload redundancy enables the modem passthrough switchover and this causes the gateway to emit redundant packets. When redundancy is enabled, 10-ms sample-sized packets are sent. When redundancy is disabled, 20-ms sample-sized packets are sent.

Redundancy is enabled on one or both of the gateways. When only a single gateway is configured for redundancy, the second gateway receives the packets correctly but does not produce redundant packets.

Clock Slip Buffer Management

When the gateway detects a data modem, both the originating gateway and the terminating gateway switch from dynamic jitter buffers to static jitter buffers of 200-ms depth. The switch from dynamic to static is to compensate for PSTN clocking differences at the originating gateway and the terminating gateway. At the conclusion of a modem call, the voice ports revert to dynamic jitter buffers.

How to Configure Modem Passthrough

Modem passthrough can be configured at two levels:

The two configuration tasks can be used separately or together. If both are configured, the dial-peer configuration overrides the global configuration.

Note You must configure modem passthrough on both the originating and terminating gateways.

Configuring Modem Passthrough Globally

Use the following steps to configure modem passthrough for all the dial peers on a gateway.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **modem passthrough** {**nse**| **protocol**}[**payload-type** *number*] **codec** {**g711ulaw** | **g711alaw**} [**redundancy** [**maximum-sessions** *sessions*] [**sample-duration** [**10** | **20**]]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

Step 3	**voice service voip**
	Example:
	`Router(config)#`
	`voice service voip`
		Enters voice-service configuration mode and configures voice service for all gateway connections.

Step 4	**modem passthrough** {**nse**| **protocol**}[**payload-type** *number*] **codec** {**g711ulaw** | **g711alaw**} [**redundancy** [**maximum-sessions** *sessions*] [**sample-duration** [**10** | **20**]]] **Example:** **Example:** `Router(conf-voi-serv)# modem passthrough nse payload-type 101 codec g711ulaw redundancy maximum-sessions 1`	Configures modem passthrough for all dial peers on the gateway. The default behavior is **no modem passthrough**. • **nse** --Specifies that named signaling events (NSEs) are used to communicate codec switchover between gateways. • **protocol** --Session Initiation Protocol (SIP)/H.323 protocol is used to signal modem pass-through. • **payload-type** *number*--(Optional) NSE payload type. Range varies, but is from 96 to 119 on most platforms. For details, refer to command-line interface (CLI) help. Default is 100. **Note** The **payload-type** must match on the originating and terminating gateways. • **codec** --Codec selections for upspeed. • **g711ulaw**--Codec G.711 u-law, 64000 bits per second for T1. • **g711alaw**--Codec G.711 a-law, 64000 bits per second for E1. • **redundancy** --(Optional) Enables a single repetition of packets (using RFC 2198) to improve reliability by protecting against packet loss. • **maximum-sessions** *value* --(Optional) Maximum number of simultaneous pass-through sessions. Ranges and defaults vary by platform.

Configuring Modem Passthrough for a Specific Dial Peer

You must configure a VoIP dial peer on both the originating and terminating gateways to match the call--for example, using a destination pattern.

When the **system** keyword is entered, the following parameters are not available: **nse**, **payload-type**, **codec**, and **redundancy**. The configuration is taken from the **modem passthrough nse**command in voice-service configuration mode.

Note When modem passthrough is configured for a specific dial peer, the dial-peer configuration takes precedence over the global configuration.

Use the following steps to configure modem passthrough for a specific dial peer.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **voip**
4. **modem passthrough** {**system** | **nse** [**payload-type** *number*] **codec** {**g711ulaw** | **g711alaw**} [**redundancy**]}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 20 voip`	Enters dial-peer configuration mode and names a specific VoIP dial peer. • *tag* --Digits that define a particular dial peer. Range is from 1 to 2147483647. • **voip** --Indicates that this is a VoIP peer that uses voice encapsulation on the POTS network.
Step 4	**modem passthrough** {**system**	**nse** [**payload-type** *number*] **codec** {**g711ulaw**	**g711alaw**} [**redundancy**]} **Example:** `Router(config-dial-peer)# modem passthrough nse codec g711ulaw redundancy`	Configures modem passthrough for a specific dial peer. The default behavior for modem passthrough in dial-peerconfiguration mode is **modem passthrough system**. • **system** --Defaults to the global configuration.

	Command or Action	Purpose

		• **nse** --Specifies that named signaling events (NSEs) are used to communicate codec switchover between gateways.
		  • **payload-type** *number*--(Optional) NSE payload type. Range varies by platform, but is from 96 to 119 on most platforms. The default is 100.
		• **codec** --Codec selections for upspeeding.
		  • **g711ulaw**--Codec G.711 u-law 64000 bits per second for T1.
		  • **g711alaw**--Codec G.711 a-law 64000 bits per second for E1.
		• **redundancy** --(Optional) Enables a single repetition of packets (using RFC 2198) to improve reliability by protecting against packet loss.

Troubleshooting Tips for Modem Passthrough

Use the following steps to troubleshoot modem passthrough:

- Ensure that you can make a voice call.
- Ensure that modem passthrough over VoIP is configured on both the originating gateway and the terminating gateway.
- Ensure that the originating and terminating gateways have the same NSE payload-type number.
- When two gateways are configured in voice-service configuration mode, ensure that the originating and terminating gateways have the same **maximum-sessions** value.

Use the following commands to troubleshoot modem passthrough:

- **debug voip vtsp** --Displays information about the voice telephony service provider (VTSP).
- **debug vtsp** --Used to trace how the router interacts with the digital signal processor (DSP) based on the signaling indications from the signaling stack and requests from the application. Effective with Cisco IOS Release 12.3(8)T, this command was replaced by the **debug voip vtsp**command.
- **show dial-peer voice** --Used to verify that modem passthrough over VoIP is enabled.
- **show call active voice** --Displays the voice information for the active call table.
- **show call history voice** --Displays the voice information for the call history table.
- **show dial-peer voice** --Displays configuration information for dial peers.

To verify that modem passthrough is configured, you can use the **show call active voice brief** command. In the following sample output, the IP call leg shows the keyword MODEMPASS to signify that the call is in modem passthrough mode:

```
11DD : 1 1565860ms.1 +15340 pid:2 Answer 100 active
```

```
dur 00:00:19 tx:864/110008 rx:858/102929
Tele 0/0/0 (1) [0/0/0] tx:12270/12270/0ms g711ulaw noise:-11 acom:6 i/0:-14/-59 dBm
11DD : 2 1570100ms.1 +11090 pid:1 Originate 200 active
dur 00:00:19 tx:858/102929 rx:864/103096
IP 1.1.1.2:16610 SRTP: off rtt:1ms pl:40/0ms lost:0/0/0 delay:60/60/60ms g711ulaw TextRelay:
 off
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a MODEMPASS nse
buf:0/0 loss 0% 0/0 last 1031s dur:0/0s
```

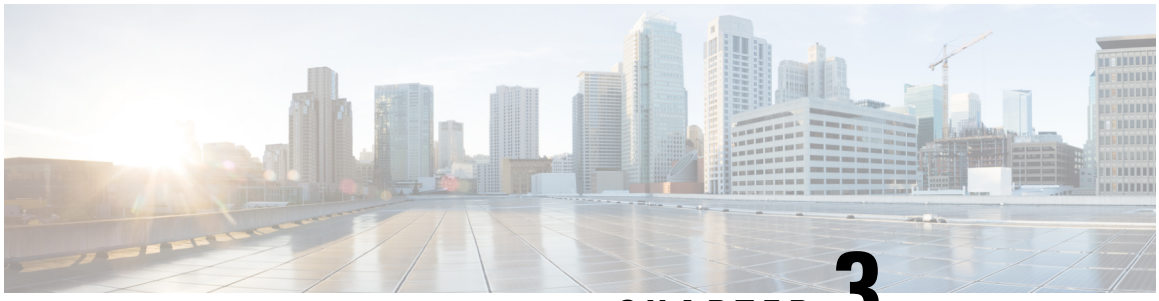
Configuration Examples for Modem Passthrough

Modem Passthrough Configuration for Cisco AS5300 Example

The following is sample configuration for the Modem Passthrough over VoIP feature for the Cisco AS5300 universal access servers:

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
voice service voip
 modem passthrough nse codec g711ulaw redundancy maximum-session 5
!
resource-pool disable
!
ip subnet-zero
ip ftp source-interface Ethernet0
ip ftp username lab
ip ftp password lab
no ip domain-lookup
!
isdn switch-type primary-5ess
cns event-service server
!
mta receive maximum-recipients 0
!
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 pri-group timeslots 1-24
!
controller T1 1
 shutdown
 clock source line secondary 1
!
interface Ethernet0
 ip address 10.10.2.2 255.0.0.0
 no ip route-cache
 no ip mroute-cache
!
interface Serial0:23
 no ip address
 encapsulation ppp
 ip mroute-cache
 no logging event link-status
 isdn switch-type primary-5ess
 isdn incoming-voice modem
 no peer default ip address
```

```
 no fair-queue
 no cdp enable
 no ppp lcp fast-start
!
interface FastEthernet0
 ip address 172.16.0.1 255.0.0.0
 no ip route-cache
 no ip mroute-cache
 load-interval 30
 duplex full
 speed auto
 no cdp enable
!
ip classless
ip route 192.168.0.0 255.255.0.0 10.10.1.1
no ip http server
!
voice-port 0:D
!
dial-peer voice 1 pots
 incoming called-number 55511..
 destination-pattern 020..
 direct-inward-dial
 port 0:D
 prefix 020
!
dial-peer voice 2 voip
 incoming called-number 020..
 destination-pattern 55511..
 modem passthrough nse codec g711ulaw redundancy
 session target ipv4:10.10.0.2
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 login
!
```



CHAPTER 3

Configuring Cisco Modem Relay

Configuring Cisco Modem Relay

This chapter describes the configuration of Cisco modem relay. Cisco modem relay provides support for modem connections across traditional time division multiplexing (TDM) networks. Modem relay demodulates a modem signal at one voice gateway and passes it as packet data to another voice gateway where the signal is remodulated and sent to a receiving modem.

History for the Modem Relay Feature

Release	Modification
12.2(11)T	This feature was introduced on the following platforms: Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, Cisco 7200 series, and Cisco AS5300.
12.4(4)T	The **gw-controlled** keyword was added to the **modem relay (dial-peer)**, **modem relay (voice-service)**, and **mgcp modem relay voip mode** commands.

Finding Support Information for Platforms and Cisco IOS Software Images

Your Cisco IOS software release may not support all of the features documented in this chapter. For the latest feature information and caveats, see the release notes for your platform and software release. Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn . An account on Cisco.com is not required.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring Cisco Modem Relay

Before you configure Cisco modem relay, perform the following steps:

- Establish a working H.323, SIP, or MGCP network for voice calls.
- Ensure that you have a Cisco IOS image that supports gateway-controlled modem relay.
- Determine network suitability to relay modem traffic. The key attributes are packet loss, delay, and jitter. These characteristics of the network can be determined by using the Cisco IOS Service Assurance Agent (SAA) feature.
- For TI 549 DSPs, you must configure high codec complexity for the originating and terminating gateways.

Restrictions for Configuring Cisco Modem Relay

Restrictions of Cisco modem relay are as follows:

- This feature does not work with third-party gateways.
- Cisco modem relay does not support the V.150.1 signaling standard.
- The originating gateway and the terminating gateway must both be configured for Cisco modem relay. If one gateway is configured for modem pass-through, the call occurs using modem pass-through.
- Both gateways must be configured for a high or flex codec complexity to use Cisco modem relay. If either the originating or terminating gateway is configured for a medium complexity codec, modem passthrough is used.
- The NSE 199 event signal is sent with triple redundancy once from the terminating gateway. If this signal is lost or not recognized, the call occurs using modem pass-through.
- Gateway-XID is enabled by default when Cisco modem relay is configured.
- There is no mechanism to indicate that an upspeed has not taken place because of a CAC failure, regardless of tone detection.
- Cisco modem relay works only if both modems are high-speed modems (V.34, V.90) that use V.42*bis* bidirectional compression. For low-speed modems, gateways that carry traffic use modem pass-through.
- Cisco modem relay works only if both modems use the V.42 error correction protocol and if the error correction layer in both modems is enabled.
- MGCP, H.323, and SIP can be configured on the same gateway with some restrictions--all calls in a particular T1 or E1 must be handled by MGCP, H.323, or SIP. If your gateway has multiple T1 or E1 facilities, calls on some T1s or E1s can be managed by MGCP and others can be managed by H.323 or SIP.

Information about Cisco Modem Relay

Modem relay demodulates a modem signal at one voice gateway and passes it as packet data to another voice gateway where the signal is remodulated and sent to a receiving modem. On detection of the modem answer tone, the gateways switch into modem passthrough mode and then, if the call menu (CM) signal is detected, the two gateways switch into modem relay mode.

Codec complexity determines the codec types supported on the DSP.

- The TI 5510 DSP supports medium, high, and flex complexity. The default is flex complexity.
- The TI 549 DSP supports only high complexity.

If your platform uses the TI 549 DSP, you must configure high codec complexity.

Cisco modem relay using MGCP and H.323 supports the following high complexity codecs:

- Clear channel: Clear channel at 64000 bps
- g711alaw: G.711 a-law 64000 bps
- g711ulaw: G.711 u-law 64000 bps
- g723ar53: G.723.1 Annex-A 5300 bps
- g723ar63: G.723.1 Annex-A 6300 bps
- g723r53: G.723.1 5300 bps
- g723r63: G.723.1 6300 bps
- g726r16: G.726 16000 bps
- g726r24: G.726 24000 bps
- g726r32: G.726 32000 bps
- g728: G.728 16000 bps
- g729br8: G.729 Annex-B 8000 bps
- g729r8: G.729 8000 bps
- gsmefr: GSMEFR 12200 bps
- gsmfr: GSMFR 13200 bps

Cisco modem relay using SIP supports the following high complexity codecs:

- g711alaw: G.711 a-law 64000 bps
- g711ulaw: G.711 u-law 64000 bps
- g723r63: G.723.1 6300 bps
- g723r16: G.723.1 1600 bps
- g728: G.728 16000 bps
- g729r8: G.729 8000 bps

Any MGCP command is applicable to the entire gateway. For MGCP calls, dial peers do not affect call handling because call agent takes care of the call routing. When configured, the following commands affect MGCP calls only and not H.323 calls. H.323 and MGCP commands must be configured separately.

Modes for Modem Transport

There are two ways to transport modem traffic over VoIP networks:

- With modem passthrough, the modem traffic is carried between the two gateways in RTP packets, using an uncompressed voice codec--G.711 u-law or a-law. Although modem passthrough remains susceptible to packet loss, jitter, and latency in the IP network, packet redundancy may be used to mitigate the effects of packet loss in the IP network.
- With modem relay, the modem signals are demodulated at one gateway, converted to digital form, and carried in Simple Packet Relay Transport (SPRT) protocol (which is a protocol running over User Datagram Protocol (UDP)) packets to the other gateway, where the modem signal is recreated and remodulated, and passed to the receiving modem.

Modem relay significantly reduces the effects that dropped packets, latency and jitter have on the modem session. Compared to modem passthrough, it also reduces the amount of bandwidth used.

Modem Tone Detection and Signaling

Modem relay supports V.34 modulation and the V.42 error correction and link layer protocol with maximum transfer rates of up to 33.6 kbps. It forces higher-rate modems to train down to the supported rates. Signaling support includes the session initiation protocol (SIP), MGCP/SGCP, and H.323:

- For MGCP and SIP, during the call setup, the gateways negotiate the following:
  - To use or not use the modem relay mode
  - To use or not use the gateway-xid
  - The value of the payload type for named signaling event (NSE) packets
- For H.323, the gateways negotiate the following:
  - To use or not use the modem relay mode
  - To use or not use the gateway-xid

Relay Switchover

When the gateways detect a data modem, both the originating gateway and the terminating gateway switch to modem passthrough mode. This includes the following elements:

- Switching to the G.711 codec
- Disabling the high pass filter
- Disabling voice activity detection (VAD)
- Using special jitter buffer management algorithms
- On detection of modem phase reversal tone, disabling the echo canceler

At the end of the modem call, the voice ports revert to the previous configuration and the digital signal processors (DSPs) switch back to the state before switchover. You can configure the codec by selecting the g711alaw or g711ulaw option of the codec command.

Payload Redundancy

You can enable payload redundancy so that the modem passthrough over VoIP switchover causes the gateway to send redundant packets. Redundancy can be enabled in one or both of the gateways. When only a single gateway is configured for redundancy, the other gateway receives the packets correctly, but does not produce redundant packets. When redundancy is enabled, 10-ms sample-sized packets are sent. When redundancy is disabled, 20-ms sample-sized packets are sent.

Note By default, modem relay over VoIP capability and redundancy are disabled.

Dynamic and Static Jitter Buffers

When the gateways detect a data modem, both the originating gateway and the terminating gateway switch from dynamic jitter buffers to static jitter buffers of 200-ms depth. The switch from dynamic to static is designed to compensate for Public Switched Telephone Network (PSTN) clocking differences at the originating and terminating gateways. When the modem call is concluded, the voice ports revert to dynamic jitter buffers.

Gateway-Controlled Modem Relay

Beginning with Cisco IOS Release, 12.4(4)T, Cisco supports gateway-controlled negotiation parameters for modem relay. This new feature is a nonnegotiated, bearer-switched mode for modem transport that does not involve call-agent-assisted negotiation during the call setup. Instead, the negotiation parameters are configured directly on the gateway. These gateway-controlled negotiation parameters use named signaling events (NSEs) to indicate the switchover from voice, to voice-band data (VBD), to modem relay.

Upon detecting 2100-Hz tone, the terminating gateway sends an NSE 192 to the originating gateway and switches over to modem pass-through. The terminating gateway also sends an NSE 199 to indicate modem relay. If this event is recognized by the originating gateway, the call occurs as modem relay. If the event is not recognized, the call occurs as modem pass-through.

Because Cisco modem relay uses configured parameters, it removes the signaling dependency from the call-agent and allows modem relay support independent of call control. Cisco modem relay can be deployed over any call-agent that is capable of setting up a voice connection between gateways, including Cisco CallManager, Cisco CallManager Express, and the BTS/PGW softswitches.

The gateway-controlled modem relay parameters are enabled by default when Cisco modem relay is configured, and when Cisco modem relay is configured, gateway exchange identification (XID) parameter negotiation is always enabled. Gateway XID parameters are negotiated using the Simple Packet Relay Transport (SPRT) protocol.

How to Configure Modem Relay

Note You must configure modem relay on *both* the originating and terminating gateways for this feature to operate.

Configuring Codec Complexity for TI 549 DSPs

To configure high codec complexity for the Cisco 2600, Cisco 2800, Cisco 3600, Cisco 3700, and Cisco 3800 series routers on both the originating and terminating gateways, follow these steps:

Note The VG224 and IAD2430 platforms only support flex complexity.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice-card** *slot*
4. **codec complexity** {**flex** | **high** | **medium**} [**ecan-extended**]
5. **description**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice-card** *slot* **Example:** `Router(config)# voice-card 0`	Enters voice-card configuration mode. • *slot--S* pecifies the voice-card slot location.

Step 4	**codec complexity** {**flex** | **high** | **medium**} [**ecan-extended**]
	Example:
	`Router(config-voice-card)#`
	`codec complexity high`
		Specifies call density and codec complexity according to the codec standard that is being used.
		• **flex** --Each DSP can support up to 16 voice channels, depending on voice traffic.
		• **high** --each DSP supports six voice channels
		• **medium** --each DSP supports eight voice channels
		• **ecan-extended** --Optional) Selects the extended echo canceller.

Step 5	**description** **Example:** `Router(config-dspfarm)# description`	(Optional) Enters a string to include descriptive text about this DSP interface connection. This information is displayed in the output for show commands and does not affect the operation of the interface.

Configuring MGCP Modem Relay

Use the following steps to configure MGCP modem relay:

- To configure MGCP modem relay using PRI, follow steps 1 to 6.
- To configure MGCP modem relay using CAS, follow steps 1 to 9.
- To change modem relay parameters from their default values, follow steps 10 to 12.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mgcp** [*port*]
4. **mgcp call-agent** {*dns-name* | *ip-address*} [*port*] [**service-type** *type*] [**version** *protocol-version*]
5. **mgcp tse payload** *value*
6. **mgcp modem relay voip mode nse** {[**codec** [**g711alaw**| **g711ulaw**]] [**redundancy**]} **gw-controlled**
7. **dial-peer voice** *tag* **pots**
8. **application** *application-name* [**out-bound**]
9. **port** *controller number* **:D**
10. **mgcp modem relay voip gateway-xid** [**compress** {**backward** | **both** | **forward** | **no**}] [**dictionary** *value*] [**string-length** *value*]
11. **mgcp modem relay voip latency** *value*
12. **mgcp modem relay voip sprt retries** *value*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**mgcp** [*port*] **Example:** `Router(config)# mgcp 4204`	Allocates resources for MGCP and starts the MGCP daemon. • *port* --(Optional) User Datagram Protocol (UDP) port for the MGCP gateway. Range is from 1025 to 65535. The default is UDP port 2427.
Step 4	**mgcp call-agent** {*dns-name* | *ip-address*} [*port*] [**service-type** *type*] [**version** *protocol-version*] **Example:**	Configures the address and protocol of the call agent for MGCP endpoints on a gateway.

	Command or Action	Purpose

	`Router(config)# mgcp call-agent 192.168.200.225 service-type mgcp version 1.0`	• *dns-name* --Fully qualified domain name (including host portion) for the call agent; for example, ca123.example.net.
		• *ip-address* --IP address for the call agent.
		• *port* --(Optional) UDP port over which the gateway sends messages to the call agent. Range is from 1025 to 65535.
		• **service-type** *type* --(Optional) Type of Gateway control service protocol. It can be one of the following values:
		  • **mgcp**--Media Gateway Control Protocol
		  • **ncs**--Network Communication Server
		  • **sgcp**--Simple Gateway Control Protocol
		  • **tgcp**--Trunking Gateway Control Protocol
		• **version** *protocol-version* --(Optional) Version of gateway control service protocol. It can be one of the following values:
		
		For **service-type mgcp**:
		• • **0.1** --Version 0.1 of MGCP (Internet Draft)
		  • **1.0** --Version 1.0 of MGCP (RFC2705 Version 1.0)
		
		Note This configuration value is used to allow the router to tailor the MGCP application behavior to be compatible based on the RFC2705 definitions.
		
		• • For **service-type ncs**: 1.0
		  • For **service-type sgcp**: 1.1, 1.5
		  • For **service-type tgcp**: 1.0

Step 5	**mgcp tse payload** *value* **Example:** `Router(config)# mgcp tse payload 100`	Enables inband telephony signaling events (TSEs) and specifies the payload value to be used during fax and modem passthrough and network continuity tests. • *value* --TSE payload value. Range is from 98 to 119. The default is 100.
Step 6	**mgcp modem relay voip mode nse** {[**codec** [**g711alaw**| **g711ulaw**]] [**redundancy**]} **gw-controlled** **Example:**	Configures Cisco modem relay parameters for MGCP. • **nse** --Named signaling event. • **codec** --Sets the voice compression selection for speech or audio signals.

	Command or Action	Purpose
	`Router(config)# mgcp modem relay voip mode nse codec g711ulaw redundancy gw-controlled`	• **g711alaw** is required for E1. • **g711ulaw** is required for T1. • **redundancy** --(Optional) Sends redundant packets for modem traffic during the pass-through phase. Disabled by default. • **gw-controlled** --Sets the gateway-configured method for establishing modem relay parameters. Enabled by default.
Step 7	**dial-peer voice** *tag* **pots** **Example:** `Router(config)# dial-peer voice 12 pots`	(Optional) Creates a data dial peer and enters dial-peer configuration mode. • *tag* --Specifies the dial-peer identifying number. The range is 1 to 2147483647. • **pots** --Specifies an incoming POTS dial peer.
Step 8	**application** *application-name* [**out-bound**] **Example:** `Router(config-dial-peer)# application MGCPAPP`	(Optional) Enable a specific application on a dial peer • *application-name* --Name of the predefined application that you wish to enable on the dial peer. Use **MGCPAPP** to enable the MGCP application on a dial-peer. • **out-bound** --(Optional) Outbound calls are handed off to the named application. This keyword is used for store-and-forward fax applications and VoiceXML applications.
Step 9	**port** *controller number* **:D** **Example:** `Router(congfig-dial-peer)# port 0:D`	(Optional) Associates a dial peer with a specific voice port. • *controller number* --T1 or E1 controller. • **:D** --The D channel associated with ISDN PRI.

Step 10	**mgcp modem relay voip gateway-xid** [**compress** {**backward** | **both** | **forward** | **no**}] [**dictionary** *value*] [**string-length** *value*]
	Example:
	`Router(config)# mgcp modem relay voip gateway-xid compress both dictionary 1024 string-length 32`
		(Optional) Enables in-band negotiation of compression parameters between two VoIP gateways using MGCP.
		• **compress** --(Optional) Direction in which data flow is compressed.
		  • **backward**--Enables compression only in the backward direction.
		  • **both**--Enables compression in both directions. For normal dialup, this is the preferred setting. This is the default.
		  • **forward**--Enables compression only in the forward direction.
		  • **no**--Disables compression in both directions.

	Command or Action	Purpose
		• **dictionary** *value* --(Optional) V.42bis parameter that specifies characteristics of the compression algorithm. The range is 512 to 2048. The default is 1024. • **string-length** *value* --(Optional) V.42bis parameter that specifies characteristics of the compression algorithm. The range is 16 to 32. The default is 32.
Step 11	**mgcp modem relay voip latency** *value* **Example:** `Router(config)# mgcp modem relay voip latency 100`	(Optional) Optimizes the Modem Relay Transport Protocol and the estimated one-way delay across the IP network MGCP. • *value* --Estimated one-way delay across the IP network, in milliseconds. The range is 100 to 1000. The default is 200.
Step 12	**mgcp modem relay voip sprt retries** *value* **Example:** `Router(config)# mgcp modem relay voip sprt retries 15`	(Optional) Sets the maximum number of times that the Simple Packet Relay Transport (SPRT) protocol tries to send a packet before disconnecting. • *value* --Maximum number of times that the SPRT protocol tries to send a packet before disconnecting. Range is from 6 to 30. The default is 12.

Configuring H.323 and SIP Modem Relay

For H.323 and SIP configurations, Cisco modem relay can be configured at two levels:

The two configuration tasks can be used separately or together. If both are configured, the dial-peer configuration overrides the global configuration.

Note You must configure Cisco modem relay parameters on originating and terminating gateways. The NSE **payload-type** *number*, **codec**,and negotiation parameter settings must match.

Configuring Cisco Modem Relay Parameters Globally for H.323 and SIP

Use the following steps to configure Cisco modem relay parameters globally.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **h323**
5. **call start slow**
6. **modem relay nse payload-type** *number*] **codec** {**g711ulaw**| **g711alaw**} [**redundancy**] [**maximum-sessions** *value*] **gw-controlled**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Router(config)# voice service voip`	Enters voice-service configuration mode.
Step 4	**h323** **Example:** `Router(config-voi-serv)# h323`	Enters H.323 voice service configuration mode.
Step 5	**call start slow** **Example:** `Router(config-serv-h323)# call start slow`	Forces an H.323 gateway to use slow-connect procedures for all VoIP calls.

Step 6	**modem relay nse payload-type** *number*] **codec** {**g711ulaw**| **g711alaw**} [**redundancy**] [**maximum-sessions** *value*] **gw-controlled**
	Example:
	`Router(conf-voi-serv)# modem relay nse payload-type 100 codec g711ulaw redundancy maximum-sessions 1 gw-controlled`
		Configures Cisco modem relay parameters.
		• **nse** --Named signaling event.
		• **payload-type** --(Optional) Sets the **payload-type** for NSE packets. The default number is 100.
		• **codec** --Sets the upspeed voice compression selection for speech or audio signals.
		  • **g711ulaw** is required for T1.
		  • **g711alaw** is required for E1.
		• **redundancy** --(Optional) Sends redundant packets for modem traffic during the pass-through phase. Disabled by default.
		• **maximum-sessions** --(Optional) Maximum number of redundant, simultaneous modem pass-through sessions. The default is 16.
		• **gw-controlled** --Sets the gateway-configured method for establishing modem relay parameters. Enabled by default.

Configuring H.323 and SIP Modem Relay for a Specific Dial Peer

Use the following steps to configure Cisco modem relay for a specific dial peer:

Note When Cisco modem relay is configured for a specific dial peer, the dial-peer configuration takes precedence over the global configuration.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **voip**
4. **modem relay** {**system** | **nse** [**payload-type** *number*] **codec** {**g711ulaw**| **g711alaw**}[**redundancy**]} **gw-controlled**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 12 voip`	Enters dial-peer configuration mode for a specific dial peer.

Step 4	**modem relay** {**system**	**nse** [**payload-type** *number*] **codec** {**g711ulaw**| **g711alaw**}[**redundancy**]} **gw-controlled**
		Example:
		`Router(config-dial-peer)# modem relay nse payload-type 100 codec g711ulaw redundancy gw-controlled`
			Configures Cisco modem relay parameters.
			• **system** --Uses the global configuration parameters set by using the **modem relay** command in voice-service configuration mode. Enabled by default.
			• **nse** --Named signaling event.
			• **payload-type** --(Optional) Sets the **payload-type** for NSE packets. The default is 100.
			• **codec** --Sets the upspeed voice compression selection for speech or audio signals.
			  • **g711ulaw** is required for T1.
			  • **g711alaw** is required for E1.

	Command or Action	Purpose
		• **redundancy** --(Optional) Sends redundant packets for modem traffic during the pass-through phase. Disabled by default. • **gw-controlled** --Uses the gateway-configured method for establishing modem relay parameters. Enabled by default.

Troubleshooting Tips

This section provides information and CLI commands for verifying and troubleshooting Cisco modem relay.

Using debug Commands for Troubleshooting

Before using **debug** commands to troubleshoot Cisco modem relay, be sure that:

- You can complete a voice call.
- Cisco modem relay is configured on both the originating and terminating gateways.
- Both the originating and terminating gateways have the same named signaling event (NSE) **payload-type** *number* and **codec**parameters.

Use the following **debug** commands to troubleshoot Cisco modem relay:

- To verify that parameter negotiation has occurred, use these **debug** commands:
  - **debug mgcp packet**--Use to check that modem relay parameters are not sent in SDP for MGCP calls.
  - **debug h245 asn1**--Use to check that modem relay parameters are not sent as part of H.245 messaging.
  - **debug ccsip calls**--Use to check SIP messages.
- The following are additional **debug** commands for troubleshooting:
  - **debug voip hpi all**--Use to check for event 199.
  - **debug voip dsmp all**--Use to check for event 199 and check for modem relay parameters.
  - **debug voip dsmp session**--Use to see if event 199 has been implemented for this session.

Note See the *Cisco IOS Debug Command Reference* for additional modem relay **debug**commands.

Using the show call active voice brief Command for Verification

To verify that modem relay is configured, you can use the **show call active voice brief**command. The following sample output shows MODEMRELAY in both the POTS and IP call legs and MODEMRELAY in the POTS call leg. Note that MODEMPASS is present for modem relay calls because modem relay calls go into modem passthrough mode before entering modem relay:

```
11E2 : 3 644890ms.1 +5390 pid:2 Answer 100 active
dur 00:12:03 tx:7089/139236 rx:112/10110
Tele 0/0/0 (3) [0/0/0] tx:0/0/0ms modem-relay noise:0 acom:0 i/0:0/0 dBm
MODEMRELAY info:0/0/0 xid:1/1 total:0/0/0
```

```
speeds(bps): local 28800/31200 remote 28800/31200 phy/ec v34/v42 gateway-controlled
11E2 : 4 647210ms.1 +3070 pid:1 Originate 200 active
dur 00:12:03 tx:6956/51275 rx:7089/82524
IP 1.1.1.2:17692 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:60/60/60ms modem-relay TextRelay:
 off
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a MODEMPASS nse
buf:0/0 loss 0% 0/0 last 0s dur:0/0s
```

DSP Modem Relay Termination Codes

Another troubleshooting method is to view the gateway DSP modem relay termination codes that display when you enter the **debug hpi all** command. The DSP-to-host messages for the modem relay termination indicate modem relay session termination time, physical or link layer, and other causes for disconnection. On receiving this indication from the DSP, the host can disconnect the call or place the channel in modem pass-through state. The table below lists the modem relay termination cause codes.

Table 2: Modem Relay Termination Cause Codes

Modem Relay Termination Cause Code	Description
0x65	SPRT--Channel 1 max retransmit count exceeded on DSP.
0x66	SPRT--Channel 1 invalid transport frame type in transmit queue.
0x67	SPRT--Channel 2 max retransmit count exceeded on DSP.
0x68	SPRT--Channel 2 invalid transport frame type in transmit queue.
0x69	SPRT--Channel 1 invalid base sequence number received by DSP from remote host.
0x6A	SPRT--Channel 2 invalid base sequence number received by DSP from remote host.
0x6B	SPRT--Received RELEASE request from peer.
0x6C	SPRT--Channel 1 invalid transmit sequence number.
0x6D	SPRT--Channel 2 invalid transmit sequence number.
0x6E	SPRT--Invalid transmit t_frame type.
0x6F	SPRT--Requested to transmit null (zero length) info t_frame.
0x71	V42--Unexpected SABME received.
0x72	V42--Client modem capability appears incompatible with V42bis capability on originating leg gateway.
0x73	V42--Client modem capability appears incompatible with V42bis capability on terminating leg gateway.
0x74	V42--Exceeded max XID retransmit count.
0x77	V42--Exceeded max SABME retransmit count.

Modem Relay Termination Cause Code	Description
0x78	V42--NR sequence exception.
0x79	V42--Invalid acknowledgement received.
0x7A	V42--Exceeded N401 retransmit count.
0x7B	SPRT--Requested to transmit info t_frame that exceeds max allowed size.
0x7C	V42--Received V42 DISC packet from client modem.
0x7D	V42--Received V42 FRMR packet from client modem.
0x82	V42--Failed to add packet to V42 transmit queue.
0x8C	V42--Invalid "VA".
0x8D	PHYSICAL--Modem data pump terminated/failed.
0xC9	SPRT--Channel 1 max retransmit count exceeded on line card.
0xCA	SPRT--Channel 2 max retransmit count exceeded on line card.
0xCD	SPRT--Channel 1 invalid base sequence number received by line card from DSP.
0xCE	SPRT--Channel 2 invalid base sequence number received by line card from DSP.
0xCF	SPRT--Channel 1 invalid base sequence number received by line card from remote host.
0xD0	SPRT--Channel 2 invalid base sequence number received by line card from remote host.

Configuration Examples for Cisco Modem Relay

Cisco Modem Relay Enabled for MGCP Example

The following example shows an MGCP configuration with modem relay voip mode NSE enabled, redundant packets, and by default, modem relay parameters that are configured on the gateway.

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption!
hostname Router
!
boot-start-marker
boot system flash:c2800nm-ipvoice-mz.andante_0224
boot-end-marker
!
card type t1 1 1
```

```
logging buffered 10000000 debugging
enable password lab
!
no aaa new-model
!
resource manager
!
clock timezone PST -8
clock summer-time PDT recurring
network-clock-participate slot 1
ip subnet-zero
!
ip cef
no ip dhcp use vrf connected
!
ip domain list cisco.com
no ip domain lookup
ip domain name cisco.com
ip host ccm 10.3.102.99
no ftp-server write-enable
isdn switch-type primary-qsig
!
voice-card 0
 codec complexity high
 dspfarm
!
voice-card 1
 dspfarm
!
voice service pots
!
voice service voip
 no fax-relay sg3-to-g3
 h323
 modem relay nse codec g711ulaw gw-controlled
!
voice service voatm
!
controller T1 1/0
 framing esf
 clock source internal
 linecode b8zs
 pri-group timeslots 1-12,16,24
!
controller T1 1/1
 framing esf
 clock source internal
 linecode b8zs
 pri-group timeslots 1-8,16,24 service mgcp
!
interface GigabitEthernet0/0
 ip address 10.2.109.103 255.255.0.0
 duplex auto
 speed auto
 no clns route-cache
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial1/0:23
 no ip address
```

```
 no logging event link-status
 isdn switch-type primary-qsig
 isdn incoming-voice voice
 no cdp enable
!
interface Serial1/1:23
 no ip address
 no logging event link-status
 isdn switch-type primary-qsig
 isdn incoming-voice voice
 isdn bind-l3 ccm-manager
 no cdp enable
!
ip default-gateway 10.2.0.1
ip classless
ip route 10.0.0.0 255.0.0.0 10.2.0.1
ip route 192.168.254.254 255.255.255.255 GigabitEthernet0/0
!
ip http server
!
control-plane
!
voice-port 0/0/0
!
voice-port 0/0/1
!
voice-port 1/0:23
 connection plar 2000
!
voice-port 1/1:23
!
ccm-manager mgcp
ccm-manager music-on-hold
ccm-manager config server 10.3.102.99
!
mgcp
mgcp call-agent ccm service-type mgcp version 0.1
mgcp dtmf-relay voip codec all mode out-of-band
mgcp rtp unreachable timeout 1000 action notify
mgcp modem relay voip mode nse redundancy gw-controlled
mgcp package-capability rtp-package
no mgcp package-capability res-package
mgcp package-capability sst-package
no mgcp package-capability fxr-package
mgcp package-capability pre-package
no mgcp timer receive-rtcp
mgcp sdp simple
mgcp fax t38 inhibit
no mgcp fax-relay sg3-to-g3
mgcp rtp payload-type g726r16 static
!
mgcp profile default
!
dial-peer voice 2000 voip
 destination-pattern 2...
 session target ipv4:10.2.109.104
!
dial-peer voice 3000 voip
 destination-pattern 3...
 modem relay nse codec g711ulaw gw-controlled
 session protocol sipv2
 session target ipv4:10.2.109.104
!
dial-peer voice 2 pots
```

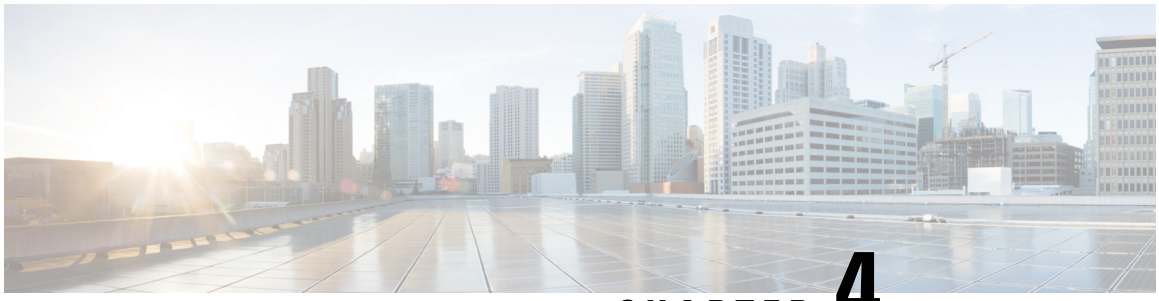
```
 incoming called-number 2...
 no digit-strip
 port 1/1:23
!
dial-peer voice 3 pots
 incoming called-number 3...
 no digit-strip
 port 1/0:23
!
dial-peer voice 5000 voip
!
dial-peer voice 10001 pots
!
dial-peer voice 10002 voip
!
dial-peer voice 1000 pots
!
dial-peer voice 6000 pots
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 exec-timeout 0 0
 password lab
 login
!
scheduler allocate 20000 1000
ntp clock-period 17180156
ntp server 10.2.0.1 prefer
!
end
```

Dial Peer Configured by System Settings Example

In this example, dial peer 2000 is configured to use modem relay NSE mode, the G.711 a-law codec, redundant packets, and modem relay parameters that are configured on the gateway.

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot system flash:c2691-ipvoice-mz.andante_0224
boot-end-marker
!
logging buffered 100000 debugging
enable password lab
!
no aaa new-model
!
resource manager
!
memory-size iomem 25
clock timezone PST -8
clock summer-time PDT recurring
no network-clock-participate slot 1
voice-card 1
 codec complexity high
```

```
 dspfarm
!
ip subnet-zero
ip cef
!
no ip dhcp use vrf connected
!
no ip domain lookup
no ftp-server write-enable
!
voice service voip
 fax protocol pass-through g711ulaw
 sip
!
controller T1 1/0
 framing sf
 linecode ami
!
controller T1 1/1
 framing sf
 linecode ami
!
interface FastEthernet0/0
 ip address 10.2.109.104 255.255.0.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
ip default-gateway 10.2.0.1
ip classless
ip route 10.0.0.0 255.255.255.255 10.2.0.1
!
no ip http server
!
control-plane
!
dial-peer voice 2000 voip
 modem relay nse codec g711alaw redundancy gw-controlled
 fax rate disable
 fax protocol pass-through g711alaw
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 1
 exec-timeout 0 0
 password lab
 login
line vty 2 4
 login
!
ntp clock-period 17180780
ntp server 192.168.254.253 prefer
!
end
```



CHAPTER 4

Configuring Fax Pass-Through

Configuring Fax Pass-Through

This chapter describes the configuration of fax pass-through. With fax pass-through, modulated fax information from the PSTN is passed in-band over a voice speech path in an IP network. Fax pass-through disables compression, echo cancellation, and issues redundant packets to ensure complete transmission.

Your software release may not support all the features documented in this chapter. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn . An account on Cisco.com is not required.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring Fax Pass-Through

Before you configure fax pass-through, perform the following tasks:

- Ensure that you install a software release that supports fax pass-through.
- Ensure that you have a working H.323 or SIP network for voice calls.
- Complete voice interoperability testing with third-party gateways and gatekeepers.
- Verify network suitability for fax pass-through by determining the packet loss threshold. Packet loss and latency are two impairments that can have a dramatic effect on fax pass-through performance.

Restrictions for Configuring Fax Pass-Through

Restrictions for fax pass-through are as follows:

- Fax pass-through does not support the switch from G.Clear to G.711. If fax pass-through and the G.Clear codec are both configured, the gateway cannot detect the fax tone.
- The Cisco AS5400 and Cisco AS5850 have the following limitations on the number of ports that can run fax pass-through simultaneously.

Subsystems are defined for these platforms, starting from port 0 and grouping consecutive ports 36 at a time. There are 3 subsystems per dfc108 card on the Cisco AS5400 (3 times 36 for a total of 108 ports) and 9 subsystems on the Cisco AS5850 tetryl card (9 times 36 for a total of 324 ports). The limitations are as follows:

- • Thirty-six 10- or 20-ms fax pass-through sessions with no redundancy
  • Thirty 20-ms fax pass-through sessions with redundancy
  • Twenty 10-ms fax pass-through sessions with redundancy

Examples of fax pass-through sessions mixed with a high load voice session type are as follows:

- • Ten 10-ms fax pass-through sessions and 20 G711, no VAD sessions
  • Twelve 10-ms fax pass-through sessions and 16 G.711, no VAD sessions
- With 10-ms fax pass-through, each subsystem has a 20-session fax pass-through limit. With 20-ms fax pass-through, each subsystem has a 30-session fax pass-through limit. The same limitations would apply to all subsequent subsystems.

The Cisco AS5400 and Cisco AS5850 have a capability to transmit 20-ms packets and receive 10-ms packets, which significantly improves performance over what can currently be handled with 10-ms packets in both directions. Currently, other Cisco universal gateway implementations may have an outgoing packet size limitation that imposes the use of 10-ms packets, as opposed to 20-ms packets, which is the optimal setting. This restriction limits the number of ports that can run fax pass-through to 20 per subsystem (10-ms connections only).

Note The **modem passthrough protocol** and **fax protocol**commands cannot be configured at the same time. If you enter either one of these commands when the other is already configured, the command-line interface returns an error message. The error message serves as a confirmation notice because the **modem passthrough protocol** command is internally treated the same as the **fax protocol pass-through** command by the Cisco IOS software. For example, no other mode of fax protocol (for example, fax protocol T.38) can operate if the **modem passthrough protocol** command is configured.

Note Even though the **modem passthrough protocol** and **fax protocol pass-through** commands are treated the same internally, be aware that if you change the configuration from the **modem passthrough protocol**command to the **modem passthrough nse** command, the configured **fax protocol pass-through** command is not automatically reset to the default. If default settings are required for the **fax protocol** command, you have to specifically configure the **fax protocol** command.

Information About Fax Pass-Through

Pass-Through Method of Transport

Fax pass-through takes place when incoming T.30 fax data is not demodulated or compressed for its transit through the packet network. The two endpoints (fax machines or modems) communicate directly to each other over a transparent IP connection. The gateway does not distinguish fax calls from voice calls.

On detection of a fax tone on an established VoIP call, the gateways switch into fax pass-through mode by suspending the voice codec and loading the pass-through parameters for the duration of the fax session. This process, called upspeeding, changes the bandwidth needed for the call to the equivalent of G.711.

With pass-through, the fax traffic is carried between the two gateways in RTP packets using an uncompressed format resembling the G.711 codec. This method of transporting fax traffic takes a constant 64-kbps (payload) stream plus its IP overhead end-to-end for the duration of the call. IP overhead is 16 kbps for normal voice traffic, but when switching to pass-through, the packetization period is reduced from 20 ms to 10 ms, which means that half as much data can be put into each frame. The result is that you need twice as many frames and twice as much IP overhead. For pass-through, the total bandwidth is 64 plus 32 kbps, for a total of 96 kbps. For normal voice traffic, total bandwidth is 64 plus 16 kbps, for a total of 80 kbps.

Packet redundancy may be used to mitigate the effects of packet loss in the IP network. Even so, fax pass-through remains susceptible to packet loss, jitter, and latency in the IP network. The two endpoints must be clocked synchronously for this type of transport to work predictably.

Performance may become an issue. To attempt to mitigate packet loss in the network, redundant encoding (1X or one repeat of the original packet) is used, which doubles the amount of data transferred in each packet. The doubling of packets imposes a limitation on the total number of ports that can run fax pass-through at one time. You can calculate that two voice sessions with no VAD equate to one fax pass-through session with redundancy.

Call Control for Fax Passthrough

Fax pass-through is supported under the following call-control protocols:

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

In addition, the following information applies to H.323 and SIP fax pass-through.

Fax Pass-Through Signaling Using the Protocol Stack or NSEs

When a fax tone is detected, the originating and terminating gateways need to communicate to each other that they are changing to fax pass-through mode. Gateway signaling of the changeover to fax mode can use either of these methods:

- H.323 or SIP protocol stack (fax pass-through)
- Named signaling events (NSEs) (modem pass-through)

Beginning with Cisco IOS Release 12.2(13)T, you can specify the use of the H.323 or SIP protocol stack to signal the changeover to fax mode. This is enabled with the **fax protocol pass-through** command.

Alternately, you can use the **modem passthrough**command to configure the gateway to use Cisco-proprietary NSEs to signal the switch to pass-through mode. Fax pass-through using NSEs has been available on the Cisco AS5300 since Cisco IOS Release 12.1(3)T and on most other platforms since Cisco IOS Release 12.2(11)T.

Note Modem pass-through is preferred if all of the involved gateways are Cisco IOS gateways.

If non-Cisco gateways are involved in the fax transmissions, fax pass-through must be used. In all cases, however, T.38 fax relay is the best solution if all of the involved gateways support it.

H.323 or SIP Support of Resource Reservation Protocol

As of Cisco IOS Release 12.2(13)T, H.323 or SIP gateways that are configured for fax pass-through or modem pass-through allow Resource Reservation Protocol (RSVP) bandwidth adjustments when the original voice call is configured to use RSVP. When the original voice codec is restored at the end of the fax session, the original RSVP bandwidth is restored as well. When current bandwidth is unavailable, the fax proceeds at a best-effort rate without RSVP and with no performance guarantees. RSVP bandwidth adjustments for fax transmissions are made as follows:

- T.38 fax relay--RSVP bandwidth is adjusted to 80 kbps.
- Fax pass-through--RSVP bandwidth is adjusted to 96 kbps.

H.323 Support for Call Admission Control

As of Cisco IOS Release 12.2(13)T, H.323 call admission control (CAC) adjustments are allowed in the case of fax pass-through and modem pass-through. An H.323 gateway that uses a gatekeeper requests the following bandwidths from the gatekeeper when codec changes are necessary:

- T.38 fax relay--Bandwidth of 80 kbps
- Fax pass-through--Bandwidth of 96 kbps

If the gatekeeper accepts the bandwidth changes, the session is permitted to continue over the fax codec (G.711). If the gatekeeper rejects the bandwidth increase, the fax codec is terminated and the gateway uses the configured fax protocol fallback or the original voice codec, in which case the fax transfer fails.

How to Configure H.323 and SIP Fax Pass-Through

For H.323 and SIP networks, fax pass-through is configured on gateway dial peers.

The purpose of these tasks is to configure VoIP dial peers for fax or modem pass-through, one at a time or globally. If both methods are used, an individual dial-peer configuration takes precedence over the global configuration, which means that a call matching a particular dial peer tries first to apply the fax method that was configured individually on that dial peer. If no individual dial peer configuration was made, the router uses the global configuration.

When configuring dial peers, you have the choice of specifying fax pass-through or modem pass-through for the pass-through method. If you use the **fax protocol pass-through** command to specify fax pass-through as the method, the gateway uses the H.323 or SIP protocol stack to signal the changeover to fax mode. If you use the **modem passthrough**command to specify modem pass-through as the method, the gateway uses NSEs for fax changeover signaling.

Note If you need to configure fax pass-through to work with Cisco CallManager (CCM), you must use the **modem passthrough nse** command. The **fax protocol pass-through**command does not work with CCM, which relies on NSE information.

Configuring One or More Individual VoIP Dial Peers

Use this task to enable fax pass-through on individual dial peers. Select the **fax protocol pass-through** command or the **modem passthrough** command, but not both.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **voip**
4. Do one of the following:
   - **fax protocol pass-through** {**g711ulaw** | **g711alaw**} | **system**
   -
   -
   - **modem passthrough** {**system** | **nse** [**payload-type** *number*] **codec** {**g711alaw** | **g711ulaw**} [**redundancy**]}
5. **fax-rate disable**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 25 voip`	Enters dial-peer configuration mode and defines a dial peer that directs traffic to or from a packet network. • *tag* --Dial-peer identifier that consists of one or more digits. Valid entries are from 1 to 2147483647. • **voip** --Calls from this dial peer use voice encapsulation on the packet network.
Step 4	Do one of the following:	Specifies the type of fax protocol to use on this dial peer.

	Command or Action	Purpose

	• **fax protocol pass-through** {**g711ulaw** | **g711alaw**} | **system**
	•
	•
	• **modem passthrough** {**system** | **nse** [**payload-type** *number*] **codec** {**g711alaw** | **g711ulaw**} [**redundancy**]}
	Example:
	`Router(config-dial-peer)# fax protocol pass-through g711ulaw`
	Example:
	Example:
	Example:
	`Router(config-dial-peer)# modem passthrough nse codec g711alaw redundancy`
		• **pass-through** --Uses the H.323 or SIP protocol stack and the G.711 u-law or G.711 a-law codec. Use the same codec type for the originating and terminating gateways.
		• **system** --Uses the protocol set under the voice-service configuration mode.
		or
		Enables faxes to use modem pass-through and NSEs for fax changeover signaling.
		• **system** --Uses the protocol set under the voice-service configuration mode+.
		• **nse** --Named signaling event (NSE) signaling is used to communicate codec switchover.
		Note You must use **modem passthrough nse** with Cisco CallManager.
		• **payload-type** *number* --(Optional) Value for NSE payload type. Range varies by platform, but is from 96 to 119 on most platforms. The default is 100.
		• **codec** --Codec selection for upspeeding. Default: g711ulaw. Use the same codec type for the originating and terminating gateways.
		• **g711alaw**--G.711 a-law codec type for E1
		• **g711ulaw**--G.711 u-law codec type for T1
		• **redundancy** --(Optional) Enables a single repetition of packets (using RFC 2198) to protect against packet loss.

Step 5	**fax-rate disable** **Example:** `Router(config-dial-peer)# fax-rate disable`	(Optional) Disables fax protocol capability on this dial peer. **Note** Use this command only when you want to force faxes to use modem pass-through. Do not use this command when you want faxes to use fax pass-through or fax relay on this dial peer.

Configuring VoIP Dial Peers Globally

If you are adding fax pass-through capability previously defined VoIP dial peers, you can configure them globally in voice-service configuration mode.

Alternately, you can configure fax pass-through VoIP dial peers one at a time by following the instructions in the Configuring One or More Individual VoIP Dial Peers, on page 61.

Note When fax or modem pass-through is configured under the dial-peer voice configuration, the configuration for an individual dial peer takes precedence over the global configuration under the **voice service voip** command.

Note If you need to configure fax pass-through to work with Cisco CallManager (CCM), you must use the **modem passthrough nse** command. The **fax protocol pass-through** command does not work with CCM, which relies on NSE information.

When using the **voice service voip** and **modem passthrough nse**commands on a terminating gateway to globally set up fax pass-through with NSEs, you must ensure that each incoming call is associated with a VoIP dial peer to retrieve the global fax configuration. Associate calls with dial peers using the **incoming called-number** command to specify a sequence of digits that incoming calls can match. You can ensure that all calls match at least one dial peer by using the following commands:

```
Router(config)# dial-peer voice tag voip
Router(config-dial-peer)# incoming called-number .
```

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. Do one of the following:
   - **fax protocol pass-through** {**g711ulaw** | **g711alaw**}
   -
   -
   - **modem passthrough** {**nse** | **protocol**}[**payload-type** *number*] {**codec** {**g711alaw** | **g711ulaw**}} [**redundancy** [**maximum-sessions** *sessions*] [**sample-duration** [**10** | **20**]]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:**	Enters voice-service configuration mode.

	Command or Action	Purpose
	`Router(config)# voice service voip`	

Step 4	Do one of the following:
	• **fax protocol pass-through** {**g711ulaw** | **g711alaw**}
	•
	•
	• **modem passthrough** {**nse** | **protocol**}[**payload-type** *number*] {**codec** {**g711alaw** | **g711ulaw**}} [**redundancy** [**maximum-sessions** *sessions*] [**sample-duration** [**10** | **20**]]]
	Example:
	`Router(config-voi-serv)# fax protocol pass-through g711ulaw`
	Example:
	Example:
	Example:
	`Router(config-voi-serv)# modem passthrough nse codec g711alaw redundancy sample-duration 20`
		Specifies fax pass-through as the global transmission method for faxes, and the H.323 or SIP protocol stack to communicate codec switchover. Use the same codec for originating and terminating gateways.
		or
		Specifies modem pass-through as the global transmission method for fax and data.
		• **nse** --Named signaling event (NSE) signaling is used to communicate codec switchover.
		Note You must use **modem passthrough nse** with Cisco CallManager.
		• **protocol** --Session Initiation Protocol (SIP)/H.323 protocol is used to signal modem pass-through.
		• **payload-type** *number* --(Optional) Value for NSE payload type. Range varies by platform, but is from 96 to 119 on most platforms. The default is 100.
		• **codec** --Codec selection for upspeeding. Default: g711ulaw. Use the same codec type for the originating and terminating gateways.
		• **g711alaw**--G.711 a-law codec type for E1
		• **g711ulaw**--G.711 u-law codec type for T1
		• **redundancy** --(Optional) Enables a single repetition of packets (using RFC 2198) to protect against packet loss.
		• **maximum-sessions** *sessions* --(Optional) Maximum number of redundant sessions that can run simultaneously on each subsystem. Range varies by platform; see CLI help.
		• **sample-duration** --(Optional) Time length of the largest RTP packet when packet redundancy is active, in ms. Valid keywords are 10 and 20. The default is 10.

How to Configure MGCP Fax Pass-Through

Use the following steps to configure MGCP fax pass-through on voice gateways. You must have the same configuration on the originating and terminating gateways.

Before you begin

Identify endpoints and configure the MGCP application as described in the *MGCP and Related Protocols Configuration Guide.*

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mgcp package-capability rtp-package**
4. **mgcp modem passthrough voip mode nse**
5. **mgcp modem passthrough voip codec** {**g711ulaw** | **g711alaw**}
6. **mgcp modem passthrough voip redundancy** [**sample-duration** [**10** | **20**]] [**maximum-sessions** *sessions*]
7. **mgcp timer nse-response t38** *timer*
8. **mgcp fax t38 inhibit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**mgcp package-capability rtp-package** **Example:** `Router(config)# mgcp package-capability rtp-package`	Specifies an MGCP package capability type for a media gateway. • **rtp-package** --Specifies events and signals for the Real-Time Transport Protocol (RTP) stream.
Step 4	**mgcp modem passthrough voip mode nse** **Example:** `Router(config)# mgcp modem passthrough voip mode nse`	Enables named signaling event (NSE) based modem relay mode for VoIP calls on an MGCP gateway. • **nse** --(Optional) Instructs the gateway to use NSE mode for upspeeding.
Step 5	**mgcp modem passthrough voip codec** {**g711ulaw** | **g711alaw**} **Example:** `Router(config)# mgcp modem passthrough voip codec g711alaw`	Selects the codec that enables the gateway to send and receive modem and fax data in VoIP configurations. • **g711ulaw** --G.711 u-law codec for changing speeds during modem and fax switchover. • **g711alaw** --G.711 a-law codec for changing speeds during modem and fax switchover. This is the default.

	Command or Action	Purpose
		Note Use the same codec type for originating and the terminating gateways.
Step 6	**mgcp modem passthrough voip redundancy** [**sample-duration** [**10** | **20**]] [**maximum-sessions** *sessions*] **Example:** `Router(config)# mgcp modem passthrough voip redundancy sample-duration 20`	(Optional) Enables redundancy on a gateway that sends and receives modem and fax data in VoIP configurations. When redundancy is enabled, all calls on the gateway are affected. • **sample-duration** --(Optional) Time length of the largest RTP packet when packet redundancy is active, in ms. Valid keywords are 10 and 20. The default is 10. • **maximum sessions** *sessions* --(Optional) Maximum number of redundant sessions that can run simultaneously on each subsystem. The range varies by platform; see CLI help.
Step 7	**mgcp timer nse-response t38** *timer* **Example:** `Router(config)# mgcp timer nse-response t38 250`	(Optional) Configures how a gateway detects the RTP stream host. • **nse-response t38** *timer* --The timeout period, in milliseconds, for awaiting T.38 named signaling event (NSE) responses from a peer gateway. Range is from 100 to 3000. The default is 200.
Step 8	**mgcp fax t38 inhibit** **Example:** `Router(config)# mgcp fax t38 inhibit`	(Optional) Configures MGCP fax T.38 parameters. • **inhibit** --Disables use of T.38 for the gateway. By default, T.38 is enabled. **Note** If the MGCP gateway uses the auto-configuration function, the **mgcp fax t38 inhibit**command is automatically configured on the gateway each time a new configuration is downloaded. Beginning with Cisco IOS Software Release 12.4T, the auto-configuration of this command is removed. For MGCP gateways running Cisco IOS version 12.4T or later, you must manually configure the **mgcp fax t38 inhibit**command to use T.38 fax relay.

Configuration Examples for Fax Pass-Through

H.323 Fax Pass-Through Example

The following example show a configuration for fax pass-through with H.323 support.

```
version 12.2
service timestamps debug uptime
```

```
service timestamps log uptime
no service password-encryption
!
hostname 5850
!
no logging buffered
no logging rate-limit
!
resource-pool disable
dial-tdm-clock priority 1 trunk-slot 1 port 0
spe link-info poll voice 5
spe default-firmware spe-firmware-1
ip subnet-zero
ip cef distributed
ip ftp username mgcusr
ip ftp password lab
no ip domain lookup
ip host colos_tftp 10.100.00.00
ip host brios 255.255.255.255
ip dhcp smart-relay
!
isdn switch-type primary-net5
!
voice service voip
 h323
 modem passthrough nse codec g711alaw redundancy sample-duration 20
!
no voice hpi capture buffer
no voice hpi capture destination
!
mrcp client session history duration 0
mrcp client session history records 0
memory check-interval 3600
memory validate-checksum 7200
redundancy
 no keepalive-enable
 mode classic-split
!
controller E1 0/0
 pri-group timeslots 1-31
!
dial-peer voice 5001 pots
 incoming called-number 550
 destination-pattern 800
 direct-inward-dial
 port 0/0:D
 prefix 800
!
dial-peer voice 500 voip
 incoming called-number 800
 destination-pattern 550
 session target ipv4:10.100.00.00
 fax rate disable
 codec g726r32
!
gateway
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
 exec-timeout 0 0
 logging synchronous
line vty 0 4
```

```
 password lab
 no login
line 2/00 5/323
 flush-at-activation
 no modem status-poll
 no modem log rs232
```

SIP Fax Pass-Through Example

The following configuration example shows fax pass-through with SIP support.

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 2691
!
boot-start-marker
boot system flash:c2691-ipvoice-mz.andante_0224
boot-end-marker
!
logging buffered 100000 debugging
enable password lab
!
no aaa new-model
!
resource manager
!
memory-size iomem 25
clock timezone PST -8
clock summer-time PDT recurring
no network-clock-participate slot 1
voice-card 1
 codec complexity high
 dspfarm
!
ip subnet-zero
ip cef
!
no ip dhcp use vrf connected
!
no ip domain lookup
no ftp-server write-enable
isdn switch-type primary-qsig
!
voice service voip
 fax protocol pass-through g711ulaw
 sip
!
controller T1 1/0
 framing sf
 linecode ami
!
controller T1 1/1
 framing sf
 linecode ami
!
interface FastEthernet0/0
 ip address 10.20.109.104 255.255.0.0
 duplex auto
 speed auto
!
```

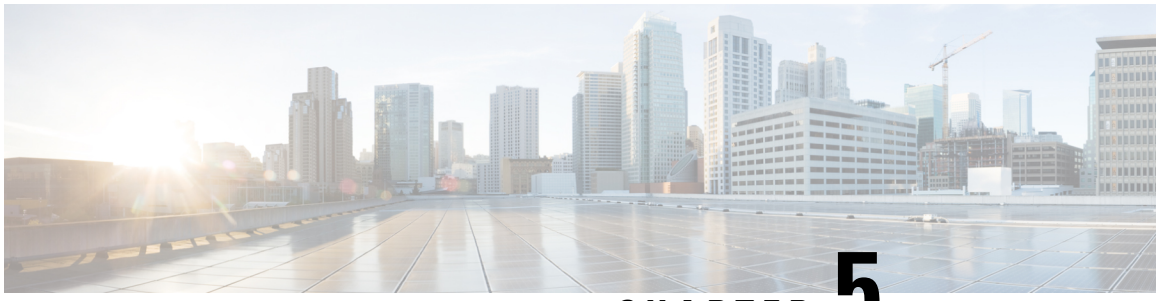
```
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
ip default-gateway 10.20.0.1
ip classless
ip route 0.0.0.0 0.0.0.0 10.20.0.1
!
no ip http server
!
control-plane
!
dial-peer voice 2000 voip
 fax rate disable
 fax protocol pass-through g711alaw
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 1
 exec-timeout 0 0
 password lab
 login
line vty 2 4
 login
!
ntp clock-period 17180778
ntp server 10.10.254.253 prefer
!
end
```

MGCP Fax Pass-Through Example

The following example shows an MGCP gateway configured for fax pass-through.

```
version 12.2
no parser cache
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname fptrtr
!
voice-card 1
!
ip subnet-zero
!
no ip domain lookup
!
isdn switch-type primary-5ess
!
voice call carrier capacity active
!
mta receive maximum-recipients 0
!
ccm-manager mgcp
no ccm-manager fax protocol cisco
!
controller T1 1/0
framing esf
clock source line primary
```

```
linecode b8zs
ds0-group 0 timeslots 1 type fxs-loop-start
!
controller T1 1/1
framing esf
linecode b8zs
ds0-group 0 timeslots 1 type e&m-wink-start
!
interface Ethernet0/0
ip address 10.3.222.6 255.255.0.0
ip helper-address 10.3.222.1
no ip mroute-cache
half-duplex
!
interface Ethernet0/1
shutdown
!
ip default-gateway 10.3.0.1
ip classless
ip route 192.168.254.0 255.255.255.0 10.3.0.1
ip http server
!
call rsvp-sync
!
voice-port 1/0:0
!
voice-port 1/1:0
!
voice-port 3/0/0
!
voice-port 3/0/1
!
mgcp
mgcp call-agent 10.3.222.1 service-type mgcp version 0.1
mgcp modem passthrough voip mode nse
mgcp package-capability rtp-package
mgcp fax t38 inhibit
!
mgcp profile default
!
dial-peer cor custom
!
dial-peer voice 3641 pots
application mgcpapp
port 3/0/0
!
dial-peer voice 3643 pots
application mgcpapp
port 1/1:0
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
exec-timeout 0 0
password cisco
login
!
!
end
```



CHAPTER 5

Configuring Cisco Fax Relay

Configuring Cisco Fax Relay

This chapter describes configuration for Cisco fax relay on an IP network. With Cisco fax relay, gateways terminate T.30 fax signaling by spoofing a virtual fax machine to the locally attached fax machine. The gateways use a Cisco-proprietary fax-relay RTP-based protocol to communicate between them.

History for the Cisco Fax Relay Feature

Release	Modification
12.2(11)T	This feature was introduced.
12.4(4)T	The **fax-relay sg3-to-g3** command was integrated into Cisco IOS release 12.4(4)T

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn . You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring Cisco Fax Relay

Before you configure Cisco fax relay, perform the following steps:

- Install a software release that supports Cisco fax relay.
- Establish a working H.323 or SIP network for voice calls.
- Complete voice interoperability testing with third-party gateways and gatekeepers.

Restrictions for Configuring Cisco Fax Relay

Restrictions for implementing Cisco fax relay are as follows.

- Some platforms, such as the Cisco AS5350, Cisco AS5800, and Cisco AS5850, do not support Cisco-proprietary fax relay.
- Third-party vendors must adhere to V.8 and T.30 specifications.
- Third-party vendors might experience a 2.5- to 4-second delay before the fax transmission begins. This is the ANSam timeout value specified in the T.30 specification.
- SG3 V.8 fax CM message suppression supports only the TI C5421, TI C549, and TI C5510 digital signal processors (DSPs).
- SG3 V.8 fax CM message suppression is enabled by default for Cisco fax relay.
- If you use modem pass-through to send SG3 faxes and you use Cisco fax relay to send G3 faxes, you must configure both modem pass-through and fax relay.
- When a two-gateway solution is used, both gateways must be configured to use SG3 V.8 fax CM message suppression.
- When a one-gateway solution is used, other gateways can be Cisco gateways that do not support SG3 V.8 fax CM message suppression or third-party gateways that are not SG3-capable if the fax CM message suppression gateway is the originating gateway.
- SG3 fax machines will scale down to G3 speeds if the SG3 V.8 fax CM message is suppressed or if the signals are not delivered reliably by low bit rate codecs.

Information About Cisco Fax Relay

Methods for Fax Relay

Cisco provides two methods for fax relay. One method is a Cisco-proprietary method called Cisco fax relay, and it is described in this chapter. The second method is based on the ITU-T T.38 standard, and it is described in the chapter “Configuring T.38 Fax Relay.”

- T.38 fax relay is the default mode for passing faxes through a VoIP network, and Cisco fax relay is the default fax relay type on Cisco voice gateways. This capability has been supported in Cisco IOS Release 11.3 and later releases and is widely available. Cisco fax relay uses Real-Time Transport Protocol (RTP) to transport the fax data.
- Cisco fax relay is configured on the VoIP dial peers that direct calls into and out of the packet network. Cisco fax relay can be configured under the H.323 and Session Initiation Protocol (SIP) call control protocols.

Fax Relay Packet Loss Concealment

Cisco fax relay supports fax relay packet loss concealment, which is a technique that allows gateways to disregard packet loss rates that might otherwise cause fax failures. High-end fax machines with the memory to store page data often are able to use Error Correction Mode (ECM) for error-free page transmission. When ECM is enabled, a fax page is transmitted in a series of blocks that contain frames with packets of data. After receiving the data for a complete page, a receiving fax machine notifies the transmitting fax machine of any frames with errors. The transmitting fax machine then retransmits the specified frames. This process is repeated until all frames are received without errors. If the receiving fax machine is unable to receive an error-free page, the fax transmission may fail and one of the fax machines may disconnect. On networks that have a packet loss rate greater than 2 per cent, fax transmissions routinely fail when ECM is enabled because of ECM's low tolerance for packet loss.

The Fax Relay Packet Loss Concealment feature allows you to control whether ECM is enabled or disabled for fax transmissions on a VoIP dial peer. By disabling ECM on networks with a large amount of packet loss, you ensure that more fax transmissions are completed, although they may not be totally error-free.

When ECM is disabled, a fax page is transmitted using high-speed modulation in its raw encoded format. When detecting line errors with ECM disabled, the receiving fax machine has three options (in order of increasing severity):

- Respond to page reception with the ReTrain Positive command. This response causes the transmitting fax to go through the training check process before transmitting the next page.
- Respond to the page reception with the ReTrain Negative command. This response causes the transmitting fax to go through the Training Check Frame (TCF) process with a lower modulation scheme.
- Disconnect immediately.

Fax relay ECM is enabled by default. To disable ECM, you use the **fax-relay ecm disable** command on the VoIP dial peer. After this command is configured, the gateway's Digital Signal Processor (DSP) fax-relay firmware modifies the T.30 Digital Information Signal (DIS) message. This modification is performed on DIS signals in both directions, so that ECM is disabled even when only one gateway is configured to disable ECM.

Disabling of ECM is recommended for dial peers handling fax relay traffic on known lossy networks, especially those with a packet loss rate of 2 percent or greater. The **debug fax relay t30** command provides information about the E.164 destination and T.30 messages associated with fax transmissions. Note than an excessive number of simultaneous debug operations can degrade performance.

Fax CM Message Tone Suppression

Super Group 3 (SG3) is a new generation of fax machines that support speeds of up to 33.6 kbps through V.34 half duplex (HD) modulation and V.8 signaling.

SG3 V.8 fax CM message tone suppression enables SG3 fax machines to scale down without end-user interaction and without using the extra bandwidth required by modem pass-through and allows SG3 fax machines to interoperate over a fax-relay network at G3 speeds by blocking the SG3 V.8 CM message, or fax tone, from reaching the called fax machine. This causes the called fax machine to time out on the ANSam tone and scale down to G3 speeds by initiating V.21 negotiations.

SG3 V.8 fax CM message tone suppression supports both the one-gateway and two-gateway solutions:

- With a one-gateway solution, the gateway on one end of the call can be configured to suppress the SG3 V.8 fax CM message independently of the gateway on the other end of the call. The one-gateway solution suppresses the fax CM tone on both TDM and IP interfaces (TI C5510 DSPs only), and can interoperate

with third-party gateways when the fax CM tone suppression gateway is the originating gateway. A one-gateway solution

- With a two-gateway solution, the gateways on both ends of the call must have this feature enabled. The two-gateway solution suppresses the fax CM tone only on the TDM interface (TI C5421 and TI C549 DSPs). Both gateways must support this feature to interoperate at G3 speeds, or the fax tone suppression gateway must be the originating gateway.

Note If both the originating gateway and the terminating gateways are configured for V.8 fax CM message suppression, the suppression occurs on the originating gateway.

How to Configure Cisco Fax Relay

Cisco fax relay can be configured globally for all VoIP dial peers or for individual dial peers. This section contains the following tasks:

Note Fax relay parameters that are set for an individual dial peer under the **dial-peer voice** command take precedence over global settings made under the **voice service voip** command.

Configuring Cisco Fax Relay for One or More Individual VoIP Dial Peers

Use the following steps to configure Cisco fax relay for individual dial peers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **voip**
4. **fax protocol** {**cisco** | **none**| **system**}
5. **fax rate** {**12000** | **14400** | **2400** | **4800** | **7200**| **9600** | **disable** | **voice**} [**bytes** *rate*]
6. **fax-relay ecm disable**
7. **fax nsf** *word*
8. **fax-relay sg3-to-g3** *system*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Router# configure terminal`	
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 25 voip`	Enters dial-peer configuration mode and defines a dial peer that directs traffic to or from a packet network. • *tag* --Dial-peer identifier that consists of one or more digits. Valid entries are from 1 to 2147483647. • **voip** --Calls from this dial peer use voice encapsulation on the packet network.
Step 4	**fax protocol** {**cisco** | **none**| **system**} **Example:** `Router(config-dial-peer)# fax protocol cisco`	Specifies the fax protocol for this dial peer. • **cisco** -- Cisco-proprietary fax protocol. This is the default. • **none** --No fax protocol. • **system** --Use global configuration for this dial peer.
Step 5	**fax rate** {**12000** | **14400** | **2400** | **4800** | **7200**| **9600** | **disable** | **voice**} [**bytes** *rate*] **Example:** `Router(config-dial-peer)# fax rate 14400`	(Optional) Selects the fax transmission speed to be attempted when this dial peer is used. • **12000** , **14400**, **2400**, **4800**, **7200**, **9600**--Maximum bits-per-second speed. • **disable** --Disables fax relay transmission capability. • **voice** --Highest possible transmission speed allowed by the voice rate. For example, if the voice codec is G.711, fax transmission occurs at up to 14400 bps because 14400 bps is less than the 64-kbps voice rate. If the voice codec is G.729 (8 kbps), the fax transmission speed is 7200 bps. This is the default. • **bytes** *rate* --(Optional) Fax packetization rate, in ms. Range is 20 to 48. The default is 20.
Step 6	**fax-relay ecm disable** **Example:** `Router(config-dial-peer)# fax-relay ecm disable`	(Optional) Disables fax-relay ECM. **Note** To enable ECM, use the **no** form of this command.
Step 7	**fax nsf** *word* **Example:** `Router(config-dial-peer)# fax nsf 000000`	(Optional) Allows the router to override the settings made by fax machines that try to implement proprietary encodings (non-standard facilities, or NSF). By default, the NSF code is not overridden. • *word* --Two-digit hexadecimal country code and a four-digit hexadecimal manufacturer code.

	Command or Action	Purpose
		Note Setting this command to all zeroes prevents transfer of NSF during fax negotiation and overwrites the NSF so that only standard fax transactions occur. Because a router demodulates and decodes fax tones based on the T.30 specification, transactions or encoding that are proprietary can cause fax relay transmissions to fail.
Step 8	**fax-relay sg3-to-g3** *system* **Example:** `Router(config-dial-peer)# fax-relay sg3-to-g3 system`	Specifies that for SIP and H.323 signaling types, V.8 fax CM message suppression is enabled on the specific dial peer. Enabled by default. • *system* --Uses the protocol set under the voice-service configuration.

Configuring Cisco Fax Relay for VoIP Dial Peers Globally

Use the following steps to configure Cisco fax relay globally for VoIP dial peers.

Note Fax relay parameters that are set for an individual dial peer under the **dial-peer voice** command take precedence over global settings made under the **voice service voip** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **fax protocol** {**cisco** | **none**}
5. **fax-relay sg3-to-g3**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**voice service voip** **Example:** `Router(config)# voice service voip`	Enters voice-service configuration mode.
Step 4	**fax protocol** {**cisco** | **none**} **Example:** `Router(config-voi-serv)# fax protocol cisco`	Specifies the fax protocol for all dial peers. • **cisco** --Cisco-proprietary fax protocol. • **none** --Disables fax relay and fax pass-through.
Step 5	**fax-relay sg3-to-g3** **Example:** `Router(config-voi-serv)# fax-relay sg3-to-g3`	(Optional) Specifies that for SIP and H.323 signaling types, V.8 fax CM message suppression is enabled for all dial peers on the digital signal processor (DSP) firmware. Enabled by default.

Configuration Examples for Cisco Fax Relay

MGCP VoIP Dial Peer Example

SG3 V.8 fax CM message suppression is enabled by default and does not appear in the running configuration. To view the configuration for:

- H.323 and SIP--Use the **show dial-peer voice** *tag* command.
- MGCP--Use the **show mgcp** command.

```
Router# show dial-peer voice 2000
VoiceOverIpPeer2000
        peer type = voice, information type = voice,
        description = `',
        tag = 2000, destination-pattern = `',
        answer-address = `', preference=0,
        CLID Restriction = None
        CLID Network Number = `'
        CLID Second Number sent
        CLID Override RDNIS = disabled,
        source carrier-id = `', target carrier-id = `',
        source trunk-group-label = `',  target trunk-group-label = `',
        numbering Type = `unknown'
        group = 2000, Admin state is up, Operation state is up,
        incoming called-number = `2...', connections/maximum = 0/unlimited,
        DTMF Relay = disabled,
        modem transport = relay, nse, payload type = 100, codec = g711alaw, , ga
  teway-controlled,
        URI classes:
            Incoming (Called) =
            Incoming (Calling) =
            Destination =
        huntstop = disabled,
        in bound application associated: 'DEFAULT'
        out bound application associated: ''
        dnis-map =
```

```
permission :both
incoming COR list:maximum capability
outgoing COR list:minimum requirement
Translation profile (Incoming):
Translation profile (Outgoing):
incoming call blocking:
translation-profile = `'
disconnect-cause = `no-service'
advertise 0x40 capacity_update_timer 25 addrFamily 4 oldAddrFamily 4
type = voip, session-target = `ipv4:10.2.109.103',
technology prefix:
settle-call = disabled
ip media DSCP = ef, ip signaling DSCP = af31,
ip video rsvp-none DSCP = af41,ip video rsvp-pass DSCP = af41
ip video rsvp-fail DSCP = af41,
UDP checksum = disabled,
session-protocol = cisco, session-transport = system,
req-qos = best-effort, acc-qos = best-effort,
req-qos video = best-effort, acc-qos video = best-effort,
req-qos audio def bandwidth = 64, req-qos audio max bandwidth = 0,
req-qos video def bandwidth = 384, req-qos video max bandwidth = 0,
RTP dynamic payload type values: NTE = 101
Cisco: NSE=100, fax=96, fax-ack=97, dtmf=121, fax-relay=122
       CAS=123, ClearChan=125, PCM switch over u-law=0,A-law=8
RTP comfort noise payload type = 19
fax rate = fax,   payload size =  20 bytes
fax protocol = system
fax-relay ecm enable
Fax Relay SG3-to-G3 Enabled (by system configuration)
fax NSF = 0xAD0051 (default)
codec = g729r8,   payload size =  20 bytes,
Media Setting = flow-through (global)
Expect factor = 10, Icpif = 20,
Playout Mode is set to adaptive,
Initial 60 ms, Max 250 ms
Playout-delay Minimum mode is set to default, value 40 ms
Fax nominal 300 ms
Max Redirects = 1, signaling-type = cas,
VAD = enabled, Poor QOV Trap = disabled,
Source Interface = NONE
voice class sip url = system,
voice class sip rel1xx = system,
redirect ip2ip = disabled
probe disabled,
voice class perm tag = `'
Time elapsed since last clearing of voice call statistics never
Connect Time = 0, Charged Units = 0,
Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
Accepted Calls = 0, Refused Calls = 0,
Last Disconnect Cause is "",
Last Disconnect Text is "",
Last Setup Time = 0.
```

Configuration Disabled for MGCP Example

When SG3 V.8 fax CM message suppression is not enabled, the running configuration shows**no mgcp fax-relay sg3-to-g3**, as shown in mgcp section of the following example:

```
Router# show runnning config
Building configuration...
Current configuration : 3231 bytes
!
! No configuration change since last restart
```

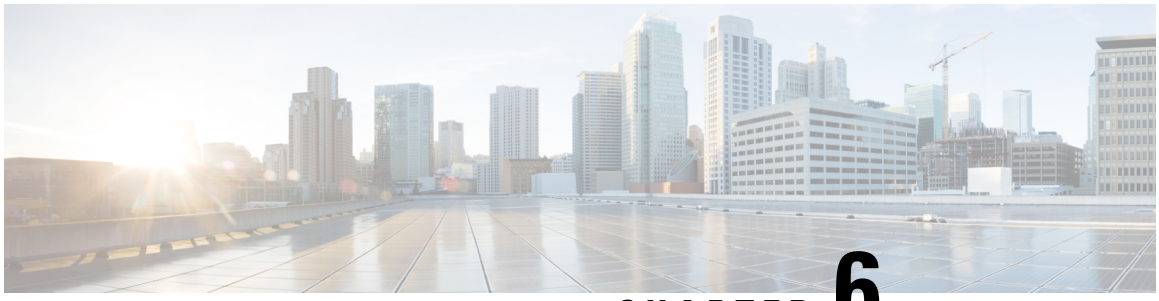
```
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
mgcp
mgcp call-agent ccm service-type mgcp version 0.1
mgcp dtmf-relay voip codec all mode out-of-band
mgcp rtp unreachable timeout 1000 action notify
mgcp modem relay voip mode nse gw-controlled
mgcp package-capability rtp-package
no mgcp package-capability res-package
mgcp package-capability sst-package
no mgcp package-capability fxr-package
mgcp package-capability pre-package
no mgcp timer receive-rtcp
mgcp sdp simple
mgcp fax t38 inhibit
no mgcp fax-relay sg3-to-g3
mgcp rtp payload-type g726r16 static
!
mgcp profile default
```

Show Fax Portion of Telephony Call Leg Example

The **show call active fax**command lists information about the fax part of the telephony call leg. Use this command to verify the SG3 fax CM suppression type, as shown in the following example:

```
Router# show call active fax
Telephony call-legs: 1
SIP call-legs: 0
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 1
 GENERIC:
SetupTime=2635990 ms
Index=1
PeerAddress=7001
PeerSubAddress=
PeerId=7000
PeerIfIndex=19
LogicalIfIndex=5
ConnectTime=2649400 ms
CallDuration=00:00:08 sec
CallState=4
CallOrigin=2
ChargedUnits=0
InfoType=fax
TransmitPackets=506
TransmitBytes=13616
ReceivePackets=134
ReceiveBytes=2388
TELE:
ConnectionId=[0x33333333 0x77777777 0xFFFFFFFF 0xDDDDDDDD
IncomingConnectionId=[0x66666666 0xBBBBBBBB 0x88888888 0xEEEEEEEE
CallID=5
TxDuration=14800 ms
VoiceTxDuration=4150 ms
```

```
FaxTxDuration=0 ms
FaxRate=7200 bps
SG3 Fax CM Suppression Type=TDM
NoiseLevel=-69
ACOMLevel=6
OutSignalLevel=-79
InSignalLevel=-73
InfoActivity=1
ERLLevel=6
EchoCancellerMaxReflector=4
SessionTarget=
ImgPages=0
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=
OriginalCallingOctet=0x0
OriginalCalledNumber=
OriginalCalledOctet=0x80
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0x0
TranslatedCallingNumber=7001
TranslatedCallingOctet=0x0
TranslatedCalledNumber=
TranslatedCalledOctet=0x80
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0x0
GwCollectedCalledNumber=9102
DSPIdentifier=3/1:1
Telephony call-legs: 1
SIP call-legs: 0
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 1
```



CHAPTER 6

Configuring T.38 Fax Relay

Configuring T.38 Fax Relay

This chapter describes configuration for T.38 fax relay on an IP network. T.38 is an ITU standard that defines how fax communications are packetized and transported over IP networks. T.38 fax relay includes the following features:

- Fax Relay Packet Loss Concealment
- MGCP Based Fax (T.38) and DTMF Relay
- SIP T.38 Fax Relay
- T.38 Fax Relay for T.37/T.38 Fax Gateway
- T.38 Fax Relay for VoIP H.323
- SG3 Fax Support on Cisco Time Division Multiplexing-Internet Protocol (TDM-IP) Voice Gateways and Cisco Unified Border Element (Cisco UBE) platforms

History for the Fax Relay Packet Loss Concealment Feature

Release	Modification
12.1(3)T	This feature was introduced.
12.1(5)XM	This feature was implemented on the Cisco AS5800.
12.1(5)XM2	This feature was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This feature was implemented on the Cisco AS5850.
12.2(11)T	This feature was integrated into this release and implemented on the Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.

History for the MGCP Based Fax (T.38) and DTMF Relay Feature

Release	Modification
12.2(2)XB	This feature was introduced.
12.2(8)T	This feature was integrated into this release and implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series.
12.2(11)T	This feature was implemented on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5800.
12.2(11)T2	The **gateway force** keyword pair was introduced.
12.2(15)T	This feature was implemented on the Cisco 1751 and Cisco 1760.
12.4T	The **mgcp fax t38 inhibit** command was no longer configured by default for MGCP gateways that use the auto-configuration function.
12.4(4)T	The **mgcp fax-relay sg3-to-g3** command was integrated into Cisco IOS release 12.4(4)T

History for the H.323 and SIP T.38 Fax Relay Feature

Release	Modification
12.2(13)T	This feature was introduced.
12.4(4)T	The **fax-relay sg3-to-g3** command was integrated into Cisco IOS release 12.4(4)T

History for the T.38 Fax Relay for T.37/T.38 Fax Gateway Feature

Release	Modification
12.1(3)X1	This feature was introduced.

History for the SG3 Fax Support Cisco TDM-IP Voice Gateways and Cisco UBE Platforms Feature

Release	Modification
15.1(1)T	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Your software release may not support all the features documented in this chapter. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn . An account on Cisco.com is not required.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring T.38 Fax Relay

Before you configure T.38 fax relay, perform the following tasks:

H.323 and SIP T.38 Fax Relay

- Ensure that your platform is supported.
- Install a software release that supports fax relay.
- Install appropriate hardware and memory for your platform.
- Establish a working H.323 or SIP network for voice calls. T.38 fax relay interoperability requires H.323 Version 2.
- Complete voice interoperability testing with third-party gateways and gatekeepers.
- To disable fax relay ECM on the AS5xxx series of voice gateways using Nextport DSP models, ensure that you have system processing engine (SPE) firmware version 2.8.3.8 or a higher version.

MGCP T.38 Fax Relay

- Install a software release that supports T.38 fax relay
- Install appropriate hardware and memory for your platform.
- Identify endpoints and configure the MGCP application as described in the appropriate section of the*Cisco IOS MGCP and Related Protocols Configuration Guide* .
- Complete voice interoperability testing with third-party gateways and gatekeepers.
- Ensure that you have adequate memory in the gateway. Although 96 to 128 MB of RAM is recommended, the memory requirement is dependent on the platform and the anticipated number of calls to be made through the system.

SG3 Fax Support on Cisco TDM-IP Voice Gateways and Cisco UBE platforms

- Working familiarity with Cisco IOS command-line interface and basic configuration procedures for voice gateway networks.
- You should be familiar with the configuration information in the Universal Voice Transcoding Support for IP-to-IP Gateways document.

Restrictions for Configuring T.38 Fax Relay

The restrictions for configuring T.38 fax relay are as follows:

H.323 T.38 Fax Relay

- The transport protocols specified in the ITU-T recommendation for T.38 are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). However, for T.38 fax relay on Cisco gateways, only UDP is supported for the transport layer.
- Some third-party gateways and gatekeepers may not be compatible with Cisco voice gateways for T.38 fax relay because different manufacturers can select certain parts of H.323 and T.38 to implement into their gateways and gatekeepers. Voice interoperability testing with these third-party gateways and gatekeepers should be performed to make sure that T.38 fax relay can be successful.
- T.38 fax relay is not supported on Cisco MC3810 series concentrators with Voice Compression Modules (VCMs).
- T.38 fax relay is not supported by Multimedia Conference Manager (MCM) H.323 proxy in Cisco IOS Release 12.1(3)T.
- If the **fax rate disable** command is configured on a dial peer, neither the originating nor the terminating gateway can enter into Cisco fax relay mode, T.38 fax relay mode, or fax pass-through mode. The **fax rate disable** command disables fax transfer support.

SIP T.38 Fax Relay

- The transport protocols specified in the ITU-T recommendation for T.38 are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). However, for T.38 fax relay on Cisco gateways, only UDP is supported for the transport layer.
- If SIP T.38 fax relay is not supported by both gateways, the T.38 negotiation fails and the call reverts to an audio codec.
- T.38 fax relay requires a 64-kbps transmission rate, the same amount of bandwidth as a voice call with the G.711 codec.
- Fax Calling Tones (CNG) are optional and are not used to initiate a switch to T.38 mode. Instead, Called Station Identifier (CED) tones or preamble flags are used.
- SIP fax relay does not rely on named signaling events (NSEs) to signal a switch to T.38 mode. Standard RFC 2543 and RFC 2327 SIP and SDP signaling are used instead.
- If the **fax rate disable** command is configured on a dial peer, neither the originating nor the terminating gateway can enter into Cisco fax relay mode, T.38 fax relay mode, or fax pass-through mode. The **fax rate disable** command disables fax transfer support.

SG3 Fax Support on Cisco TDM-IP Voice Gateways and Cisco UBE Platforms

- SG3 fax capability is not supported for Cisco Fax Relay.
- For T.38 fax sessions to operate at SG3 speeds, all the endpoints involved must support T.38 Version 3 (v3) configuration and have negotiated T.38 v3. If all endpoints are not configured for SG3/V.34 speeds, then the slowest speed in the topology is the one supported by all endpoints.

- SG3 fax support on TDM-IP gateways is available in H.323 and SIP configurations.

MGCP T.38 Fax Relay

- Only UDP is supported for the transport layer.
- The gateway does not dynamically issue a call admission control (CAC) request to increase the bandwidth allocated for a call when the call is switched from voice to fax. A best-effort support of bandwidth requirements for the call is supported.

Information About T.38 Fax Relay

Methods for Fax Relay

Cisco provides two methods for fax relay; Cisco fax relay and T.38 fax relay.

- Cisco fax relay, a Cisco-proprietary method, is the default on most platforms if a fax method is not explicitly configured.
- T.38 fax relay is a method based on the ITU-T T.38 standard.T.38 fax relay is real-time fax transmission; that is, two fax machines communicating with each other as if there were a direct phone line between them. Fax relay is configured by using a few additional commands on gateway dial peers that have already been defined and configured for voice over IP calls.

T.38 fax relay is described in this chapter. Cisco fax relay is described in the "Configuring Cisco Fax Relay" chapter.

T.38 Fax Relay Functions

T.38 fax gateways provide the following functions:

- Demodulation of incoming T.30 fax signals at the transmitting gateway (T.30 is the standard procedure for fax transmission in the PSTN.)
- Translation of T.30 fax signals into T.38 Internet Fax Protocol (IFP) packets
- Exchange of IFP packets between the transmitting and receiving T.38 gateways
- Translation of T.38 IFP packets back into T.30 signals at the receiving gateway

T.38 Fax Relay Call Control

The T.38 fax relay feature can be configured for H.323, Session Initiation Protocol (SIP), Media Gateway Control Protocol (MGCP), and Skinny Client Control Protocol (SCCP) call control protocols. For H.323 and SIP networks, the only configuration tasks that differ are configuration of VoIP dial peers.

H.323 and SIP T.38 Fax Relay

This section describes the capabilities available with H.323 and SIP T.38 fax relay.

Fax Relay Packet Loss Concealment

High-end fax machines with the memory to store page data often are able to use Error Correction Mode (ECM) for error-free page transmission. When ECM is enabled, a fax page is transmitted in a series of blocks that contain frames with packets of data. After receiving the data for a complete page, a receiving fax machine notifies the transmitting fax machine of any frames with errors. The transmitting fax machine then retransmits the specified frames. This process is repeated until all frames are received without errors. If the receiving fax machine is unable to receive an error-free page, the fax transmission may fail and one of the fax machines may disconnect. On networks that have a packet loss rate greater than 2 per cent, fax transmissions routinely fail when ECM is enabled because of ECM's low tolerance for packet loss.

The fax relay packet loss concealment feature allows you to control whether ECM is enabled or disabled for fax transmissions on a VoIP dial peer. By disabling ECM on networks with a large amount of packet loss, you ensure that more fax transmissions are completed, although they may not be totally error-free.

When ECM is disabled, a fax page is transmitted using high-speed modulation in its raw encoded format. When detecting line errors with ECM disabled, the receiving fax machine has three options (in order of increasing severity):

- Respond to page reception with the ReTrain Positive command. This response causes the transmitting fax to go through the training check process before transmitting the next page.
- Respond to the page reception with the ReTrain Negative command. This response causes the transmitting fax to go through the Training Check Frame (TCF) process with a lower modulation scheme.
- Disconnect immediately.

Fax relay ECM is enabled by default. To disable ECM, you use the **fax-relay ecm disable** command on the VoIP dial peer. After this command is configured, the gateway's Digital Signal Processor (DSP) fax-relay firmware modifies the T.30 Digital Information Signal (DIS) message. This modification is performed on DIS signals in both directions, so that ECM is disabled even when only one gateway is configured to disable ECM.

Disabling of ECM is recommended for dial peers handling fax relay traffic on known lossy networks, especially those with a packet loss rate of 2 percent or greater. The **debug fax relay t30** command provides information about the E.164 destination and T.30 messages associated with fax transmissions. Note than an excessive number of simultaneous debug operations can degrade performance.

H.323 or SIP T.38 Fax Relay Fallback

You can specify a fallback fax method for the gateway to attempt if H.323 or SIP T.38 fax relay cannot be successfully initiated between gateways. A failure to switch to T.38 fax relay can occur if you are interworking with a network that does not support T.38 fax relay. The following are the fallback options:

- Cisco fax relay.
- Fax pass-through using a G.711 codec.
- No fallback. The fax is transmitted using the existing voice codec. If modem pass-through has been configured, the fax is transferred through named signaling event (NSE) pass-through.

H.323 or SIP Support of Resource Reservation Protocol for T.38 Fax Relay

H.323 or SIP gateways that are configured for T.38 fax relay allow Resource Reservation Protocol (RSVP) bandwidth adjustments when the original voice call is configured to use RSVP. When the original voice codec is restored at the end of the fax session, the original RSVP bandwidth is restored as well. When current

bandwidth is unavailable, the fax proceeds at a best-effort rate without RSVP and with no performance guarantees. RSVP bandwidth adjustments for fax transmissions are made as follows:

- T.38 fax relay--RSVP bandwidth is adjusted to 80 kbps
- Fax pass-through--RSVP bandwidth is adjusted to 96 kbps

H.323 Support for Call Admission Control

H.323 call admission control (CAC) adjustments are allowed in the case of fax relay and fax pass-through. An H.323 gateway that uses a gatekeeper requests the following bandwidths from the gatekeeper when codec changes are necessary:

- T.38 fax relay--Bandwidth of 80 kbps
- Fax pass-through--Bandwidth of 96 kbps

If the gatekeeper accepts the bandwidth changes, the session is permitted to continue over the fax codec (G.711). If the gatekeeper rejects the bandwidth increase, the fax codec is terminated and the gateway uses the configured fax protocol fallback or the original voice codec, in which case the fax transfer fails.

H.323 or SIP Support for NSEs with T.38 Fax Relay

Use the **fax protocol** command to specify that a gateway should use NSEs for fax signaling. This option allows interoperability with MGCP gateways as well as other H.323 and SIP gateways. The use of NSEs and their payload type is negotiated in Session Description Protocol (SDP) messages. Because NSEs are passed in the media stream, they avoid the signaling delays that can be introduced by MGCP call agents. The addition of the NSE capability to Cisco SIP and H.323 gateways addresses these delays and improves interoperability between MGCP, SIP, and H.323 products.

If NSEs are specified and NSE use is not successfully negotiated between gateways, T.38 fax relay signaled through the protocol stack is attempted. If protocol-stack T.38 fax relay also fails, the configured fallback fax transfer protocol is used.

H.323 or SIP T.38 Fax Relay Interworking with Cisco MGCP Gateways

Specify that gateways must use T.38 fax relay and NSEs even though those gateways may be unable to negotiate those attributes by themselves at the time of call setup. This may happen during negotiations for fax attributes between H.323 or SIP gateways and MGCP gateways.

Both gateways must be configured to use T.38 fax relay and NSEs. On an H.323 or SIP gateway, use the **fax protocol t38 nse force** command. On an MGCP gateway, use the **mgcp fax t38 gateway force** command.

SG3 Fax Support on Cisco TDM-IP Voice Gateways and Cisco UBE Platforms

This feature provides support for V.34 fax relay based on the ITU Specification T.38 version 3 (04/2007) and for fax pass-through at SG3 speed. Prior to Cisco IOS Release 15.1(1)T, SG3-to-SG3 calls would fail because the V.34 modulation was not supported. A fallback solution allowed SG3-to-SG3 connections to be made, but the transmission speed was set to G3 levels.

For T.38 fax sessions to operate at SG3 speeds, all the endpoints involved must support T.38 Version 3 (v3) configuration and have negotiated T.38 v3. For example:

Originating Gateway(T.38 v3)--IP-(T.38 v3)Cisco UBE or TDM-IP GW(T.38 v3)-IP--Terminating Gateway(T.38 v3)

In this context, all currently supported TDM-IP gateways and Cisco UBE T.38 flows (H.323-H.323, H.323-SIP and SIP-SIP) are supported in Release 15.1(1)T. However, in topologies where at least one endpoint has a T.38 v0 configuration, the TDM-IP gateway or Cisco UBE configuration must be T.38 v0 (the lowest common version). Any other combination of T.38 v3 or v0 configuration involved in the Cisco UBE topologies is not supported.

When two endpoints are involved in negotiating the T.38 parameter, the mandatory parameter is the "FaxVersion." That is, when one of the endpoints supports Version 0 (v0), the resulting session operates as a v0 session. As long as Cisco UBE is configured for the lowest common version of the traffic expected, calls are completed successfully.

The information for supported calls is summarized in the tables below.

Table 3: Supported Call Flows with Mixed Endpoints at v0 and v3 Speeds

Emitting End	Receiving End	Resulting Session
v0	v0	v0
v0	v3	v0
v3	v0	v0
v3	v3	v3

Table 4: Supported Call Flows with Mixed Endpoints and Cisco UBE

Emitting End	Cisco UBE	Receiving End	Resulting Session
v0	v0	v0	v0
v0	v0	v3	v0
v3	v0	v0	v0
v3	v3	v3	v3

Beginning in Cisco IOS Release 15.1(1)T, full SG3 fax support is enabled on Cisco TDM-IP voice gateways and Cisco UBE platforms. To enable this feature, complete the procedures in the *How to Configure H.323 and SIP Fax Pass-Through* section of the Configuring Fax Pass-Through chapter of the *Cisco IOS Fax, Modem, and Text Support over IP Configuration Guide*, Release 15.1 and the procedures in the How to Configure H.323 and SIP T.38 Fax Relay, on page 91.

MGCP T.38 Fax Relay

When MGCP-based fax relay is disabled, MGCP networks use passthrough for fax relay transmission. However, when MGCP-based fax relay is enabled, ITU-T T.38 support is added, providing a standardized method of supporting reliable fax transmission in the MGCP network. With MGCP-based fax relay, interworking is allowed between the T.38 application that already exists on Cisco gateways and the MGCP applications on call agents (CAs).

MGCP-based fax relay provides two modes of implementation: gateway-controlled mode and CA-controlled mode. In gateway-controlled mode, a gateway advertises its capabilities using Session Description Protocol (SDP) messages during the establishment of a call, using the call-control protocol that was used to establish the call. After the call is established, the connected gateways negotiate the actual switch from voice to T.38

fax relay by exchanging named signaling event (NSE) or named telephony event (NTE) messages embedded in the RTP stream. That transmission is transparent to the CA, which knows only about the voice call. Gateway-controlled mode allows you to use MGCP-based fax relay (T.38) without upgrading the CA software to support the capability.

In CA-controlled mode, the gateways rely on the MGCP CA to direct the T.38 fax relay call flow.

Gateway-Controlled MGCP T.38 Fax Relay

In gateway-controlled mode, the gateways do not need instruction from the CA to switch to T.38 mode. This mode should be used if the CA has not been upgraded to support T.38 and MGCP interworking or if the CA does not want to manage fax calls.

Gateway-controlled mode can also be used to bypass the message delay overhead caused by CA handling; for example, to meet time requirements for switchover to T.38 mode. If the CA does not specify a mode to the gateway, the gateway defaults to gateway-controlled mode.

In gateway-controlled mode, the gateways exchange NSEs that provide the following services:

- Instruct the peer gateway to switch to T.38 for the call.
- Either acknowledge the switch and a readiness to accept packets or indicate that a gateway cannot accept T.38 packets.

MGCP-based fax relay in gateway-controlled mode uses the following call flow:

1. An incoming call is initially established as a voice call.
2. The gateways advertise capabilities in an SDP exchange during connection establishment.
3. If both gateways do not support T.38, fax passthrough is used for fax transmission. If both gateways do support T.38, they attempt to switch to T.38 upon fax tone detection. The existing audio channel is used for T.38 fax relay, and the existing connection port is reused to minimize delay. If failure occurs at some point during the switch to T.38, the call reverts to the original settings that it had as a voice call. If this failure occurs, a fallback to fax passthrough is not supported.
4. Upon completion of the fax image transfer, the connection remains established and reverts to a voice call using the previously designated codec, unless the CA instructs the gateway to do otherwise. If the CA has been configured to control fax relay, the CA instructs the gateway on processing the call with the fx: extension of the local connection option (LCO).

CA-Controlled MGCP T.38 Fax Relay

CA-controlled MGCP T.38 fax relay enables T.38 fax relay interworking between H.323 gateways and MGCP gateways and between two MGCP gateways under the control of a call agent. In Cisco IOS Release 12.3(1) and later releases, the feature has been modified. The new method supersedes previous methods for CA-controlled fax relay and introduces the following gateway capabilities to enable this functionality:

- Ability to accept the MGCP FXR package, to receive the fxr prefix in commands from the call agent, and to send the fxr prefix in notifications to the call agent.
- Ability to accept a new port when switching from voice to fax transmission during a call. This new ability allows successful T.38 CA-controlled fax between H.323 and MGCP gateways for those occasions in which the H.323 gateway assigns a new port when changing the call type from voice to fax. New ports are assigned in H.323 gateways using Cisco IOS images from Release 12.2(2)T to Release 12.2(7.5)T. Note that gateways in MGCP-to-MGCP fax calls simply reuse the same port. CA-controlled T.38 fax

relay enables MGCP gateways to handle both situations, either switching to a new port or reusing the same port, as directed by the call agent.

Note The CA-controlled mode described in this document makes obsolete the previous method that was described in *Media Gateway Control Protocol-Based Fax (T.38) and Dual Tone Multifrequency (IETF RFC 2833) Relay* . The previous CA-controlled mode for T.38 fax relay used the ca parameter to communicate with the call agent, and the ca parameter is no longer supported as of Cisco IOS Release 12.3(1). The previous method has been superseded by the CA-controlled mode described in this document. Note that the gateway (GW)-controlled mode that is described in the previous document remains supported and is the same as the GW-controlled mode that is described in this document.

The sequence for T.38 CA-controlled fax is as follows:

1. The MGCP call agent determines that CA-controlled mode is necessary for fax relay because the far end of the connection is an H.323 gateway or other entity incapable of directly negotiating T.38 with the Cisco IOS MGCP gateway.
2. The call agent establishes a voice call with the local MGCP gateway and specifies that any subsequent fax transmissions should take place using T.38 fax relay in CA-controlled mode. The call agent includes an "fxr/fx:t38" or "fxr/fx:t38-loose" parameter in the Local Connection Options parameter of the Create Connection (CRCX) command that it sends to the MGCP gateway. The term "loose" indicates that a description of T.38 capabilities is not required in the resulting Session Description Protocol (SDP) message.
3. When the voice call is established between the gateways, the call agent asks the MGCP gateway to notify it of any T.38 events with an "R: fxr/t38" requested event parameter in a Notification Request(RQNT) or Modify Connection (MDCX) command. If the MGCP gateway detects fax transmission during this call, it generates a Notify (NTFY) command with an "O: fxr/t38(start)" observed event parameter and sends it to the call agent.
4. The call agent responds with an MDCX containing one or both of the following:
   - "a:image/t38" descriptor in the Local Connection Options parameter
   - "m=image *port* udptl t38" line in the included SDP message

Note that *port* is replaced in the MDCX with the actual port number for the fax transmission. This port number can be the same as or different from the port number negotiated earlier when the voice call was established. T.38 CA-controlled fax supports either using the same port or switching to a new port for fax. Note that if the MGCP gateway does not detect fax first, it may receive the same MDCX prior to sending a NTFY.

1. When the fax transmission is complete, the MGCP gateway sends the call agent a NTFY command with an "O: fxr/t38(stop)" parameter. The call agent then has the option of either sending another MDCX to return to voice or using a Delete Connection (DLCX) command to terminate the call.

MGCP T.38 Fax Relay Interworking with Cisco H.323 and SIP Gateways

Some MGCP call agents do not properly pass those portions of Session Description Protocol (SDP) messages that advertise T.38 and NSE capabilities. As a result, gateways that are controlled by these call agents are unable to use NSEs to signal T.38 fax relay to other gateways that use NSEs. As of Cisco IOS Release 12.2(13)T, you can configure gateways to use T.38 fax relay and NSEs even though those gateways may be unable to negotiate those attributes by themselves at the time of call setup.

The **mgcp fax t38 gateway force** command provides a way to ensure gateway-controlled T.38 fax relay between an MGCP gateway and another gateway. The other gateway in the negotiation can be an H.323, Session Initiation Protocol (SIP), or MGCP gateway. Both gateways must be configured to use NSEs to signal T.38 fax relay mode switchover. On H.323 and SIP gateways, use the **fax protocol t38 nse force** command to specify the use of NSEs for T.38 fax relay. On MGCP gateways, use the **mgcp fax t38 gateway force** command.

NSEs are the Cisco-proprietary version of named telephony events (NTEs), which are defined in IETF RFC 2833. NSEs and NTEs are used to communicate telephony signaling events that are normally indicated by the presence of tones, such as dual-tone multifrequency (DTMF) or fax transmissions. NSEs and NTEs do not transmit audible signaling tones across the network, but instead work by sending a binary code that is later used to recreate a tone. NSEs use different values to represent events and tones than NTEs use.

NSEs and NTEs are passed in the media stream. They consist of Real-Time Transport Protocol (RTP) packets that have the same source and destination IP addresses and User Datagram Protocol (UDP) ports as the rest of the media stream. However, NSE and NTE packets use different RTP payload types than the rest of the media stream so that they can stand apart from the audio packets in the stream. NSEs are normally sent with RTP payload type 100.

SCCP and T.38 Fax Relay

For information about this capability, refer to the Configuring DTMF Relay, Fax Relay and Modem Relay chapter in the *Supplementary Services Features for FXS Ports on Cisco IOS Voice Gateways Configuration Guide.*

Fax CM Message Tone Suppression

Super Group 3 (SG3) is a new generation of fax machines that support speeds of up to 33.6 kbps through V.34 half duplex (HD) modulation and V.8 signaling.

SG3 V.8 fax CM message tone suppression enables SG3 fax machines to scale down without end-user interaction and without using the extra bandwidth required by modem pass-through and allows SG3 fax machines to interoperate over a fax-relay network at G3 speeds by blocking the SG3 V.8 CM message, or fax tone, from reaching the called fax machine. This causes the called fax machine to time out on the ANSam tone and scale down to G3 speeds by initiating V.21 negotiations.

SG3 V.8 fax CM message tone suppression supports both one-gateway and two-gateway solutions:

- With a one-gateway solution, the gateway on one end of the call can be configured to suppress the SG3 V.8 fax CM message independently of the gateway on the other end of the call. The one-gateway solution suppresses the fax CM tone on both TDM and IP interfaces (TI C5510 DSPs only), and can interoperate with third-party gateways when the fax CM tone suppression gateway is the originating gateway.
- With a two-gateway solution, the gateways on both ends of the call must have this feature enabled. The two-gateway solution suppresses the fax CM tone only on the TDM interface (TI C5421 and TI C549 DSPs). Both gateways must support this feature to interoperate at G3 speeds, or the fax tone suppression gateway must be the originating gateway.

How to Configure H.323 and SIP T.38 Fax Relay

There are two ways to configure T.38 fax relay on VoIP gateways:

Note Beginning in Cisco IOS Release 15.1(1)T, you can configure SG3 Fax Support when you enter the **fax protocol t38** command. This is described in the following sections.

Note Fax relay parameters that are set for an individual dial peer under the **dial-peer voice** command take precedence over global settings made under the **voice service voip** command.

Configuring One or More Individual VoIP Dial Peers for T.38 Fax Relay

Use the following tasks to configure T.38 Fax Relay for an individual VoIP dial peer.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **voip**
4. **dtmf-relay h245-signal**
5. **fax protocol t38** [**nse** [**force**]] [**version** {**0** | **3**}] [**ls-redundancy** *value* [**hs-redundancy** *value*]] [**fallback** {**cisco** | **none**| **pass-through** {**g711ulaw**| **g711alaw**}}]
6. **fax rate** {**12000** | **14400** | **2400** | **4800** | **7200** | **9600** | **disable** | **voice**} [**bytes** *rate*]
7. **fax-relay ecm disable**
8. **fax-relay sg3-to-g3 system**
9. **session protocol sipv2**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 25 voip`	Enters dial-peer configuration mode and defines a dial peer that directs traffic to or from a packet network. • *tag* --Dial-peer identifier that consists of one or more digits. Range: 1 to 2147483647. • **voip** --Calls from this dial peer use voice encapsulation on the packet network.

	Command or Action	Purpose
Step 4	**dtmf-relay h245-signal** **Example:** `Router(config-dial-peer)# dtmf-relay h245-signal`	Specifies how an H.323 or Session Initiation Protocol (SIP) gateway relays dual tone multifrequency (DTMF) tones between telephony interfaces and an IP network. • **h245-signal** --(Optional) Forwards DTMF tones by using the H.245 signal User Input Indication method. Supports tones from 0 to 9, *, #, and from A to D.

Step 5	**fax protocol t38** [**nse** [**force**]] [**version** {**0** | **3**}] [**ls-redundancy** *value* [**hs-redundancy** *value*]] [**fallback** {**cisco** | **none**| **pass-through** {**g711ulaw**| **g711alaw**}}]
	Example:
	`Router(config-dial-peer)# fax protocol t38 version 3`
		Specifies the global default ITU-T T.38 standard fax protocol to be used for all VoIP dial peers.
		• **nse** --(Optional) Uses Named Signaling Events (NSEs) to switch to T.38 fax relay.
		• **force** --(Optional) Unconditionally, uses Cisco NSE to switch to T.38 fax relay. This option allows T.38 fax relay to be used between Cisco H.323 or Session Initiation Protocol (SIP) gateways and Media Gateway Control Protocol (MGCP) gateways.
		• **version** --(Optional) Specifies a version for configuring fax speed:
		  • **0**--Configures version 0, which uses T.38 version 0 (1998, G3 faxing)
		  • **3**--Configures version 3, which uses T.38 version 3 (2004, V.34 or SG3 faxing)
		Note The **version 0**| **3** option was added in Cisco IOS Release 15.1(1)T to enable SG3 fax support.
		• **ls-redundancy** *value* --(Optional) Specifies the number of redundant T.38 fax packets to be sent for the low-speed V.21-based T.30 fax machine protocol. Range varies by platform from 0 (no redundancy) to 5 or 7. The default is 0.
		• **hs-redundancy** *value* --(Optional) Specifies the number of redundant T.38 fax packets to be sent for high-speed V.17, V.27, and V.29 T.4 or T.6 fax machine image data. Range varies by platform from 0 (no redundancy) to 2 or 3. The default is 0.
		Note Setting the **hs-redundancy** parameter to a value greater than 0 causes a significant increase in the network bandwidth consumed by the fax call.
		• **fallback** --(Optional) A fallback mode is used to transfer a fax across a VoIP network if T.38 fax relay could not be successfully negotiated at the time of the fax transfer.

	Command or Action	Purpose
		• **cisco** --(Optional) Cisco-proprietary fax protocol. **Note** Do not use the **cisco** keyword for the fallback option if you specified **version 3** for SG3 fax transmission. • **none** --(Optional) No fax pass-through or T.38 fax relay is attempted. All special fax handling is disabled, except for modem pass-through if configured with the modem pass-through command. • **pass-through** --(Optional) The fax stream uses one of the following high-bandwidth codecs: • **g711ulaw**--Uses the G.711 u-law codec. • **g711alaw**--Uses the G.711 a-law codec.
Step 6	**fax rate** {**12000** | **14400** | **2400** | **4800** | **7200** | **9600** | **disable** | **voice**} [**bytes** *rate*] **Example:** `Router(config-dial-peer)# fax rate 14400`	(Optional) Selects the fax transmission speed to be attempted when this dial peer is used. • **12000** , **14400**, **2400**, **4800**, **7200**, **9600**--Maximum bits-per-second speed. • **bytes** *rate* --(Optional) Fax packetization rate, in ms. Range: 20 to 48. Default: 20. For T.38 fax relay, this keyword-argument pair is valid only on Cisco 5350, Cisco 5400, and Cisco 5850 routers. For other routers, the packetization rate for T.38 fax relay is fixed at 40 ms and cannot be changed with this keyword-argument pair. • **disable** --Disables fax relay transmission capability. • **voice** --Highest possible transmission speed allowed by the voice rate. For example, if the voice codec is G.711, fax transmission occurs at up to 14400 bps because 14400 bps is less than the 64-kbps voice rate. If the voice codec is G.729 (8 kbps), the fax transmission speed is 7200 bps. This is the default.
Step 7	**fax-relay ecm disable** **Example:** `Router(config-dial-peer)# fax-relay ecm disable`	(Optional) Disables fax-relay ECM. **Note** To enable ECM, use the **no** form of this command. **Note** If you are using Cisco IOS Release 15.1(1)T and enabling SG3 fax support, do not enter this command.

	Command or Action	Purpose
Step 8	**fax-relay sg3-to-g3 system** **Example:** `Router(config-dial-peer)# fax-relay sg3-to-g3 system`	Specifies that for SIP and H.323 signaling types, V.8 fax CM message suppression is enabled on the specific dial peer. Enabled by default. • **system** --Uses the protocol set under the voice-service configuration mode. **Note** If you are using Cisco IOS Release 15.1(1)T and enabling SG3 fax support, do not enter this command.
Step 9	**session protocol sipv2** **Example:** `Router(config-dial-peer)# session protocol sipv2`	(Optional) Specifies the IETF SIP session protocol for calls between the local and remote routers using the packet network. **Note** This command is required for SIP calls.

Configuring T.38 Fax Relay on VoIP Dial Peers Globally

Use the following steps to configure T.38 fax relay globally for previously defined VoIP dial peers.

Alternately, you can configure fax relay for individual VoIP dial peers. See the Configuring One or More Individual VoIP Dial Peers for T.38 Fax Relay, on page 92.

Note Fax relay parameters that are set for an individual dial peer under the **dial-peer voice** command take precedence over global settings made under the **voice service voip** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **fax protocol t38** [**nse** [**force**]] [**version** {**0** | **3**}] [**ls-redundancy** *value* [**hs-redundancy** *value*]] [**fallback** {**cisco** | **none** | **pass-through** {**g711ulaw** | **g711alaw**}}]
5. **fax-relay sg3-to-g3**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Router# configure terminal`	
Step 3	**voice service voip** **Example:** `Router(config)# voice service voip`	Enters voice-service configuration mode.

Step 4	**fax protocol t38** [**nse** [**force**]] [**version**{**0** | **3**}] [**ls-redundancy** *value* [**hs-redundancy** *value*]] [**fallback** {**cisco** | **none** | **pass-through** {**g711ulaw** | **g711alaw**}}]
	Example:
	`Router(config-voi-srv)# fax protocol t38 version 3`
		Specifies the global default ITU-T T.38 standard fax protocol to be used for all VoIP dial peers.
		• **nse** --(Optional) Uses Named Signaling Events (NSEs) to switch to T.38 fax relay.
		• **force** --(Optional) Unconditionally, uses Cisco NSE to switch to T.38 fax relay. This option allows T.38 fax relay to be used between Cisco H.323 or Session Initiation Protocol (SIP) gateways and Media Gateway Control Protocol (MGCP) gateways.
		• **version** --(Optional) Specifies a version for configuring fax speed:
		  • **0**--Configures version 0, which uses T.38 version 0 (1998, G3 faxing)
		  • **3**--Configures version 3, which uses T.38 version 3 (2004, V.34 or SG3 faxing)
		Note The **version 0**| **3** option was added in Cisco IOS Release 15.1(1)T to enable SG3 fax support.
		• **ls-redundancy** *value* --(Optional) Specifies the number of redundant T.38 fax packets to be sent for the low-speed V.21-based T.30 fax machine protocol. Range varies by platform from 0 (no redundancy) to 5 or 7. The default is 0.
		• **hs-redundancy** *value* --(Optional) Specifies the number of redundant T.38 fax packets to be sent for high-speed V.17, V.27, and V.29 T.4 or T.6 fax machine image data. Range varies by platform from 0 (no redundancy) to 2 or 3. The default is 0.
		Note Setting the **hs-redundancy** parameter to a value greater than 0 causes a significant increase in the network bandwidth consumed by the fax call.
		• **fallback** --(Optional) A fallback mode is used to transfer a fax across a VoIP network if T.38 fax relay could not be successfully negotiated at the time of the fax transfer.

	Command or Action	Purpose
		• **cisco** --(Optional) Cisco-proprietary fax protocol. **Note** Do not use the **cisco** keyword for the fallback option if you specified **version 3** for SG3 fax transmission. • **none** --(Optional) No fax pass-through or T.38 fax relay is attempted. All special fax handling is disabled, except for modem pass-through if configured with the modem pass-through command. • **pass-through** --(Optional) The fax stream uses one of the following high-bandwidth codecs: • **g711ulaw**--Uses the G.711 u-law codec. • **g711alaw**--Uses the G.711 a-law codec.
Step 5	**fax-relay sg3-to-g3** **Example:** `Router(config-voi-serv)# fax-relay sg3-to-g3`	Specifies that for SIP and H.323 signaling types, V.8 fax CM message suppression is enabled for all dial peers on the digital signal processor (DSP) firmware. Enabled by default. **Note** If you are using Cisco IOS Release 15.1(1)T and enabling SG3 fax support, do not enter this command.

Troubleshooting Tips for H.323 or SIP T.38 Fax Relay

To troubleshoot T.38 fax relay, perform the following steps:

- Ensure that you can make a voice call.
- Ensure that the desired fax protocol was set using the **fax protocol** command on both the originating and terminating gateways.
- Ensure that the fax protocol is configured as T.38 at the global configuration level or at the dial-peer configuration level for both the originating and terminating gateways.
- Use the **show call active voice** command to display information for the active call table.
- Use the **show call history fax** command to display recent call history for faxes.
- Use the **show dial-peer voice** command to display configuration information for dial peers.
- For H.323 gateways, use the **debug cch323 all** command to enable all H.323 debugging capabilities, or use one of the following commands to debug problems while making the call:
  - **debug cch323 error**
  - **debug cch323 h225**
  - **debug cch323 h245**
  - **debug cch323 RAS**
  - **debug cch323 session**
  - **debug voip ccapi inout**

- **debug vtsp session**

- For SIP gateways, use the **debug ccsip all** command to enable all SIP debugging capabilities, or use one of the following SIP debug commands:
  - **debug ccsip calls**
  - **debug ccsip error**
  - **debug ccsip events**for T.38 fax relay
  - **debug ccsip info**
  - **debug ccsip media**
  - **debug ccsip messages**
  - **debug ccsip states**

How to Configure MGCP T.38 Fax Relay

Cisco supports two modes of MGCP T.38 fax relay:

- In gateway-controlled mode, a call agent uses the fx: extension of the local connection option (LCO) to instruct a gateway about how to process a call. Gateways do not need instruction from the call agent to switch to T.38 mode.
- In call-agent (CA)-controlled mode, the call agent can instruct the gateway to switch to T.38 for a call. In Cisco IOS Release 12.3(1) and later releases, CA-controlled mode enables T.38 fax relay interworking between H.323 gateways and MGCP gateways and between two MGCP gateways under the control of a call agent.

Select one of the following MGCP T.38 fax relay configuration tasks:

Configuring Gateway-Controlled MGCP T.38 Fax Relay

Use the following steps to configure gateway-controlled MGCP T.38 fax relay.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mgcp fax t38** {**ecm** | **gateway force**| **hs_redundancy** *value* | **inhibit** | **ls_redundancy** *value* | **nsf** *word*}
4. **mgcp tse payload** *value*
5. **mgcp timer nse-response t38** *timer*
6. **mgcp fax rate** {**2400** | **4800** | **7200** | **9600** | **12000** | **14400** | **voice**
7. **mgcp fax-relay sg3-to-g3**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**mgcp fax t38** {**ecm** | **gateway force**| **hs_redundancy** *value* | **inhibit** | **ls_redundancy** *value* | **nsf** *word*} **Example:** `Router(config)# mgcp fax t38 ls_redundancy 2`	(Optional) Configures MGCP T.38 fax relay parameters. • **ecm** --Enables Error Correction Mode (ECM) for the gateway. By default, ECM is not enabled. • **gateway force** --Forces gateway-controlled T.38 fax relay using Cisco-proprietary named signaling events (NSEs) even if the capability to use T.38 and NSEs cannot be negotiated by the MGCP call agent at call setup time. By default, force is not enabled. • **hs_redundancy** *value* --Number of redundant T.38 fax packets to send for high-speed V.17, V.27, and V.29 T.4 or T.6 fax machine image data. Range: 0 (no redundancy) to 2. The default is 0. • **ls_redundancy** *value* --Number of redundant T.38 fax packets to send for low-speed V.21-based T.30 fax machine protocol. Range: 0 (no redundancy) to 5. The default is 0. **Note** Setting the **hs_redundancy** parameter greater than 0 causes a significant increase in network bandwidth consumed by a fax call. • **inhibit** --Disables MGCP-based T.38 fax relay on the gateway. By default, T.38 is enabled. **Note** If the MGCP gateway uses the auto-configuration function, the **mgcp fax t38 inhibit**command is automatically configured on the gateway each time a new configuration is downloaded. Beginning with Cisco IOS Software Release 12.4T, the auto-configuration of this command is removed. For MGCP gateways running Cisco IOS version 12.4T or later, you must manually configure the **mgcp fax t38 inhibit**command to use T.38 fax relay. • **nsf** --Overrides the non-standard facilities (NSF) code with the code provided in the *word* argument. NSFs are capabilities that fax manufacturers have built into fax machines to distinguish their products from others. By default, the NSF code is not overridden.

	Command or Action	Purpose
		• *word*--Two-digit country code and four-digit manufacturer code, in hexadecimal.
Step 4	**mgcp tse payload** *value* **Example:** `Router(config)# mgcp tse payload 106`	(Required) Enables inband telephony signaling events (TSEs) and specifies the payload value to be used during fax and modem pass-through and network continuity tests. • *value* --TSE payload value. The range is 98 to 119. The default is 100.
Step 5	**mgcp timer nse-response t38** *timer* **Example:** `Router(config)# mgcp timer nse-response t38 250`	Configures how a gateway detects the Real-Time Transport Protocol (RTP) stream host. • **nse-response t38** *timer* --Timeout period, in milliseconds, for awaiting T.38 named signaling event (NSE) responses from a peer gateway. Range is from 100 to 3000. The default is 200.
Step 6	**mgcp fax rate** {**2400** | **4800** | **7200** | **9600** | **12000** | **14400** | **voice** **Example:** `Router(config)# mgcp fax rate 9600`	(Optional) Establishes the maximum fax rate for MGCP T.38 sessions. • **2400** , **4800**, **7200**, **9600**, **14400**--Maximum bits-per-second speed. • **voice** --Highest possible transmission speed allowed by the voice rate. For example, if the voice codec is G.711, fax transmission occurs at up to 14400 bps because 14400 bps is less than the 64-kbps voice rate. If the voice codec is G.729 (8 kbps), the fax transmission speed is 7200 bps. This is the default. **Note** MGCP normally limits the maximum fax rate on a voice port to the bandwidth of the configured voice codec. This ensures that the fax session does not exceed the bandwidth initially authorized for the voice call. In some cases an administrator may desire to exceed the voice bandwidth when the call switches to fax in order to offer the best possible fax rate. The **mgcp fax rate** command allows you to override this limitation. **Note** When the MGCP fax rate is set to the highest possible transmission speed allowed by the voice codec (**mgcp fax rate voice**), all MGCP endpoints limit T.38 fax calls to this speed. **Note** The values for this command apply only to the fax transmission speed and do not affect the quality of the fax itself.

	Command or Action	Purpose
Step 7	**mgcp fax-relay sg3-to-g3** **Example:** `Router(config)# mgcp fax-relay sg3-to-g3`	Specifies that for MGCP signaling types, V.8 fax CM message suppression is enabled on the digital signal processor (DSP) firmware.

Configuring CA-Controlled MGCP T.38 Fax Relay

Use the following steps to configure CA-controlled MGCP T.38 fax relay.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no mgcp fax t38 inhibit**
4. **mgcp package-capability fxr-package**
5. **mgcp default-package fxr-package**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**no mgcp fax t38 inhibit** **Example:** `Router(config)# no mgcp fax t38 inhibit`	(Optional) Enables T.38 fax relay on the gateway if it has been previously disabled. **Note** T.38 fax relay is enabled on the gateway by default. The command is included here to illustrate how you would enable T.38 if it were disabled by a previous command. **Note** If the MGCP gateway uses the auto-configuration function, the **mgcp fax t38 inhibit**command is automatically configured on the gateway each time a new configuration is downloaded. Beginning with Cisco IOS Software Release 12.4T, the auto-configuration of this command is removed. For MGCP gateways running Cisco IOS version 12.4T or later, you must manually configure the **mgcp fax t38 inhibit**command to use T.38 fax relay.

	Command or Action	Purpose
Step 4	**mgcp package-capability fxr-package** **Example:** `Router(config)# mgcp package-capability fxr-package`	(Optional) Specifies an MGCP package capability type for a media gateway. • **fxr-package** --FXR package for fax transmissions.
Step 5	**mgcp default-package fxr-package** **Example:** `Router(config)# mgcp default-package fxr-package`	(Optional) Configures the default package capability type for the media gateway. • **fxr-package** --FXR package for fax transmissions.

Troubleshooting Tips for MGCP T.38 Fax Relay

Use the following steps to troubleshoot MGCP T.38 fax relay:

- Ensure that you have a working MGCP network and that you can make a voice call.
- Ensure that T.38 fax relay for MGCP is configured on both the originating and terminating gateways.
- Use the following commands during the call:
  - The **show mgcp** [**connection** | **endpoint** | **statistics**] command displays information about MGCP calls.
  - The **show voice call summary** command indicates, during a T.38 fax transmission, a change of state from S_CONNECT to S_FAX in the VTSP STATE column and a change from the codec name to a numeric fax rate in the CODEC column (for example, g711u changes to 14400).
  - The **debug mgcp packets** command displays the MGCP side of the call flow.

For CA-controlled T.38 fax relay, you can verify the MGCP side of the call flow by using the **debug mgcp packets** command. You should see the following output:

- CRCX from the call agent with "fxr/fx:t38-loose" or "fxr/fx:t38" parameter
- RQNT from the call agent with "R: fxr/t38" parameter
- NTFY from the gateway with "O: fxr/t38(start)" parameter (optionally)
- MDCX from the call agent with either "m=image" in the SDP message, or "a:image/t38" in the Local Connection Options message, or both.

For CA-controlled T.38 fax relay, you should see the following messages in the output from a **show voice call summary** command on the MGCP gateway during a T.38 fax transmission:

- Change of state from S_CONNECT to S_FAX in the VTSP STATE column
- Change from codec name to numeric fax rate (such as "g711u" to 14400") in the CODEC column

Configuration Examples for T.38 Fax Relay

H.323 T.38 Fax Relay with ECM Enabled Example

This example configuration shows T.38 fax relay in an H.323 network with ECM enabled:

```
.
.
.
voice service voip
 fax protocol t38
.
.
.
interface Ethernet0/0
 ip address 10.0.47.47 255.255.0.0
 h323-gateway voip interface
 h323-gateway voip id ipaddr 10.0.47.36 1719
 h323-gateway voip h323-id 36402
.
.
.
dial-peer voice 14151 voip  ! Uses t38 fax from voice service voip.
 destination-pattern 14151..
 session target ras
dial-peer voice 14152 voip  ! Uses Cisco fax for a specific dial peer.
 destination-pattern 14152..
 session target ras
 fax protocol cisco
gateway
end
```

T.38 Fax Relay with ECM Disabled on Dial Peer Example

This example shows ECM disabled on dial peer 50:

```
.
.
.
dial-peer voice 100 pots
 destination-pattern 5550919
 port 2/0:D
 prefix 5550
!
dial-peer voice 50 voip
 incoming called-number 5550919
 codec g711ulaw
 fax-relay ecm disable
 fax rate 9600
 fax protocol t38 ls-redundancy 0 hs-redundancy 0
.
.
.
```

Gateway-Controlled MGCP T.38 Fax Relay Example

The following example shows a configuration for gateway-controlled T.38 fax in an MGCP network. This configuration uses the defaults for the **mgcp fax t38** command and the **mgcp timer nse-response t38** commands, so they do not appear in the running configuration presented in the example.

```
.
.
.
!
mgcp
mgcp call-agent 192.168.195.147 2427 service-type mgcp version 0.1
```

```
mgcp dtmf-relay voip codec all mode nse
mgcp modem passthrough voip mode ca
mgcp package-capability dtmf-package
mgcp default-package mo-package
mgcp tse payload 110
no mgcp timer receive-rtcp
mgcp timer net-nse-rsp 300
.
.
.
```

CA-Controlled MGCP T.38 Fax Relay Example

This example configuration shows CA-controlled MGCP T.38 fax relay.

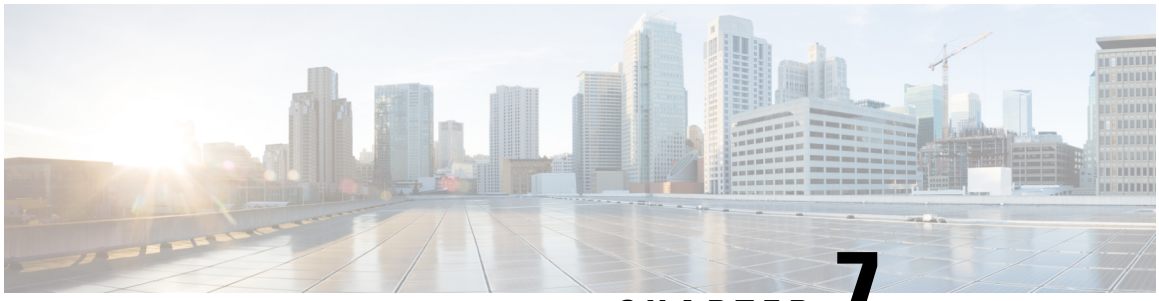
```
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname tyler
!
boot system tftp project/c2600-is-mz.0711 192.168.222.10
no logging buffered
no logging rate-limit
enable password mary
!
ip subnet-zero
!
!
no ip domain lookup
ip domain name abctrading.com
ip host jackson 192.168.184.144
ip host lincoln 192.168.222.10
ip name-server 192.168.12.13
ip name-server 192.168.12.134
ip name-server 192.168.222.72
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
mrcp client session history duration 0
mrcp client session history records 0
fax interface-type fax-mail
mta receive maximum-recipients 0
!
!
interface FastEthernet0/0
 ip address 192.168.191.132 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.184.1
ip route 192.168.0.0 255.255.0.0 192.168.184.1
```

```
ip http server
ip http port 1111
ip pim bidir-enable
!
!
access-list 101 permit tcp any any
access-list 101 permit udp host 192.168.184.144 any
access-list 101 permit udp host 192.168.222.10 any
access-list 102 permit ip any any
access-list 111 permit udp host 192.168.184.144 any
access-list 111 permit udp host 192.168.191.132 any
access-list 111 permit icmp any any
!
snmp-server packetsize 4096
snmp-server enable traps tty
call rsvp-sync
!
voice-port 1/0/0
!
voice-port 1/0/1
!
voice-port 1/1/0
!
voice-port 1/1/1
!
mgcp
mgcp call-agent 192.168.184.144 3562 service-type mgcp version 0.1
mgcp dtmf-relay voip codec all mode nse
mgcp tse payload 102
no mgcp timer receive-rtcp
!
mgcp profile default
!
dial-peer cor custom
!
!
dial-peer voice 110 pots
 application mgcpapp
 port 1/1/0
!
dial-peer voice 111 pots
 application mgcpapp
 port 1/1/1
!
!
line con 0
 exec-timeout 0 0
line aux 0
 exec-timeout 0 0
line vty 0 4
 exec-timeout 0 0
 password lab
 login
line vty 5 15
 exec-timeout 0 0
 password lab
 login
!
end
```

SG3 Fax Support on the Cisco TDM-IP Voice Gateways and Cisco UBE Platforms Example

The following example shows fax protocol T.38 version 3 enabled to provide SG3 fax support:

```
!
voice service voip
 fax protocol t38 version 3 ls-redundancy 0 hs-redundancy 0 fallback cisco
!
!
interface FastEthernet0/0
 ip address 1.2.103.1 255.255.0.0
!
!
!
dial-peer voice 100 voip
 destination-pattern 1.....
 session target ipv4:1.2.103.3
 dtmf-relay h245-signal
 fax protocol t38 version 3 ls-redundancy 0 hs-redundancy 0 fallback cisco
!
dial-peer voice 200 voip
 destination-pattern 2.....
 session protocol sipv2
 session target ipv4:1.2.103.3
 dtmf-relay rtp-nte
 fax protocol pass-through g711ulaw
!
dial-peer voice 6789 voip
 destination-pattern 6789
 session target ipv4:1.2.102.2
 dtmf-relay rtp-nte
 fax protocol pass-through g711ulaw
!
!
sip-ua
```



CHAPTER 7

T.38 Fax Support on Cisco UBE for IPv6

T.38 Fax Support on Cisco UBE for IPv6

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About T.38 Fax Support on Cisco UBE for IPv6

Cisco Unified Border Element in VoIPv6

The Cisco Unified Border Element (UBE) feature adds IPv6 capability to existing VoIP features. This feature adds dual-stack support on voice gateways and MTP, IPv6 support for SIP trunks, and support for SCCP-controlled analog voice gateways. Real-time control protocol (RTCP) pass-through and T.38 fax over IPv6 have also been added to Cisco UBE.

How to Configure T.38 Fax Support on Cisco UBE for IPv6

Configuring IPv6 Support for Cisco UBE

Perform this task to configure IPv6 support for Cisco UBE.

Note In Cisco UBE, IPv4-only and IPv6-only modes are not supported when endpoints are dual-stack. In this case, Cisco UBE must also be configured in dual-stack mode.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sip-ua**
4. **protocol mode** {**ipv4** | **ipv6** | **dual-stack preference** {**ipv4** | **ipv6**}}
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**sip-ua** **Example:** `Router(config)# sip-ua`	Enters SIP user-agent configuration mode.
Step 4	**protocol mode** {**ipv4**	**ipv6**	**dual-stack preference** {**ipv4**	**ipv6**}} **Example:** `Router(config-sip-ua)# protocol mode ipv6`	Configures the Cisco IOS SIP stack. • **protocol mode dual-stack preference** {**ipv4**	**ipv6**}--Sets the IP preference when the **anat** command is configured. • **protocol mode** {**ipv4**	**ipv6**}--Passes the IPv4 or IPv6 address in the SIP invite. • **protocol mode dual-stack** --Passes both the IPv4 addresses and the IPv6 addresses in the SIP invite and sets priority based on the far-end IP address.
Step 5	**end** **Example:** `Router(config-sip-ua)# end`	Exits SIP user-agent configuration mode.

Configuring T.38 Fax Globally

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **no ip address trusted authenticate**
5. **allow-connections** {**h323** | **sip**} **to** {**h323** | **sip**}
6. **fax protocol t38** [**nse** [**force**]] [**version** {**0** | **3**}] [**ls-redundancy** *value* [**hs-redundancy** *value*]] [**fallback** {**cisco** | **none** | **pass-through** {**g711ulaw** | **g711alaw**}}]
7. **sip**
8. **bind control source-interface** *type number*
9. **bind media source-interface** *type number*
10. **no anat**
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Router(config)# voice service voip`	Enters voice service configuration mode.
Step 4	**no ip address trusted authenticate** **Example:** `Router(conf-voi-serv)# no ip address trusted authenticate`	Disables the IP address trusted authentication feature for incoming H.323 or SIP trunk calls for toll-fraud prevention.
Step 5	**allow-connections** {**h323**	**sip**} **to** {**h323**	**sip**} **Example:** `Router(conf-voi-serv)# allow-connections sip to sip`	Allows connections between specific types of endpoints in a VoIP network.

	Command or Action	Purpose
Step 6	**fax protocol t38** [**nse** [**force**]] [**version** {**0** | **3**}] [**ls-redundancy** *value* [**hs-redundancy** *value*]] [**fallback** {**cisco** | **none** | **pass-through** {**g711ulaw** | **g711alaw**}}] **Example:** `Router(conf-voi-serv)# fax protocol t38 version 0 ls-redundancy 0 hs-redundancy 0 fallback cisco`	Specifies the global default ITU-T T.38 standard fax protocol to be used for all VoIP dial peers.
Step 7	**sip** **Example:** `Router(conf-voi-serv)# sip`	Enters SIP configuration mode.
Step 8	**bind control source-interface** *type number* **Example:** `Router(conf-serv-sip)# bind control source-interface GigabitEthernet 0/0`	Binds Session Initiation Protocol (SIP) signaling packets and specifies an interface as the source address of SIP packets.
Step 9	**bind media source-interface** *type number* **Example:** `Router(conf-serv-sip)# bind media source-interface GigabitEthernet 0/0`	Binds only media packets to the IPv4 or IPv6 address of a specific interface and specifies an interface as the source address of SIP packets.
Step 10	**no anat** **Example:** `Router(conf-serv-sip)# no anat`	Enables Alternative Network Address Types (ANAT) on a SIP trunk.
Step 11	**end** **Example:** `Router(conf-serv-sip)# end`	Exits SIP configuration mode and returns to the privileged EXEC mode.

Configuration Examples for T.38 Fax Support on Cisco UBE for IPv6

Example: Verifying T.38 Fax Configuration

```
Router# debug ccsip all
Received:
INVITE sip:5555555555@[2001:DB8:1:1:1:1:1:1118]:5060 SIP/2.0
Via: SIP/2.0/UDP [2001:DB8:1:1:1:1:1:1115]:5060;branch=z9hG4bK83AE3
Remote-Party-ID:
<sip:2222222222@[2001:DB8:1:1:1:1:1:1115]>;party=calling;screen=no;privacy=off
From: <sip:2222222222@[2001:DB8:1:1:1:1:1:1115]>;tag=627460F0-1259
To: <sip:5555555555@[2001:DB8:1:1:1:1:1:1118]>
```

```
Date: Tue, 01 Mar 2011 08:49:48 GMT
Call-ID: B30FCDEB-431711E0-8EDECB51-E9F6B1F1@2001:DB8:1:1:1:1:1:1115
Supported: 100rel,timer,resource-priority,replaces
Require: sdp-anat
Min-SE:  1800
Cisco-Guid: 2948477781-1125585376-2396638033-3925258737
User-Agent: Cisco-SIPGateway/IOS-15.1(3.14.2)PIA16
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO,
REGISTER
CSeq: 101 INVITE
Max-Forwards: 70
Timestamp: 1298969388
Contact: <sip:2222222222@[22001:DB8:1:1:1:1:1:1115]:5060>
Expires: 180
Allow-Events: telephone-event
Content-Type: application/sdp
Content-Disposition: session;handling=required
Content-Length: 495
v=0
o=CiscoSystemsSIP-GW-UserAgent 7880 7375 IN IP6 2001:DB8:1:1:1:1:1:1115
s=SIP Call
c=IN IP6 2001:DB8:1:1:1:1:1:1115
t=0 0
a=group:ANAT 1 2
m=audio 17836 RTP/AVP 0 101 19
c=IN IP6 2001:DB8:1:1:1:1:1:1115
a=mid:1
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=rtpmap:19 CN/8000
a=ptime:20
m=audio 18938 RTP/AVP 0 101 19
c=IN IP4 9.45.36.111
a=mid:2
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=rtpmap:19 CN/8000
a=ptime:20
"Received:
INVITE sip:2222222222@[2001:DB8:1:1:1:1:1:1117]:5060 SIP/2.0
Via: SIP/2.0/UDP [2001:DB8:1:1:1:1:1:1116]:5060;branch=z9hG4bK38ACE
Remote-Party-ID:
<sip:5555555555@[2001:DB8:1:1:1:1:1:1116]>;party=calling;screen=no;privacy=off
From: <sip:5555555555@[2001:DB8:1:1:1:1:1:1116]>;tag=4FE8C9C-1630
To: <sip:2222222222@[2001:DB8:1:1:1:1:1:1117]>;tag=1001045C-992
Date: Thu, 10 Feb 2011 12:15:08 GMT
Call-ID: 5DEDB77E-ADC11208-808BE770-8FCACF34@2001:DB8:1:1:1:1:1:1117
Supported: 100rel,timer,resource-priority,replaces,sdp-anat
Min-SE:  1800
Cisco-Guid: 1432849350-0876876256-2424621905-3925258737
User-Agent: Cisco-SIPGateway/IOS-15.1(3.14.2)PIA16
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO,
REGISTER
CSeq: 101 INVITE
Max-Forwards: 70
Timestamp: 1297340108
Contact: <sip:5555555555@[2001:DB8:1:1:1:1:1:1116]:5060>
Expires: 180
Allow-Events: telephone-event
Content-Type: application/sdp
Content-Length: 424
v=0
```

```
o=CiscoSystemsSIP-GW-UserAgent 8002 7261 IN IP6 2001:DB8:1:1:1:1:1:1116
s=SIP Call
c=IN IP6 2001:DB8:1:1:1:1:1:1116
t=0 0
m=image 17278 udptl t38
c=IN IP6 2001:DB8:1:1:1:1:1:1116
a=T38FaxVersion:0
a=T38MaxBitRate:14400
a=T38FaxFillBitRemoval:0
a=T38FaxTranscodingMMR:0
a=T38FaxTranscodingJBIG:0
a=T38FaxRateManagement:transferredTCF
a=T38FaxMaxBuffer:200
a=T38FaxMaxDatagram:320
a=T38FaxUdpEC:t38UDPRedundancy"
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Cisco IOS IPv6 commands	Cisco IOS IPv6 Command Reference
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	*IPv6 RFCs*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

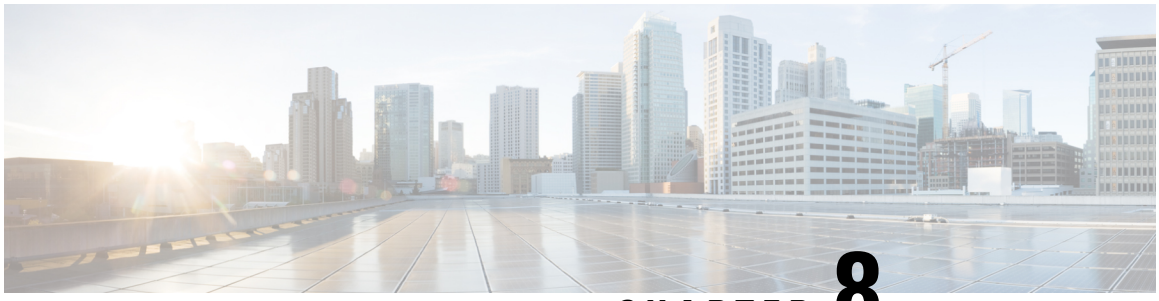
Feature Information for T.38 Fax Support on Cisco UBE for IPv6

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 5: Feature Information for T.38 Fax Support on Cisco UBE for IPv6

Feature Name	Releases	Feature Information
T.38 Fax Support on Cisco UBE for IPv6	15.2(1)T	IPv6 supports this feature.



CHAPTER 8

Configuring T.37 Store-and-Forward Fax

Configuring T.37 Store-and-Forward Fax

Fax pass-through is a method for sending faxes over IP networks. This chapter describes the configuration of T.37 store-and-forward fax on H.323 and Session Initiation Protocol (SIP) networks. It includes the following features:

- Extended Simple Mail Transfer Protocol (ESMTP) Accounting in Store-and-Forward Fax
- T.37 Store-and-Forward Fax

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring T.37 Store-and-Forward Fax

- Ensure that your IP network is configured and operational.
- Ensure that your system meets the requirements for store-and-forward fax and supported call-control protocols.
- The T.37 on-ramp gateway requires the system to have at least 2 MB I/O memory and 8 MB process memory for a session. If either of these memory requirements are not met, the T.37 session will fail.

Restrictions for Configuring T.37 Store-and-Forward Fax

- T.37 store-and-forward fax is not supported on Media Gateway Control Protocol (MGCP) networks.

- For T.37 store-and-forward fax, Cisco does not support any encryption with the Simple Mail Transfer Protocol (SMTP) implementation.
- Cisco fax gateways support only the TIFF format described in RFC 2301, *File Format for Internet Fax* , and RFC 2302, Tagged *>Image File Format (TIFF)--Image/TIFF MIME Sub-Type Registration* with Profile S. The TIFF header offset must be less than 1 KB and the header must be at the top of the TIFF page.
- Cisco's implementation of T.37 does not provide support for the optional Error Correction Mode (ECM) feature found on most G3 fax machines. ECM retransmits any corrupted scan lines that make up the image on the fax page to ensure that fax communications are received error-free. In networks with impairments, the lack of ECM support does not allow fax page information to be corrected. In some cases, this can lead to fax pages that have image quality issues, incomplete attachments in the fax e-mail, or even failure of the fax call.
- SG3 faxes are not supported.

Information About T.37 Store-and-Forward Fax

The purpose of an on-ramp gateway in store-and-forward fax is to receive faxes from the PSTN or standard fax devices. The on-ramp gateway performs the following actions:

1. Converts a fax message into a TIFF file.
2. Creates a standard Multipurpose Internet Mail Extension (MIME) e-mail message.
3. Attaches the TIFF file to the e-mail message.
4. Forwards the e-mail message and attachment to the messaging infrastructure of a designated SMTP server, where the message is stored.

The on-ramp gateway uses the sending Message Transfer Agent (MTA) and dial peers to receive fax calls from the PSTN and to define delivery parameters for the resulting e-mail message to which the fax TIFF file is attached. MTAs define the following elements of e-mail messages to which fax TIFF files are attached:

- Originator
- Subject of the message
- Destination mail server
- Return path
- Postmaster (default mail station for undeliverable messages)
- E-mail header information
- Address to which any disposition notices are sent

A DSN message notifies the sender of an e-mail message that contains a fax TIFF image about the status of that message. DSNs are automatically generated by the SMTP server and are described in RFC 1891, RFC 1892, RFC 1893, and RFC 1894. The following states can be reported to the sender:

- Delay--Message delivery was delayed.
- Success--Message was successfully delivered to the recipient mailbox.

- Failure--SMTP server was unable to deliver the message to the recipient.

The on-ramp gateway security controls who can send fax messages over the packet network. On-ramp accounting keeps track of who uses the packet network resources and how long they use them. On-ramp security and accounting are facilitated by authentication, authorization, and accounting (AAA) security services using RADIUS or TACACS+ as the local security protocol. On-ramp gateway faxing is a client of either the RADIUS or the TACACS+ authentication server. User information is forwarded to the AAA interface, and authentication requests are forwarded to the security server.

Authentication must be completed before the first page of the faxed material is accepted by the Fax Application Process (FAP). If a response is not received from the AAA server before the first page is received, the fax modem or voice card disconnects the call.

RADIUS attributes define specific AAA elements in a user profile. The user profile is stored on the RADIUS server. The Cisco implementation of RADIUS supports Internet Engineering Task Force (IETF) and vendor-proprietary attributes. IETF RADIUS attribute 26 enables vendors to support extended attributes not suitable for general use. The Cisco fax applications use the RADIUS implementation of vendor-specific options in the recommended format.

The "RADIUS Vendor-Specific Attributes" appendix lists the supported vendor-specific options (subtype numbers from 3 through 21) using IETF RADIUS attribute 26 and the Cisco vendor-ID company code of 9.

There are two kinds of off-ramp fax messages:

- Faxes that originate in the PSTN. On entering a packet network, these faxes are converted to TIFF files that are attached to e-mail messages for their transit through the network.
- Faxes that originate from e-mail messages on a PC in the packet network.

Either type can be delivered to a PC on the network before reaching an off-ramp gateway. Upon reaching the off-ramp gateway, however, both types are converted to standard Group 3 fax format for transmission through the PSTN to terminating fax machines.

A basic e-mail operation that store-and-forward fax supports is MDN (return receipt). An MDN is sent to an e-mail originator when the e-mail recipient opens a fax e-mail. MDNs are described in RFC 2298, which also states that e-mail recipients must be able to disable the automatic generation of MDNs.

MDNs are initiated by the sending e-mail client. Return receipts are generated by the receiving e-mail client. Most PC-based e-mail software applications, such as Eudora, Netscape Messenger, and Microsoft Outlook, support MDNs.

Off-ramp security controls who can send outgoing fax messages and is facilitated by AAA security services using either RADIUS or TACACS+. Authentication begins as soon as a fax e-mail message header is received from the e-mail server on the off-ramp gateway. The off-ramp gateway does not dial the destination fax device until authentication for each fax mail is successfully completed.

On-Ramp and Off-Ramp Fax Machines

The transmitting gateway is referred to as an on-ramp gateway, and the terminating gateway is referred to as an off-ramp gateway.

- In on-ramp faxing, either a voice gateway handles incoming calls from a standard fax machine or the PSTN converts a traditional Group 3 fax to an e-mail message with a Tagged Image File Format (TIFF) attachment. The fax e-mail message and attachment are handled by an e-mail server while traversing the packet network and can be stored for later delivery or delivered immediately to a PC or to an off-ramp gateway.

- In off-ramp faxing, either a voice gateway handles calls going out from the network to a fax machine or the PSTN converts a fax e-mail with a TIFF attachment into a traditional fax format that can be delivered to a standard fax machine or the PSTN.

On-ramp and off-ramp faxing processes can be combined on a single gateway, or they can occur on separate gateways. Store-and-forward fax uses two different interactive voice response (IVR) applications for on-ramp and off-ramp functionalities. The applications are implemented in two Tool Command Language (Tcl) scripts that you download from Cisco.com.

The basic functionality of store-and-forward fax is facilitated through SMTP, along with an additional functionality that provides confirmation of delivery using existing SMTP mechanisms, such as ESMTP.

Dial Peer Parameters for T.37 Store-and-Forward Fax

Store-and-forward fax requires you to configure gateway dial peers and specify values for the following types of parameters:

- IVR application parameters and IVR security and accounting parameters--These items load applications on the router and enable authorization and accounting for applications.
- Fax parameters--These items specify the cover sheet and header information that appears on faxes generated in the packet network.
- Mail transfer agent (MTA) parameters--These items define delivery parameters for e-mail messages that accompany fax TIFF images.
- Message disposition notification (MDN) parameters--These items specify the generation of messages to notify e-mail originators of the delivery of their fax e-mail messages.
- Delivery status notification (DSN) parameters--These items instruct the SMTP server to send messages to e-mail originators to inform them of the status of their e-mail messages.
- Gateway security and accounting parameters--These items define authentication, authorization, and accounting (AAA) for faxes that enter or exit the packet network.

Fax calls from the PSTN enter the network through an on-ramp gateway, which is sometimes called an originating gateway. Fax calls exit the packet network to the PSTN through an off-ramp gateway, which is sometimes called a terminating gateway. In small networks, on-ramp and off-ramp functionalities can reside in the same gateway. For store-and-forward fax, each type of gateway is configured with two types of dial peers:

- The on-ramp gateway is configured with one or more plain old telephone system (POTS) dial peers to handle fax calls inbound to the gateway from the public switched telephone network (PSTN) and with one or more multimedia over IP (MMoIP) dial peers to direct calls outbound from the gateway to the network.
- The off-ramp gateway is configured with one or more MMoIP dial peers to handle fax calls inbound from the IP network and with one or more POTS dial peers to direct calls outbound through POTS voice ports to the PSTN.

Note The instructions in this chapter assume that your packet network includes separate gateways for on-ramp and off-ramp functions. For smaller networks that use a single router for both on-ramp and off-ramp functionalities, follow both the on-ramp and off-ramp instructions on the same router.

How to Configure T.37 Store-and-Forward Fax

Downloading the T.37 Store-and-Forward Fax Scripts

You must download the Tcl scripts for the store-and-forward fax application; the scripts are contained in compressed zip files on Cisco.com. Save the downloaded files in a location that the gateway can access. The Cisco IOS File System (IFS) is used to read the files, so you can use any IFS-supported URL for the file location. URLs can include TFTP, FTP, or pointers to a device on the router. For more information, see the Tcl IVR API Version 2.0 Programmer's Guide.

SUMMARY STEPS

1. Log in to the Cisco website and go to http://www.cisco.com/cgi-bin/tablebuild.pl/tclware .
2. Select and download the following zip files which contain the T.37 applications.
3. Unzip the files.
4. Move the application script files to a location that can be accessed by your gateway using a standard URL that points to the location of the script. The following are examples:

DETAILED STEPS

Step 1 Log in to the Cisco website and go to http://www.cisco.com/cgi-bin/tablebuild.pl/tclware .

When you are logged in to the Cisco website, navigate to the TCLWare page from the Cisco home page by following this path: Technical Support / Software Center / Access Software / TCLWare.

Step 2 Select and download the following zip files which contain the T.37 applications.

- app-faxmail-onramp.2.0.1.2.zip (or a later version)
- app-faxmail-offramp.2.0.1.1.zip (or a later version)

When asked, provide the following information:

- The Cisco Connection Online (CCO) server nearest to your physical location
- The location to save the files on your disk

Step 3 Unzip the files.

The zip files that you download include the following files:

- T.37 on-ramp application Tcl script (app-faxmail-onramp.2.0.1.2.tcl or later)
- T.37 off-ramp application Tcl script (app-faxmail-offramp.2.0.1.1.tcl or later)
- README file

Step 4 Move the application script files to a location that can be accessed by your gateway using a standard URL that points to the location of the script. The following are examples:

- flash:myscript.tcl--The script called myscript.tcl is located in Flash memory on the router.
- slot0:myscript.tcl--The script called myscript.tcl is located in a device in slot 0 on the router.

- tftp://BigServer/myscripts/MouseTrap.tcl--The script called MouseTrap.tcl is located in a server called BigServer in a directory within the tftpboot directory called myscripts.

Note Flash memory is limited to 32 entries, which may prevent you from loading all Tcl and audio files there.

Configuring an On-Ramp Gateway for T.37 Store-and-Forward Fax

On-ramp gateway configuration for store-and-forward fax consists of the following tasks:

Note The T.37 store-and-forward fax configuration tasks are the same for H.323 and SIP networks.

Note Starting with Cisco IOS Release 12.3(14)T, the **call application voice configuration** commands were restructured. Configuration commands for Cisco IOS Release 12.3(11)T and earlier are described in the "Fax and Modem Services over IP Overview" module.

Enabling T.37 Store-and-Forward Fax on the On-Ramp Gateway

Perform this task to enable T.37 store-and-forward fax by specifying the following information:

- A fully qualified domain name for the SMTP server
- Name and location of the T.37 application
- Type of T.37 processing to occur on this gateway
- Called subscriber number definition

Before you begin

- The T.37 application that processes fax calls on inbound POTS dial peers is an IVR application that is written in a Tool Command Language (Tcl) script. Download the script from Cisco.com and install it on your network before you load the T.37 application on the gateway (see the How to Configure T.37 Store-and-Forward Fax, on page 119).
- After you have installed the script at a location that is accessible to the gateway, load it using a name of your choice. All later commands that refer to this application use the name that you select when you load the application on the gateway.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip domain-name** *name*
4. **fax interface-type** {**fax-mail** | **modem**}
5. **fax receive called-subscriber** {**d** | *string*}

6. **application**
7. **service** *service-name location*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip domain-name** *name* **Example:** `Router(config)# ip domain-name ABC.com`	Defines a default domain name that the Cisco IOS software uses to complete unqualified hostnames (without dotted-decimal domain names). • *name* --Default domain name used to complete unqualified hostnames. Do not include the initial period that separates an unqualified name from the domain name. **Note** Cisco AS5300 gateways must be reloaded for this command to take effect.
Step 4	**fax interface-type** {**fax-mail** | **modem**} **Example:** `Router(config)# fax interface-type fax-mail`	Enables the T.37 functionality and specifies the type of fax processing. • **fax-mail** --Uses voice cards for the T.37 interface. This is the default for all platforms except the Cisco AS5300 and for Cisco AS5300 gateways with VFC cards only. • **modem** --(Cisco AS5300 only) Uses modem cards for the T.37 interface. This is the default for Cisco AS5300 gateways with modem cards only or with a combination of modem and VFC cards. **Note** If you change the fax interface type with this command, the gateway must be reloaded for the new setting to take effect. **Note** Before Cisco IOS Release 12.2(8)T, this command was **fax interface-type** {**vfc** | **modem**}. The **vfc** keyword was replaced by the **fax-mail** keyword to better represent all platforms.

	Command or Action	Purpose
Step 5	**fax receive called-subscriber** {**d** | *string*} **Example:** `Router(config)# fax receive called-subscriber $d$`	Configures the on-ramp gateway to send the called subscriber identity (CSI) regardless of whether the off-ramp gateway is converting a fax TIFF file to a standard fax or sending an e-mail message as a fax. The CSI is the telephone number associated with the receiving fax device and it typically appears in the LCD of the sending fax device. • **d** --Wildcard that is replaced by the sender name in the To: field in the RFC 822 header. • *string* --Destination telephone number. Valid entries are the plus sign (+), numbers 0 through 9, and the space character. Use a plus sign as the first character to specify an E.164 phone number.
Step 6	**application** **Example:** `Router(config)# application`	Enters application configuration mode to configure voice applications and services.
Step 7	**service** *service-name location* **Example:** `Router(config-app)# service fax_detect flash:app_fax_detect.2.1.2.2.tcl`	Loads a VoiceXML document or Tcl script and defines its application name. • *service-name* --Name that identifies the voice application. This is a user-defined name and does not have to match the script name. • *location* --Directory and filename of the Tcl script or VoiceXML document in URL format. For example, Flash memory (flash:filename), a TFTP (tftp://../filename) or an HTTP server (http://../filename) are valid locations.
Step 8	**end** **Example:** `Router(config-app)# end`	Exits application configuration mode.

Configuring Dial Peers on the On-Ramp Gateway

The purpose for configuring on-ramp gateway dial peers is to allow the router to receive inbound fax traffic from the PSTN and to direct that traffic to the appropriate SMTP server.

This task consists of the following subtasks:

Note For typical network operations, we recommend that you use the default configuration for image resolution/encoding on outbound MMoIP dial peers.

Configuring One or More Inbound POTS Dial Peers

An inbound dial peer on an on-ramp gateway receives fax calls from the PSTN.

The gateway selects an inbound dial peer for a fax call by matching information elements in the call setup message with configured dial peer attributes. Several methods of matching are available, but for store-and-forward fax, we recommend using the **incoming called-number** command, which configures the gateway to use the called number or the Digital Number Identification Service (DNIS) to match a dial peer. This method is recommended because call setups always include DNIS information, and this attribute has matching priority over other methods.

Note To learn about other methods of dial peer matching, see the *Dial Peer Configuration on Voice Gateway Routers* document.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **pots**
4. **service** *service-name*
5. **direct-inward-dial**
6. **incoming called-number** *string*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **pots** **Example:** `Router(config)# dial-peer voice 24 pots`	Enters dial-peer configuration mode and defines a local dial peer that directs traffic to or from a POTS interface. • *tag* --Dial-peer identifier that consists of one or more digits. Valid entries are from 1 to 2147483647. • **pots** --Specifies that this dial peer directs traffic to or from a POTS interface.
Step 4	**service** *service-name* **Example:**	Associates the on-ramp store-and-forward fax application with this dial peer.

	Command or Action	Purpose
	`Router(config-dial-peer)# service onramp-app`	
Step 5	**direct-inward-dial** **Example:** `Router(config-dial-peer)# direct-inward-dial`	Enables the direct inward dial (DID) call treatment for incoming called numbers, in which the entire incoming dial string is used to find a matching outbound dial peer. The gateway does not present a dial tone to the caller and does not collect digits; the setup message contains all the digits necessary to route the call.
Step 6	**incoming called-number** *string* **Example:** `Router(config-dial-peer)# incoming called-number 5105551212`	Defines the called number (dialed number identification service or DNIS) string. The called number is used to match the incoming call leg to an inbound dial peer. • *string* --The incoming called telephone number. Valid entries are any series of digits that specify the E.164 telephone number. **Note** A gateway that is used for both voice calls and inbound T.37 fax calls requires one inbound POTS dial peer for voice calls (without the application command) and one inbound POTS dial peer for T.37 fax calls (with the application command).
Step 7	**end** **Example:** `Router(config-dial-peer)# end`	Exits dial-peer configuration mode.

Configuring One or More Outbound MMoIP Dial Peers

The outbound MMoIP dial peer on an on-ramp gateway directs fax traffic through the IP network to an SMTP server.

Note For typical network operations, we recommend that you use the default configuration for image resolution/encoding on outbound MMoIP dial peers. You should only configure additional outbound MMoIP dial peers for troubleshooting or when you need to force a dial peer into a specific resolution/encoding while receiving a fax. Changing this configuration might cause fax negotiation failure.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **mmoip**
4. **service fax_on_vfc_onramp_app out-bound**
5. **destination-pattern** [+]*string*[**T**]

6. **information-type fax**
7. **session protocol smtp**
8. **session target** {**mailto**:{*host-name* | **d** | **m**}*@domain-name*| **ipv4:** *destination-address* | **dns:**{**d.**| **e.** | **s.** | **u.**}*host-name*}
9. **image encoding** {**mh** | **mr** | **mmr** | **passthrough**}
10. **image resolution** {**fine** | **standard** | **super-fine** | **passthrough**}
11. **max-conn** *number*
12. **dsn** {**delay** | **failure** | **success**}
13. **mdn**
14. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **mmoip** **Example:** `Router(config)# dial-peer voice 17 mmoip`	Enters dial-peer configuration mode and defines a local dial peer that directs traffic to or from an SMTP server. • *tag* --Dial-peer identifier that consists of one or more digits. Valid entries are from 1 to 2147483647. • **mmoip** --Specifies that this dial peer conducts traffic to or from an SMTP server.
Step 4	**service fax_on_vfc_onramp_app out-bound** **Example:** `Router(config-dial-peer)# service fax_on_vfc_onramp_app out-bound`	Names the IVR application to which calls from this dial peer are handed off. • **fax_on_vfc_onramp_app** --Name of the T.37 IVR application that handles calls on MMoIP dial peers. • **out-bound** --Instructs the application that the calls it handles are outbound from the dial peer. **Note** This application name must be typed exactly as it appears here; you cannot abbreviate it as you can do with other Cisco IOS command keywords.

	Command or Action	Purpose
		Note You must use the **fax interface-type fax-mail** command and reload the router to make the fax_on_vfc_onramp_app script available. See the Enabling T.37 Store-and-Forward Fax on the On-Ramp Gateway, on page 120.

Step 5	**destination-pattern** [+]*string*[**T**]
	Example:
	`Router(config-dial-peer)# destination-pattern 14085554321`
		Specifies a pattern that represents either the prefix or the full E.164 telephone number (depending on your dial plan) that identifies the destination store-and-forward fax telephone number on this dial peer. This pattern of numbers should fall within the pattern of numbers that was configured as the incoming called number on the inbound POTS dial peer.
		• + --(Optional) Plus sign indicates that an E.164 standard number follows. The plus sign (+) is not supported on the Cisco MC3810.
		• *string* --E.164 or private dialing plan telephone number. Valid entries are digits 0 through 9, letters A through D, and the following special characters:
		  • Asterisk (*) and pound sign (#) that appear on standard touch-tone dial pads. These characters cannot be used as leading characters in a string (for example, *650).
		  • Comma (,), which inserts a pause between digits.
		  • Period (.), which matches any entered digit (this character is used as a wildcard). The period cannot be used as a leading character in a string (for example, .650).
		• **T** --(Optional) Timer, or control, character that indicates that the destination-pattern value is a variable-length dial string. This instructs the router to collect dialed digits until the interdigit timer expires (10 seconds, by default) or until the termination character (#, by default) is dialed. The timer character must be a capital T.

Step 6	**information-type fax** **Example:** `Router(config-dial-peer)# information-type fax`	Identifies calls associated with this dial peer as being fax transmissions, and not voice calls.
Step 7	**session protocol smtp** **Example:** `Router(config-dial-peer)# session protocol smtp`	Specifies the session protocol for calls between the on-ramp gateway and the remote mail server as SMTP.

	Command or Action	Purpose
Step 8	**session target** {**mailto**:{*host-name* | **d** | **m**}*@domain-name*| **ipv4:** *destination-address* | **dns:**{**d.**| **e.** | **s.** | **u.**}*host-name*} **Example:** `Router(config-dial-peer)# session target mailto:$d$@abccompany.com`	Designates a network-specific address to receive calls from this dial peer (the SMTP server). • **mailto:** --Indicates that the argument that follows is an e-mail address. • **ipv4:** -- Indicates that the argument that follows is an IP address. • **dns:** --Indicates that the argument that follows is a router hostname to be resolved by the domain name server. • *host-name* --String that contains the hostname of the network-specific address to receive calls from this dial peer. • *@domain-name* --String that contains the domain name to be associated with the target address, preceded by the at sign (@); for example, @mycompany.com. • *destination-address* --String that contains the IP address of the network-specific address to receive calls from this dial peer. • **d.** --Wildcard that is replaced by the destination (called) number, followed by a period (.). • **e.** --Wildcard that is replaced by the digits in the called number in reverse order with periods added between the digits, followed by a period (.). • **m.** --Wildcard that is replaced by the redirecting dialed number (RDNIS) if present; otherwise, it is replaced by the gateway access number (dialed number, or DNIS), followed by a period (.). This wildcard is used only with the Fax Detection application. • **s.** --Wildcard that is replaced by the source destination pattern, followed by a period (.). • **u.** --Wildcard that is replaced by the unmatched portion of the destination pattern (such as a defined extension number), followed by a period (.).
Step 9	**image encoding** {**mh** | **mr** | **mmr** | **passthrough**} **Example:** `Router(config-dial-peer)# image encoding mh`	(Optional) Selects a specific encoding method for the fax TIFF images that are forwarded using this dial peer. • **mh** --Specifies Modified Huffman image encoding. This is the IETF standard. • **mr** --Specifies Modified Read image encoding.

	Command or Action	Purpose
		• **mmr** --Specifies Modified Modified Read image encoding. • **passthrough** --Specifies that the image is not to be modified by an encoding method. This is the default.
Step 10	**image resolution** {**fine** | **standard** | **super-fine** | **passthrough**} **Example:** `Router(config-dial-peer)# image resolution fine`	(Optional) Selects a specific resolution for the fax TIFF images that are forwarded using this dial peer. • **fine** --Fax TIFF image resolution is 204-by-196 pixels per inch. • **standard** --Fax TIFF image resolution is 204-by-98 pixels per inch. • **super-fine** --Fax TIFF image resolution is 204-by-391 pixels per inch. • **passthrough** --Resolution of the fax TIFF image is not to be altered. This is the default.
Step 11	**max-conn** *number* **Example:** `Router(config-dial-peer)# max-conn 248`	(Optional) Specifies the maximum number of simultaneous connections that are allowed to and from this dial peer. • *number* --Number of simultaneous connections. Ranges from 1 to 2147483647. Default: the **no** form of this command, meaning that an unlimited number of connections is permitted.
Step 12	**dsn** {**delay** | **failure** | **success**} **Example:** `Router(config-dial-peer)# dsn failure`	(Optional) Requests delivery status notification of e-mail with fax TIFF images to be sent to the address specified by the **mta send mail-from** command (the FROM address). DSN must be supported by the remote mail server. • **delay** --Requests the next-hop mailer to notify the FROM address if a mail message is delayed. Each mailer in the path to the recipient that supports the DSN extension receives the same request. • **failure** --Requests the next-hop mailer to notify the FROM address if the mail message is not delivered. Each mailer in the path to the recipient that supports the DSN extension receives the same request. • **success** --Requests the next-hop mailer to notify the FROM address if the mail message is successfully delivered. Each mailer in the path to the recipient that supports the DSN extension receives the same request. The default is **failure** and **success**.

	Command or Action	Purpose
		Note Select more than one notification option by reissuing the command. To discontinue a specific notification option, use the **no** form of the command for that specific keyword. **Note** In the absence of any other DSN settings (either **no dsn** or a mailer in the path that does not support the DSN extension), a failure to deliver always generates a nondelivery message, which is called a bounce.
Step 13	**mdn** **Example:** `Router(config-dial-peer)# mdn`	(Optional) Requests generation of an MDN by the mail user agent when the e-mail is processed (typically opened or read). The MDN is generated by the receiving mail user agent and sent to the address defined by the **mta send return-receipt-to** command. The return receipt must be supported and initiated by the receiving e-mail client.
Step 14	**end** **Example:** `Router(config-dial-peer)# end`	Exits dial-peer configuration mode.

Configuring MTA Parameters on the On-Ramp Gateway

Perform this task to configure parameter values associated with the MTA on the on-ramp gateway.

Note The **mta send mail-from username** and **mta send mail-from hostname** commands define the From: username. The To: address is defined using the **session target** command on the on-ramp gateway MMoIP dial peer.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mta send server** {*host-name* | *ip-address*[**port** *port-number*]}
4. **mta send postmaster** *e-mail-address*
5. **mta send mail-from hostname** *string*
6. **mta send mail-from username** {*string* | **s**}
7. **mta send subject** *string*
8. **mta send origin-prefix** *string*
9. **mta send return-receipt-to** {**hostname** *string*| **username** *string*| **username s**}
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**mta send server** {*host-name* | *ip-address*[**port** *port-number*]} **Example:** `Router(config)# mta send server california.fax.com`	Specifies a destination server. This command can be repeated to define up to ten mail servers for backup purposes. DNS mail exchange (MX) records are not used to look up the hostnames provided to this command. • *host-name* --String that contains the name of the destination e-mail server. • *ip-address* --String that contains the IP address of the destination e-mail server. • **port** *port-number* --(Optional) Keyword-argument pair that designates a particular port for the e-mail server. The default is 25. **Note** When using this command, configure the gateway to perform name lookups using the **ip name-server** command.
Step 4	**mta send postmaster** *e-mail-address* **Example:** `Router(config)# mta send postmaster mailtop@mail23.abcorp.com`	Identifies where an e-mail message should be delivered (the mail server postmaster account) if the evaluated string from the **mta send mail-from** command or the Simple Mail Transfer Protocol (SMTP) server is blank. • *e-mail-address* --Character string that defines the address to which an undeliverable e-mail should be diverted (the mail server postmaster account).
Step 5	**mta send mail-from hostname** *string* **Example:** `Router(config)# mta send mail-from hostname newyork.fax.com`	Specifies the originator (host-name portion) of the e-mail fax message. This information appears in the RFC 822 From: field and the RFC 821 MAIL FROM field of the e-mail fax message. This information is also used for generating delivery status notifications (DSNs). When the **mta send mail-from hostname** command is configured, the configured hostname is used with the **mta send mail-from username** command to form a complete e-mail address, such as faxuser@onramp-gateway.com.

	Command or Action	Purpose
		• *string* --Character string that specifies the SMTP hostname or IP address of the e-mail originator. If you specify an IP address, you must enclose the IP address in brackets as follows: [xxx.xxx.xxx.xxx].
Step 6	**mta send mail-from username** {*string* | **s**} **Example:** `Router(config)# mta send mail-from username $s$`	(Optional) Specifies the originator (username portion) of the e-mail fax message. This information appears in the RFC 822 From: field and the RFC 821 MAIL FROM field of the e-mail fax message. This information is also used for generating DSNs. When the **mta send mail-from hostname** command is configured, the configured hostname is used with the **mta send mail-from username** command to form a complete e-mail address, such as faxuser@onramp-gateway.com. • *string* --Character string that specifies the user name of the e-mail originator. • **s** --Wildcard that specifies that the username is to be derived from the calling number. When the **s** keyword is used, a transmission report is sent to the originating fax machine.
Step 7	**mta send subject** *string* **Example:** `Router(config)# mta send subject "mail from joe"`	(Optional) Defines the text that appears in the Subject field of the e-mail message. • *string* --Character string that specifies the subject header of an e-mail message.
Step 8	**mta send origin-prefix** *string* **Example:** `Router(config)# mta send origin-prefix "Cisco-powered Fax System"`	(Optional) Defines additional identifying information to be prepended to the e-mail prefix header. • *string* --Character string to be added to the beginning of an e-mail prefix header. If the string contains spaces, the string value should be enclosed within quotation marks ("abc xyz").
Step 9	**mta send return-receipt-to** {**hostname** *string*| **username** *string*| **username s**} **Example:** `Router(config)# mta send return-receipt-to username $s$`	(Optional) Specifies the address to which message disposition notifications (MDNs) are sent. • **hostname** *string* --Text string that specifies the Simple Mail Transfer Protocol (SMTP) hostname or IP address to which MDNs are sent. If you specify an IP address, you must enclose the IP address in brackets as follows: [xxx.xxx.xxx.xxx]. • **username** *string* --Text string that specifies the sender username to which MDNs are sent. • **username s** --Wildcard that specifies that the username is derived from the calling number.

	Command or Action	Purpose
		Note To generate return receipts in off-ramp fax-mail messages, enable MDN in the MMoIP dial peer, as described in the Configuring One or More Outbound MMoIP Dial Peers, on page 124.
Step 10	**end** **Example:** `Router(config)# end`	Exits global configuration mode.

Configuring DSNs on the On-Ramp Gateway

The **dsn** command allows you to enable or disable the generation of DSNs for each state by reissuing the command and specifying a different notification option each time. To discontinue a specific notification option, use the **no** form of the command for that specific keyword.

For fax calls received at an on-ramp gateway, requests for DSNs are included as part of the fax-mail messages sent by the on-ramp gateway. DSN requests are generated only when the MMoIP dial peer that matches the fax call has been configured to enable DSNs (see the Configuring One or More Outbound MMoIP Dial Peers, on page 124).

DSNs are delivered to the sender that is defined in the **mta send mail-from** command.

Note The following steps are also used in other tasks, but they are repeated here to show the complete set of steps that are used to generate DSNs.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mta send mail-from hostname** *string*
4. **mta send mail-from username** {*string* | **s**}
5. **dial-peer voice** *tag* **mmoip**
6. **dsn** {**delayed**| **failure** | **success**}
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**mta send mail-from hostname** *string* **Example:** `Router(config)# mta send mail-from hostname newyork.fax.com`	See the Configuring MTA Parameters on the On-Ramp Gateway, on page 129.
Step 4	**mta send mail-from username** {*string* | **s**} **Example:** `Router(config)# mta send mail-from username $s$`	See the Configuring MTA Parameters on the On-Ramp Gateway, on page 129.
Step 5	**dial-peer voice** *tag* **mmoip** **Example:** `Router(config)# dial-peer voice 24 mmoip`	Enters dial-peer configuration mode for the MMoIP dial peer. See the Configuring One or More Outbound MMoIP Dial Peers, on page 124.
Step 6	**dsn** {**delayed**| **failure** | **success**} **Example:** `Router(config-dial-peer)# dsn failure`	See the Configuring One or More Outbound MMoIP Dial Peers, on page 124.
Step 7	**end** **Example:** `Router(config -dial-peer) # end`	Exits dial-peer configuration mode.

Configuring Security and Accounting on the On-Ramp Gateway

Perform this task to configure security and accounting on the on-ramp gatway.

Note Steps 10 through 13 do not apply to Cisco AS5300 gateways with modem cards.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login fax radius**

5. **aaa accounting connection fax start-stop group radius**
6. **radius-server host** *ip-address* **auth-port** *number* **acct-port** *number*
7. **radius-server key** {**0** *string* | **7** *hidden-string*| *string*}
8. **radius-server vsa send accounting**
9. **radius-server vsa send authentication**
10. **mmoip aaa method fax authentication** *method-list-name*
11. **mmoip aaa receive-authentication enable**
12. **mmoip aaa method fax accounting** *method-list-name*
13. **mmoip aaa receive-accounting enable**
14. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables AAA security and accounting services.
Step 4	**aaa authentication login fax radius** **Example:** `Router(config)# aaa authentication login fax radius`	Defines a method list called fax in which RADIUS is defined as the only method of login authentication. **Note** The method list name (fax) must match the name used in the Configuring T.37 IVR Application Security and Accounting, on page 136.
Step 5	**aaa accounting connection fax start-stop group radius** **Example:** `Router(config)# aaa accounting connection fax start-stop group radius`	Defines the accounting method list called fax with RADIUS as a method and with an option to send both start and stop accounting records to the AAA server. **Note** The method list name (fax) must match the name used in Configuring T.37 IVR Application Security and Accounting, on page 136.
Step 6	**radius-server host** *ip-address* **auth-port** *number* **acct-port** *number* **Example:**	Identifies the RADIUS server and the ports that are used for authentication and accounting services. You can use multiple **radius-server host** commands to specify multiple

	Command or Action	Purpose
	`Router(config)# radius-server host 10.168.23.24 auth-port 1812 acct-port 1813`	hosts. The software searches for hosts in the order in which you specify them. • *ip-address* --IP address of the RADIUS server host. • *number* --Port number for authentication or accounting requests. If set to 0, the host is not used. If unspecified for authentication, the port number defaults to 1645. If unspecified for accounting, the port number defaults to 1646.
Step 7	**radius-server key** {**0** *string* | **7** *hidden-string*| *string*} **Example:** `Router(config)# radius-server key 0 3hd905kdh`	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon on the server. • **0** --Unencrypted (clear-text) shared key follows. • **7** --Hidden shared key follows. • *hidden-string* --Hidden shared key. • *string* --Unencrypted (clear-text) shared key.
Step 8	**radius-server vsa send accounting** **Example:** `Router(config)# radius-server vsa send accounting`	Enables the network access server to recognize and use accounting vendor-specific attributes (VSAs) as defined by RADIUS Internet Engineering Task Force (IETF) attribute 26. VSAs allow vendors to support their own extended attributes not suitable for general use.
Step 9	**radius-server vsa send authentication** **Example:** `Router(config)# radius-server vsa send authentication`	Enables the network access server to recognize and use authentication VSAs as defined by RADIUS IETF attribute 26.
Step 10	**mmoip aaa method fax authentication** *method-list-name* **Example:** `Router(config)# mmoip aaa method fax authentication fax`	Defines the name of the method list to be used for store-and-forward fax AAA authentication. The method list, which defines the type of authentication services provided for store-and-forward fax, is itself defined using the **aaa authentication** global configuration command. Unlike standard AAA (in which each defined method list can be applied to specific interfaces and lines), the AAA authentication method lists used in store-and-forward fax are applied globally on the gateway. • *method-list-name* --Character string that names a list of authentication methods to be used with store-and-forward fax.
Step 11	**mmoip aaa receive-authentication enable** **Example:**	Enables AAA authentication services if an AAA authentication method list has been defined using both the

	Command or Action	Purpose
	`Router(config)# mmoip aaa receive-authentication enable`	**aaa authentication** command and the **mmoip aaa method fax authentication** command.
Step 12	**mmoip aaa method fax accounting** *method-list-name* **Example:** `Router(config)# mmoip aaa method fax accounting fax`	Defines the name of the method list to be used for store-and-forward fax AAA accounting. The method list, which defines the type of accounting services provided for store-and-forward fax, is itself defined using the **aaa accounting** global configuration command. Unlike standard AAA (in which each defined method list can be applied to specific interfaces and lines), the AAA accounting method lists used in store-and-forward fax are applied globally on the gateway. • *method-list-name* --Character string that names a list of accounting methods to be used with store-and-forward fax.
Step 13	**mmoip aaa receive-accounting enable** **Example:** `Router(config)# mmoip aaa receive-accounting enable`	Enables on-ramp AAA accounting service if an AAA accounting method list has been defined using both the **aaa accounting** command and the **mmoip aaa method fax accounting** command.
Step 14	**end** **Example:** `Router(config)# end`	Exits global configuration mode.

Configuring T.37 IVR Application Security and Accounting

Perform this task to configure the specified T.37 IVR application to perform authentication and accounting tasks in conjunction with a RADIUS server.

Note The commands in this section configure an IVR application, and they are not supported by Cisco IOS help. For example, if you type **param accounting-list ?**, the Cisco IOS software does not supply a list of entries that are valid in place of the question mark because the IVR application commands pass parameters to the named Tcl script, rather than to the Cisco IOS software.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **application**
4. **service** *service-name location*
5. **param accounting enable**
6. **param accounting-list** *method-list-name*

7. **param authentication enable**
8. **param authen-list** *method-list-name*
9. **param authen-method** {**prompt-user** | **ani** | **dnis** | **gateway** | **redialer-id** | **redialer-dnis**}
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**application** **Example:** `Router(config)# application`	Enters application configuration mode to configure voice applications and services.
Step 4	**service** *service-name location* **Example:** `Router(config-app)# service fax_detect flash:app_fax_detect.2.1.2.2.tcl`	Loads a VoiceXML document or Tcl script and defines its application name. • *service-name* --Name that identifies the voice application. This is a user-defined name and does not have to match the script name. • *location* --Directory and filename of the Tcl script or VoiceXML document in URL format. For example, Flash memory (flash:filename), a TFTP (tftp://../filename) or an HTTP server (http://../filename) are valid locations.
Step 5	**param accounting enable** **Example:** `Router(config-app)# param accounting enable`	Enables AAA accounting for a Tcl application.
Step 6	**param accounting-list** *method-list-name* **Example:** `Router(config-app)# param accounting-list fax`	Defines the name of the accounting method list to be used for AAA with store-and-forward fax on a voice feature card (VFC). • *method-list-name* --Character string used to name a list of accounting methods to be used with store-and-forward fax.

	Command or Action	Purpose
		Note The method list name should match the name used in the Configuring Security and Accounting on the On-Ramp Gateway, on page 133.
Step 7	**param authentication enable** **Example:** `Router(config-app)# param authentication enable`	Enables AAA authentication for a Tcl application.
Step 8	**param authen-list** *method-list-name* **Example:** `Router(config-app)# param authen-list fax`	Specifies the name of an authentication method list for a Tcl application. • *method-list-name* --Character string used to name a list of authentication methods to be used with store-and-forward fax. **Note** The method list name should match the name used in the Configuring Security and Accounting on the On-Ramp Gateway, on page 133.
Step 9	**param authen-method** {**prompt-user** | **ani** | **dnis** | **gateway** | **redialer-id** | **redialer-dnis**} **Example:** `Router(config-app)# param authen-method ani`	Specifies the type of authentication method for the named application. • **prompt-user** --The user is prompted for the Tcl application account identifier. • **ani** --The calling-party telephone number (automatic number identification [ANI]) is used as the Tcl application account identifier. • **dnis** --The called party telephone number (dialed number identification service [DNIS]) is used as the Tcl application account identifier. • **gateway** --The router-specific name derived from the hostname and domain name is used as the Tcl application account identifier. It is displayed in the following format: router-name.domain-name. • **redialer-id** --The account string returned by the external redialer device is used as the Tcl application account identifier. In this case, the redialer ID is either the redialer serial number or the redialer account number. • **redialer-dnis** --The called party telephone number (DNIS) is used as the Tcl application account identifier captured by the redialer if a redialer device is present.

	Command or Action	Purpose
Step 10	**end** **Example:** `Router(config)# end`	Exits application configuration mode.

How to Configure an Off-Ramp Gateway for T.37 Store-and-Forward Fax

The purpose of an off-ramp gateway in store-and-forward fax is to receive fax e-mail messages and TIFF attachments from the packet network and transmit them to the PSTN for delivery to terminating fax machines.

The off-ramp gateway performs the following actions:

- Converts a TIFF file or fax e-mail to a standard Group 3 fax message. During off-ramp faxing, the gateway uses the receiving MTA and dial peers to convert a fax-mail TIFF file or plain text file into a standard fax format and then delivers it as a standard fax transmission.
- Appends headers and cover pages only for fax plain-text e-mail messages, as described in the Configuring Fax Headers and Cover Pages on the Off-Ramp Gateway, on page 146.
- Forwards fax messages to voice ports that interface with the PSTN, as configured in the dial peers.

Various aspects of the off-ramp gateway must be configured to enable the preceding actions. The off-ramp gateway uses dial peers to route calls to appropriate POTS voice ports. An IVR application handles the conversion of fax messages. In addition, you can configure the gateway to request notifications when the fax messages are delivered. AAA security and accounting are also important for off-ramp fax services.

The off-ramp gateway configuration for store-and-forward fax consists of the following tasks:

Note Starting with Cisco IOS Release 12.3(14)T, the **call application voice** configuration commands were restructured. This application guide uses the new command structure.

Enabling T.37 Store-and-Forward Fax on the Off-Ramp Gateway

Perform this task to enable T.37 store-and-forward fax by specifying the following information:

- A fully qualified domain name for the SMTP server
- The name and location of the T.37 application
- The type of T.37 processing to occur on this gateway
- Transmitting-subscriber number definition

Before you begin

This section describes prerequisites for enabling T.37 store-and-forward fax on the off-ramp gateway.

- The T.37 application that processes fax calls on inbound MMoIP dial peers is an IVR application written in a Tcl script. Download the script from Cisco.com and install it on your network before you load the T.37 application on the gateway (see the How to Configure T.37 Store-and-Forward Fax, on page 119).

- After you have installed the script at a location that is accessible to the gateway, load it using a name of your choice. All later commands that refer to this application will use the name that you select when you load the application on the gateway.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip domain-name** *name*
4. **fax interface-type** {**fax-mail** | **modem**}
5. **fax send transmitting-subscriber** {**s**| *string*}
6. **service**
7. **service** *service-name location*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip domain-name** *name* **Example:** `Router(config)# ip domain-name ABC.com`	Defines a default domain name that the Cisco IOS software uses to complete unqualified hostnames (without dotted-decimal domain names). • *name* --Default domain name used to complete unqualified hostnames. Do not include the initial period that separates an unqualified name from the domain name. **Note** Cisco AS5300 gateways must be reloaded for this command to take effect.
Step 4	**fax interface-type** {**fax-mail**	**modem**} **Example:** `Router(config)# fax interface-type fax-mail`	Enables T.37 functionality and specifies the type of fax processing. • **fax-mail** --Uses voice cards for the T.37 interface. This is the default for all platforms except the Cisco AS5300 and for Cisco AS5300 gateways with VFC cards only. • **modem** --(Cisco AS5300 only) Uses modem cards for the T.37 interface. This is the default for Cisco AS5300

	Command or Action	Purpose
		gateways with modem cards only or with a combination of modem and VFC cards. **Note** If you change the fax interface type with this command, the gateway must be reloaded in order for the new setting to take effect. **Note** Before Cisco IOS Release 12.2(8)T, this command was **fax interface-type** {**vfc** | **modem**}. The **vfc** keyword was replaced by the **fax-mail** keyword to better represent all platforms.
Step 5	**fax send transmitting-subscriber** {**s**| *string*} **Example:** `Router(config)# fax send transmitting-subscriber $s$`	Configures the on-ramp gateway to send the transmitting subscriber number (TSI) regardless of whether the off-ramp gateway is converting a fax TIFF file to a standard fax or sending an e-mail message as a fax. The TSI is the telephone number associated with the transmitting, or sending, fax device and it typically appears in the LCD of the receiving fax device. • **s** --Wildcard that is replaced by the name in the From: field in the RFC 822 header. • *string* --Destination telephone number. Valid entries are the plus sign (+), numbers 0 through 9, and the space character. To specify an E.164 phone number, use a plus sign (+) as the first character.
Step 6	**service** **Example:** `Router(config)# service`	Specifies the configuration mode to enter voice applications and services.
Step 7	**service** *service-name location* **Example:** `Router(config-app)# service fax_detect flash:app_fax_detect.2.1.2.2.tcl`	Loads a VoiceXML document or Tcl script and defines its application name. • *service-name* --Name that identifies the voice application. This is a user-defined name and does not have to match the script name. • *location* --Directory and filename of the Tcl script or VoiceXML document in URL format. For example, Flash memory (flash:filename), a TFTP (tftp://../filename) or an HTTP server (http://../filename) are valid locations.
Step 8	**end** **Example:**	Exits application configuration mode.

	Command or Action	Purpose
	`Router(config)# end`	

Configuring Dial Peers on the Off-Ramp Gateway

The purpose for configuring off-ramp gateway dial peers is to allow the router to receive inbound fax traffic from an SMTP server in the packet network and to direct that traffic to voice ports that interface with the PSTN.

This task consists of the following subtasks:

Configuring One or More Inbound MMoIP Dial Peers

The inbound MMoIP dial peer on an off-ramp gateway receives fax traffic from an SMTP server in the packet network. Perform this task to configure inbound MMoIP dial peers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **mmoip**
4. **application** *application-name*
5. **incoming called-number** *string*
6. **information-type fax**
7. **image encoding** {**mh** | **mr** | **mmr** | **passthrough**}
8. **image resolution** {**fine** | **standard** | **super-fine** | **passthrough**}
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **mmoip** **Example:** `Router(config)# dial-peer voice 29 mmoip`	Enters dial-peer configuration mode and defines a local dial peer that directs traffic to or from an SMTP server. • *tag* --Dial-peer identifier consisting of one or more digits. The range is from 1 to 2147483647. • **mmoip** --Specifies that this dial peer conducts traffic to or from an SMTP server.

	Command or Action	Purpose
Step 4	**application** *application-name* **Example:** `Router(config-dial-peer)# application offramp-app`	Names the IVR application to which calls from this dial peer are handed off.
Step 5	**incoming called-number** *string* **Example:** `Router(config-dial-peer)# incoming called-number 14085552345`	Defines the dialed number identification service (DNIS) string, or called fax telephone number. The called number is used to match the incoming call leg to an inbound dial peer. • *string* --Specifies the incoming called telephone number. Valid entries are any series of digits that specify the E.164 telephone number.
Step 6	**information-type fax** **Example:** `Router(config-dial-peer)# information-type fax`	Identifies calls associated with this dial peer as being fax transmissions, not voice calls.
Step 7	**image encoding** {**mh** | **mr** | **mmr** | **passthrough**} **Example:** `Router(config-dial-peer)# image encoding mh`	(Optional) Selects a specific encoding method for the fax TIFF images that are handled by this dial peer. • **mh** --Modified Huffman image encoding (IETF standard). • **mr** --Modified Read image encoding. • **mmr** --Modified Modified Read image encoding. • **passthrough** --Existing image is not modified. This is the default.
Step 8	**image resolution** {**fine** | **standard** | **super-fine** | **passthrough**} **Example:** `Router(config-dial-peer)# image resolution standard`	(Optional) Selects a specific resolution for the fax TIFF images that are handled by this dial peer. • **fine** --204-by-196 pixels per inch. • **standard** --204-by-98 pixels per inch. • **super-fine** --204-by-391 pixels per inch. • **passthrough** --Existing resolution is not altered. This is the default.
Step 9	**end** **Example:** `Router(config-dial-peer)# end`	Exits dial-peer configuration mode.

Configuring One or More Outbound POTS Dial Peers

The outbound POTS dial peer on an off-ramp gateway directs fax calls to a POTS interface. Perform this task to configure outbound POTS dial peers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **pots**
4. **destination-pattern** [+]*string*[**T**]
5. **port** *voice-port*
6. **prefix** *string*
7. **max-conn** *number*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **pots** **Example:** `Router(config)# dial-peer voice 54 pots`	Enters dial-peer configuration mode and defines a local dial peer that directs traffic to or from a POTS interface. • *tag* --Dial-peer identifier that consists of one or more digits. Valid entries are from 1 to 2147483647. • **pots** --Specifies that this dial peer directs traffic to or from a POTS interface.
Step 4	**destination-pattern** [+]*string*[**T**] **Example:** `Router(config-dial-peer)# destination-pattern 15175550119`	Identifies the E.164 or private dialing plan telephone number associated with this dial peer. For outbound dial peers, the destination-pattern string is matched against the called number (DNIS string). • + --(Optional) Plus sign, indicating that an E.164 standard number follows. The plus sign (+) is not supported on the Cisco MC3810. • *string* --E.164 or private dialing plan telephone number. Valid entries are digits 0 through 9, letters A through D, and the following special characters:

	Command or Action	Purpose
		• Asterisk (*) and pound sign (#) that appear on standard touch-tone dial pads. These characters cannot be used as leading characters in a string (for example, *650). • Comma (,), which inserts a pause between digits. • Period (.), which matches any entered digit (this character is used as a wildcard). The period cannot be used as a leading character in a string (for example, .650). • **T** --(Optional) Timer, or control, character that indicates that the destination-pattern value is a variable-length dial string. Instructs the router to collect dialed digits until the interdigit timer expires (10 seconds, by default) or until the termination character (#, by default) is dialed. The timer character must be a capital T.
Step 5	**port** *voice-port* **Example:** `Router(config-dial-peer)# port 1/0/1`	Maps the dial peer to a specific logical voice-port interface. • *voice-port* --Voice port to which traffic from this dial peer should be routed. Voice-port identifiers are platform-specific.
Step 6	**prefix** *string* **Example:** `Router(config-dial-peer)# prefix 9,`	(Optional) Specifies the prefix of the dialed digits associated with this dial peer. If you configure a prefix, when an outgoing call is initiated, the prefix string value is added to the telephone interface first, before the telephone number configured for this dial peer. • *string* --Characters that represent the prefix of the telephone number associated with the specified dial peer. Valid characters are 0 through 9, and comma (,). Use a comma to include a pause in the prefix.
Step 7	**max-conn** *number* **Example:** `Router(config-dial-peer)# max-conn 48`	(Optional) Specifies the maximum number of simultaneous connections that are allowed to and from this dial peer. • *number* --Number of simultaneous connections. The range is from 1 to 2147483647. The default is the **no** form of this command, which means that an unlimited number of connections is permitted.
Step 8	**end** **Example:** `Router(config)# end`	Exits dial-peer configuration mode.

Configuring Fax Headers and Cover Pages on the Off-Ramp Gateway

The purpose of this task is to create headers and cover pages for fax messages that originate from plain-text e-mail messages. This task does not apply to fax TIFF files because headers and cover pages are generated by the originating fax machines and also because the off-ramp gateway does not alter TIFF files when converting them.

This task consists of the following two subtasks:

Configuring Fax Header Parameters

For faxes in plain-text e-mails that originate in the packet network, the off-ramp gateway can append header information to the top of each faxed cover and text page.

Note Because the off-ramp gateway does not alter fax TIFF attachments, fax headers cannot be configured for faxes that are being converted from TIFF files to standard fax transmissions.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **fax send center-header** {**a** | **d** | **p** | **s** | **t** | *string*}
4. **fax send right-header** {**a** | **d** | **p** | **s** | **t** | *string*}
5. **fax send left-header** {**a** | **d** | **p** | **s** | **t** | *string*}
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**fax send center-header** {**a** | **d** | **p** | **s** | **t** | *string*} **Example:** `Router(config)# fax send center-header $d$`	Specifies the header information to be displayed in the center position. • **a** --Date. • **d** --Destination address. • **p** --Page count. • **s** --Sender address.

	Command or Action	Purpose
		• **t** --Transmission time. • *string* --Combination of text and tokens.
Step 4	**fax send right-header** {**a** | **d** | **p** | **s** | **t** | *string*} **Example:** `Router(config)# fax send right-header $t$`	Specifies the header information to be displayed on the right. • **a** --Date. • **d** --Destination address. • **p** --Page count. • **s** --Sender address. • **t** --Transmission time. • *string* --Combination of text and tokens.
Step 5	**fax send left-header** {**a** | **d** | **p** | **s** | **t** | *string*} **Example:** `Router(config)# fax send left-header $a$`	Specifies the header information to be displayed on the left. • **a** --Date. • **d** --Destination address. • **p** --Page count. • **s** --Sender address. • **t** --Transmission time. • *string* --Combination of text and tokens.
Step 6	**end** **Example:** `Router(config)# end`	Exits global configuration mode.

Configuring Fax Cover Page Parameters

For faxes from plain-text e-mail messages that originate in the packet network, the off-ramp gateway can create fax cover pages.

Note Because the off-ramp gateway does not alter fax TIFF attachments, cover pages cannot be configured for faxes that are being converted from TIFF files to standard fax transmissions.

The table below contains examples of entries in the e-mail To: field to control the generation of fax cover pages and explains how these entries relate to the **fax send coverpage enable** command.

Table 6: Sample To: Field Descriptions for Fax Cover Pages

To: Field Entry in Fax E-Mail Message	Description
`FAX=+1-312-555-0119@fax.com`	Fax sent to an E.164-compliant long distance telephone number in the United States. If the **fax send coverpage enable** command has been configured, store-and-forward fax generates a fax cover page.
`FAX=+1-312-555-0119/cover=no@fax.com`	Fax sent to an E.164-compliant long distance telephone number in the United States. In this example, the **fax send coverpage enable** command is superseded by the cover=no statement. No cover page is generated.
`FAX=+1-312-555-0119/cover=yes@fax.com`	Fax sent to an E.164-compliant long distance telephone number in the United States. In this example, the **fax send coverpage enable** command is superseded by the cover=yes statement. Store-and-forward fax generates a fax cover page.
`FAX=+49-515-555-0119@faxgateway.com`	Fax sent to an E.164-compliant long distance telephone number in Germany.
`FAX=+61-2-555-0119@fax.host.com`	Fax sent to an E.164-compliant long distance telephone number in Australia.
`FAX=+33-65-555-0119@fax.com`	Fax sent to an E.164-compliant long distance telephone number in France.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **fax send coverpage enable**
4. **fax send coverpage comment** *string*
5. **fax send coverpage show-detail**
6. **fax send coverpage email-controllable**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**fax send coverpage enable** **Example:** `Router(config)# fax send coverpage enable`	Enables the off-ramp gateway to send cover sheets with faxes that originate from e-mail messages.
Step 4	**fax send coverpage comment** *string* **Example:** `Router(config)# fax send coverpage comment Fax Cover Sheet`	(Optional) Adds personalized text in the title field of a fax cover sheet generated by the gateway. • *string* --ASCII character string.
Step 5	**fax send coverpage show-detail** **Example:** `Router(config)# fax send coverpage show-detail`	(Optional) Prints all of the e-mail header information as part of the text on fax cover sheets generated by the gateway.
Step 6	**fax send coverpage email-controllable** **Example:** `Router(config)# fax send coverpage email-controllable`	(Optional) Allows the fax e-mail address to enable cover page generation on a per-recipient basis. This means that if an e-mail header has a parameter that sets cover to no or cover to yes, the setting for the **fax send coverpage enable** command is overridden. For example, if the address has the cover parameter set to no, the parameter overrides the setting for the **fax send coverpage enable** command and the off-ramp gateway does not generate a fax cover page. If the address has the cover parameter set to yes, the off-ramp gateway defers to the setting configured in the e-mail address and generates a cover page whether or not the **fax send coverpage enable** command has been used. The table above contains examples of entries in the e-mail To: field to control the generation of fax cover pages.
Step 7	**end** **Example:** `Router(config)# end`	Exits global configuration mode.

Configuring MTA Parameters on the Off-Ramp Gateway

Perform this task to configure the way in which the off-ramp gateway receives messages from the MTA. In store-and-forward fax, the MTA is the messaging infrastructure in the packet network that performs message routing, storage, and transport. The MTA can be either a standard Internet MTA (for example, UNIX sendmail) or a custom store-and forward fax software.

For added security, with the MTA, you can define SMTP host aliases that are different from the normal host-name system (DNS) hostnames on your network. The gateway accepts incoming mail if the destination hostname of the incoming mail matches one of the aliases configured by the **mta receive aliases** command.

The MTA also controls the generation of MDN status messages.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mta receive aliases** *string*
4. **mta receive maximum-recipients** *number*
5. **mta receive generate** [**mdn** | **permanent-error**]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**mta receive aliases** *string* **Example:** `Router(config)# mta receive aliases fax24.ABC.com`	Defines a hostname to be used as an alias for the off-ramp gateway. Up to ten aliases can be defined. The gateway accepts incoming mail if the destination hostname of the inbound fax e-mail matches an alias. • *string* --Hostname or IP address. If specifying an IP address, enclose it in brackets as follows: [xxx.xxx.xxx.xxx]. The default is the hostname of the gateway. **Note** This command is mandatory unless you are using the gateway hostname as the e-mail hostname. For example, the router does not accept an e-mail to FAX=5550119@10.80.8.107 unless 10.80.8.107 is defined as an alias.
Step 4	**mta receive maximum-recipients** *number* **Example:** `Router(config)# mta receive maximum-recipients 48`	Defines the number of simultaneous SMTP recipients handled by this gateway. This definition is intended to limit the number of resources allocated for fax transmissions. • *number* --Number of simultaneous SMTP recipients. Range: 0 to 1024. The default is 0 recipients, which means that incoming mail messages are not accepted; therefore, no faxes are sent by the off-ramp gateway.

	Command or Action	Purpose
Step 5	**mta receive generate** [**mdn** | **permanent-error**] **Example:** `Router(config)# mta receive generate permanent-error`	Specifies the type of fax delivery response message that a T.37 fax off-ramp gateway should return. To return to the default, use the **no** form of this command. **Note** The **mta receive generate** command replaces the **mta receive generate-mdn** command in Cisco IOS Release 12.3(7)T. • When DSN messages are requested, more information is provided in the DSNs than if this command is not enabled. • The **mdn**keyword directs the T.37 off-ramp gateway to process response MDNs from an SMTP server. • The **permanent-error** keyword directs the T.37 off-ramp fax gateway to classify all fax delivery errors as permanent so that they are forwarded in DSN messages with descriptive error codes to an MTA. The default is that standard SMTP status messages are returned to the SMTP client with error classifications of permanent or transient. **Note** Messages returned to the originator of an e-mail message indicating that the e-mail message has been opened is reported through MDN. Specifications for MDN are described in RFC 2298. For more information, see the Configuring MDNs on the Off-Ramp Gateway, on page 151.
Step 6	**end** **Example:** `Router(config)# end`	Exits global configuration mode.

Configuring MDNs on the Off-Ramp Gateway

MDNs are sent to an address chosen by the sender. The following text is included in the e-mail header of the message:

```
Disposition-Notification-To:
```

This text is followed by the address of the sender as defined in the **mta send return-receipt-to** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mta receive generate mdn**

4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**mta receive generate mdn** **Example:** `Router(config)# mta receive generate mdn`	Instructs the off-ramp gateway to respond to and process MDN requests from the SMTP server. **Note** The **mta receive generate mdn**command replaces the **mta receive generate-mdn** command in Cisco IOS Release 12.3(7)T.
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode.

Configuring Security and Accounting on the Off-Ramp Gateway

This task consists of the following subtasks:

Note It is recommended that access control lists (ACLs) be configured to restrict which IP addresses can connect to the SMTP port (port 25). For information about configuring ACLs, see the Creating an IP Access List and Applying it to an Interface module in the *Cisco IOS Security Configuration Guide*. We recommend that the off-ramp gateway accept incoming SMTP connections only from trusted mailers. Configure packet filters to permit only certain trusted IP addresses to send faxes to the store-and-forward fax off-ramp gateway.

Configuring Off-Ramp Gateway Security and Accounting

Perform this task to set up authorization and billing for the off-ramp gateway.

Note Steps 10 through 13 do not apply to Cisco AS5300 gateways with modem cards.

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login fax radius**
5. **aaa accounting connection fax start-stop group radius**
6. **radius-server host** *host* **auth-port** *number* **acct-port** *number*
7. **radius-server key** {**0** *string* | **7** *hidden-string*| *string*}
8. **radius-server vsa send accounting**
9. **radius-server vsa send authentication**
10. **mmoip aaa method fax authentication** *method-list-name*
11. **mmoip aaa receive-authentication enable**
12. **mmoip aaa method fax accounting** *method-list-name*
13. **mmoip aaa receive-accounting enable**
14. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables AAA security and accounting services.
Step 4	**aaa authentication login fax radius** **Example:** `Router(config)# aaa authentication login fax radius`	Defines a method list called fax in which RADIUS is defined as the only method of login authentication. **Note** The method list name (fax) should match the name used in the Configuring T.37 IVR Application Security and Accounting on the Off-Ramp Gateway, on page 156.
Step 5	**aaa accounting connection fax start-stop group radius** **Example:** `Router(config)# aaa accounting connection fax start-stop group radius`	Defines the accounting method list called fax with RADIUS as a method and with an option to send both start and stop accounting records to the AAA server. The fax method list is static and is applied by default to all voice interfaces.

	Command or Action	Purpose
		Note The method list name (fax) should match the name used in the Configuring T.37 IVR Application Security and Accounting on the Off-Ramp Gateway, on page 156.
Step 6	**radius-server host** *host* **auth-port** *number* **acct-port** *number* **Example:** `Router(config)# radius-server host accthost.ABC.com auth-port 2222 acct-port 2223`	Identifies the RADIUS server and the port that is used for authentication and accounting services. You can use multiple **radius-server host** commands to specify multiple hosts. The software searches for hosts in the order in which you specify them. • *host* --Hostname or IP address of the RADIUS server host. • *number* --Port number for authentication or accounting requests. If set to 0, the host is not used. If unspecified for authentication, the port number defaults to 1645. If unspecified for accounting, the port number defaults to 1646.
Step 7	**radius-server key** {**0** *string* | **7** *hidden-string*| *string*} **Example:** `Router(config)# radius-server key 0 3j59g3qpc`	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon on the server. • **0** --Unencrypted (clear-text) shared key follows. • **7** --Hidden shared key follows. • *hidden-string* --Hidden shared key. • *string* --Unencrypted (clear-text) shared key.
Step 8	**radius-server vsa send accounting** **Example:** `Router(config)# radius-server vsa send accounting`	Enables the network access server to recognize and use accounting vendor-specific attributes (VSAs) as defined by RADIUS Internet Engineering Task Force (IETF) attribute 26. VSAs allow vendors to support their own extended attributes not suitable for general use.
Step 9	**radius-server vsa send authentication** **Example:** `Router(config)# radius-server vsa send authentication`	Enables the network access server to recognize and use authentication VSAs as defined by RADIUS IETF attribute 26.
Step 10	**mmoip aaa method fax authentication** *method-list-name* **Example:** `Router(config)# mmoip aaa method fax authentication authen-fax`	Defines the name of the method list to be used for store-and-forward fax AAA authentication. The method list, which defines the type of authentication services provided for store-and-forward fax, is itself defined using the **aaa authentication** global configuration command. Unlike standard AAA (in which each defined method list can be applied to specific interfaces and lines), the AAA

	Command or Action	Purpose
		authentication method lists used in store-and-forward fax are applied globally on the gateway. • *method-list-name* --Character string that names a list of authentication methods to be used with store-and-forward fax.
Step 11	**mmoip aaa receive-authentication enable** **Example:** `Router(config)# mmoip aaa receive-authentication enable`	Enables AAA authentication services if an AAA authentication method list has been defined using both the **aaa authentication** command and the **mmoip aaa method fax authentication** command.
Step 12	**mmoip aaa method fax accounting** *method-list-name* **Example:** `Router(config)# mmoip aaa method fax accounting acctg-fax`	(Required) Defines the name of the method list to be used for store-and-forward fax AAA accounting. The method list, which defines the type of accounting services provided for store-and-forward fax, is itself defined using the aaa accounting global configuration command. Unlike standard AAA (in which each defined method list can be applied to specific interfaces and lines), the AAA accounting method lists used in store-and-forward fax are applied globally on the gateway. • *method-list-name* --Character string that names a list of accounting methods to be used with store-and-forward fax.
Step 13	**mmoip aaa receive-accounting enable** **Example:** `Router(config)# mmoip aaa receive-accounting enable`	Enables off-ramp AAA accounting services if an AAA accounting method list has been defined using both the **aaa accounting** command and the **mmoip aaa method fax accounting** command.
Step 14	**end** **Example:** `Router(config)# end`	Exits global configuration mode.

Creating SMTP filters with ACLs

Incoming ACLs can be used on Ethernet or Fast Ethernet interfaces to filter SMTP traffic for store-and-forward fax. It is recommended that ACLs be configured to restrict access to the SMTP port (port 25) to only trusted e-mail servers. The creation of ACLs is beyond the scope of this document.

The following example, though, provides a starting point by restricting access to the SMTP port 25 to a trusted e-mail server (IP address 10.0.0.1):

```
! Configure ACLs to restrict access to the SMTP port (port 25) to only "trusted"
! e-mail servers. Depending on the topology of your particular network, replace the
! any keyword with the destination IP addresses of the Ethernet and Fast Ethernet
! interfaces. Define all trusted e-mail servers using the tcp host ip-address
```

```
! portion of this command.
access-list 100 permit tcp host 10.0.0.1 any eq smtp
 access-list 100 deny tcp any any eq smtp
 access-list 100 permit ip any any
!
! Enter interface configuration mode for Ethernet interface 0.
interface ethernet 0
! Apply the access list to this interface.
 access-group 100 in
!
! Enter interface configuration mode for Fast Ethernet interface 0.
interface fastethernet 0
! Apply the access list to this interface.
access-group 100 in
```

Note For complete information about configuring ACLs, see the *Cisco IOS Security Configuration Guide*.

Configuring T.37 IVR Application Security and Accounting on the Off-Ramp Gateway

Perform this task to configure the specified IVR application to perform authentication and accounting tasks in conjunction with a RADIUS server. IVR uses (Tcl) scripts to gather information and to process accounting and billing. For example, a Tcl IVR script plays when a caller receives a voice-prompt instruction to enter a specific type of information, such as a personal identification number (PIN). After playing the voice prompt, the Tcl IVR application collects the predetermined number of touch tones and sends the collected information to an external server for user authentication and authorization.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **application**
4. **service** *service-name location*
5. **param accounting enable**
6. **param accounting-list** *method-list-name*
7. **param authentication enable**
8. **param authen-list** *method-list-name*
9. **param authen-method** {**prompt-user** | **ani** | **dnis** | **gateway** | **redialer-id** | **redialer-dnis**}
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Router# configure terminal`	
Step 3	**application** **Example:** `Router(config)# application`	Enters application configuration mode to configure voice applications and services.
Step 4	**service** *service-name location* **Example:** `Router(config-app)# service fax_detect flash:app_fax_detect.10.1.2.2.tcl`	Loads a VoiceXML document or Tcl script and defines its application name. • *service-name* --Name that identifies the voice application. This is a user-defined name and does not have to match the script name. • *location* --Directory and filename of the Tcl script or VoiceXML document in URL format. For example, Flash memory (flash:filename), a TFTP (tftp://../filename), or an HTTP server (http://../filename) are valid locations.
Step 5	**param accounting enable** **Example:** `Router(config-app)# param accounting enable`	Enables AAA accounting for a Tcl application.
Step 6	**param accounting-list** *method-list-name* **Example:** `Router(config-app)# param accounting-list fax`	Defines the name of the accounting method list to be used for AAA with store-and-forward fax on a voice feature card (VFC). • *method-list-name* --Character string used to name a list of accounting methods to be used with store-and-forward fax. **Note** The method list name should match the name used in the Configuring Security and Accounting on the Off-Ramp Gateway, on page 152.
Step 7	**param authentication enable** **Example:** `Router(config-app)# param authentication enable`	Enables AAA authentication for a Tcl application.
Step 8	**param authen-list** *method-list-name* **Example:** `Router(config-app)# param authen-list fax`	Specifies the name of an authentication method list for a Tcl application. • *method-list-name* --Character string used to name a list of authentication methods to be used with store-and-forward fax.

	Command or Action	Purpose
		Note The method list name should match the name used in the Configuring Security and Accounting on the Off-Ramp Gateway, on page 152.
Step 9	**param authen-method** {**prompt-user** | **ani** | **dnis** | **gateway** | **redialer-id** | **redialer-dnis**} **Example:** `Router(config-app)# param authen-method ani`	Specifies the type of authentication method for the named application. • **prompt-user** --The user is prompted for the Tcl application account identifier. • **ani** --The calling-party telephone number (automatic number identification [ANI]) is used as the Tcl application account identifier. • **dnis** --The called party telephone number (dialed number identification service [DNIS]) is used as the Tcl application account identifier. • **gateway** --The router-specific name derived from the hostname and domain name is used as the Tcl application account identifier. It is displayed in the following format: router-name.domain-name. • **redialer-id** --The account string returned by the external redialer device is used as the Tcl application account identifier. In this case, the redialer ID is either the redialer serial number or the redialer account number. • **redialer-dnis** --The called party telephone number (DNIS) is used as the Tcl application account identifier captured by the redialer if a redialer device is present.
Step 10	**end** **Example:** `Router(config-app)# end`	Exits application configuration mode.

Troubleshooting Tips

Use the following show commands to troubleshoot store-and-forward fax on both the on-ramp and off-ramp gateways.

- **show dial-peer voice** [*tag*] [**summary**]--Displays configuration information for MMoIP and POTS dial peers so that you can verify that store-and-forward fax is enabled.
- **show call application voice summary** --Lists all voice applications that are loaded on the router so that you can confirm that the scripts that you are interested in are loaded.

- **show call application voice** *application-name* --Displays the line-by-line contents of the Tcl script associated with the specified application.
- **show accounting** --No specific **show** command exists for either RADIUS or TACACS+ accounting. To obtain accounting records that display information about users currently logged in, use the **show accounting** command.

Configuration Examples for T.37 Store-and-Forward Fax

Example On-Ramp Gateway

The following example is sample configuration of a T.37 on-ramp gateway:

```
! Define the called subscriber number. In this case, the number configured as the
! destination pattern will be used as the called subscriber identifier.
fax receive called-subscriber $d$
!
! Specify the originator of the e-mail address. In this case, the originator information
! is derived from the calling number.
mta send mail-from username $s$
!
! (Optional) Provide additional information about the sending device. In this example,
! the sending device's hostname is alabama
mta send origin-prefix alabama
!
! Define where this fax-mail should be delivered (which is the mail server postmaster
! account) if it cannot be delivered to the defined destination.
mta send postmaster postmaster@company.com
!
! (Optional) If configuring MDNs, specify the address to which they should be
! sent.
mta send return-receipt-to username postmaster@company.com
!
! Specify the destination e-mail server that accepts on-ramp fax mail.
mta send server california.fax.com
!
! Define the text string that will be displayed as the subject of the fax mail.
mta send subject Fax-Mail Message
!
! Enter dial-peer configuration mode and define an on-ramp POTS peer.
dial-peer voice 1000 pots
!
! Designate fax as the type of information handled by this dial peer.
 information-type fax
!
! Specify direct inward dial for this dial peer.
 direct-inward-dial
!
! Define the incoming called number associated with this dial peer.
 incoming called number 5105550119
!
! (Optional) Define the maximum number of connections that will be used simultaneously
! to transmit fax mail.
 max-conn 10
!
! Define an on-ramp MMoIP dial peer.
dial-peer voice 1001 mmoip
!
! Define the telephone number associated with this dial peer.
```

```
 destination-pattern 14085550119
!
! Define a destination e-mail address for this dial peer.
 session-target mailto:$d$@abccompany.com
!
! (Optional) Request that DSNs be sent.
 dsn failure
!
! Specify a particular image encoding method to be used for fax images. In this
! example, Modified Huffman (IETF standard) is being specified.
 image encoding mh
!
!Specify a particular fax image resolution. In this example, the image resolution was
!set to 204 by 196 pixels per inch (fine).
 image resolution fine
!
!Designate fax as the type of information handled by this dial peer.
 info-type fax
!
!(Optional) Define the maximum number of connections that will be used simultaneously
!to transmit fax mail.
 max-conn 10
!
!(Optional) Request that MDNs be sent.
 mdn
!
! Specify SMTP as the protocol to be used for store-and-forward fax.
 session protocol smtp
```

Example Off-Ramp Gateway

The following is sample configuration of a T.37 off-ramp gateway:

```
.
.
! Define the transmitting subscriber number (TSI); this is the number that is
! displayed in the LCD of the receiving fax machine. In this example, the sender's
! name (captured by the on-ramp from the sending fax machine) will be used.
fax send transmitting-subscriber $s$
!
! Configure the speed of the fax transmission. In this case, fax transmissions will be
! sent at 14400 bits per second.
fax send max-speed 14400
!
! Define a hostname to be used as an alias for the off-ramp Cisco AS5300 device.
mta receive aliases abccompany.com
!
! (Optional) Specify that the Cisco AS5300 universal access server will respond to an MDN
! request.
mta receive generate mdn
!
! Define the number of simultaneous SMTP recipients (in this case, 10) handled by this
! Cisco AS5300 device.
mta receive maximum-recipients 10
!
!
! Specify that the company name will appear in the center position of the fax
! header information.
fax send center-header Acme Company
!
! Specify that the page count will appear in the right position of the fax header
! information.
fax send right-header $p$
```

```
!
! Specify that the date will appear in the left position of the fax header
! information.
fax send left-header $a$
!
! Enable the Cisco AS5300 device to send a cover sheet with faxes that originate from
! e-mail messages.
fax send coverpage enable
!
! Add a personalized comment to the title field of the fax cover sheet. In this case,
! the phrase FAX TRANSMISSION was added.
fax send coverpage comment FAX TRANSMISSION
!
! Enter dial-peer configuration mode and define an off-ramp POTS dial peer.
dial-peer voice 1002 pots
!
! Designate fax as the type of information handled by this dial peer.
 information-type fax
!
! Define a telephone number to be associated with this dial peer.
 destination-pattern 1408555....
!
! Add prefix.
 prefix 9,555
!
! Define an off-ramp MMoIP peer.
dial-peer voice 1003 mmoip
!
! Designate fax as the type of information handled by this dial peer.
 information-type fax
!
! Define an incoming called number to be associated with this dial peer.
 incoming called-number 14085550020
!
! Specify a particular fax image resolution. In this example, the image resolution was
! set to 204 by 196 pixels per inch (fine).
 image resolution fine
!
```

Example Combined On-Ramp and Off-Ramp Gateway

The following is sample T.37 store-and-forward fax configuration for a single gateway that performs both on-ramp and off-ramp gateway functions:

```
fax interface-type fax-mail
!
service timestamps debug uptime
service timestamps log uptime
!
hostname fax-gateway
!
enable password lab
!
username betatest password 0 password
!
ip subnet-zero
ip host mars 192.168.254.254
ip host saturn 172.28.129.150
ip domain-name abcwrecking.com
ip name-server 10.14.116.1
!
! Used for fallback from T.38 fax relay to T.37 fax.
voice hunt user-busy
```

```
!
!
! Global service for fax relay.
voice service voip
 fax protocol t38 ls_redundancy 0 hs_redundancy 0
!
application
 service app_offramp tftp://mars/libretto-test/app_offramp5.tcl
  param authen-list fax
  param authen-method gateway
  param accounting-list fax
!
application
 service app_onramp tftp://mars/smith/faxdir/onramp13.nc.tcl
  param authen-list fax
  param authen-method gateway
  param language 1 en
  param accounting-list fax
application
 service app_onramp set-location en 0 tftp://mars/smith/WV/en_new/
!
fax receive called-subscriber $d$
fax send transmitting-subscriber $s$
fax send left-header $s$
fax send center-header $t$
fax send right-header Page: $p$
fax send coverpage enable
fax send coverpage email-controllable
fax send coverpage comment ABC Wrecking cover page
mta receive aliases [10.14.120.2]
mta send server saturn_smtp_server
mta send subject "Facsimile Transmission"
mta send origin-prefix ABCWrecking Fax
mta send postmaster postmaster postmaster@abcwrecking.com
mta send mail-from hostname saturn
mta send mail-from username fax-user
mta send return-receipt-to hostname return.host.com
mta send return-receipt-to username $s$
mta receive aliases bock.abcwrecking.com
mta receive aliases abcwrecking.com
mta receive maximum-recipients 200
mta receive generate mdn
!
!
controller T1 1/1
 framing esf
 clock source line primary
 linecode b8zs
 ds0-group 0 timeslots 1-24 type e&m-fgd
!
interface Ethernet0
 ip address 10.14.120.2 255.255.0.0
 no ip directed-broadcast
!
interface FastEthernet0
 no ip address
 no ip directed-broadcast
 shutdown
 duplex auto
 speed auto
!
ip default-gateway 10.14.0.1
ip classless
ip route 192.168.254.0 255.255.255.0 10.14.0.1
```

```
no ip http server
!
!
voice-port 1/1:0
!
!
! Inbound peer for T.37 on-ramp operation.
dial-peer voice 2 pots
 application app_onramp
 incoming called-number 5......
 direct-inward-dial
 port 1/1:0
!
! Outbound peer for T.37 on-ramp operation.
dial-peer voice 3 mmoip
! The application named below must be exactly as shown!
 service fax_on_vfc_onramp_app out-bound
 destination-pattern 57108..
 session target mailto:$d$@mail-server.abcwrecking.com
! MDN and DSN configuration can be set in this peer.
!
! Inbound peer for T.37 off-ramp operation.
dial-peer voice 21 mmoip
 application app_offramp
 incoming called-number 5......
 information-type fax
!
! Outbound peer for T.37 off-ramp operation.
dial-peer voice 20 pots
 destination-pattern 5......
 port 1/1:0
 prefix 5
```

Example Combined On-Ramp and Off-Ramp Gateway with Security

The following is sample configuration for a combined on-ramp and off-ramp gateway enabled for security:

```
!
! Enable AAA security services.
aaa new-model
! Define the method list to be used with store-and-forward fax authentication.
mmoip aaa method fax authentication onramp-auth
! Define the method list to be used with store-and-forward fax accounting services.
mmoip aaa method fax accounting onramp-acct
! Define and enable the AAA authentication method list for store-and-forward fax.
aaa authentication login onramp-auth radius local
! Define and enable the AAA accounting method list for store-and-forward fax.
aaa accounting connection onramp-acct stop-only radius
! Enable on-ramp authentication.
mmoip aaa receive-authentication enable
! Enable on-ramp accounting services.
mmoip aaa receive-accounting enable
! Enable off-ramp authorization.
mmoip aaa send-authentication enable.
! Enable off-ramp accounting services.
mmoip aaa receive-accounting enable
! Define the gateway ID as the means by which AAA identifies the user for
! off-ramp authentication.
mmoip aaa send-id primary gateway
! Define the gateway ID as the means by which AAA identifies the user for on-ramp
! authentication.
mmoip aaa receive-id primary gateway
! Configure the Cisco AS5300 device to support RADIUS.
```

```
radius-server host 172.18.11.13 auth-port 1645 acct-port 1646
radius-server key password
! Configure the RADIUS server to recognize and use vendor-specific attributes.
radius-server vsa send accounting
radius-server vsa send authentication
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco IOS Voice commands : complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Voice Command Reference*
Configuring ACL	Creating an IP Access List and Applying it to an Interface module in the Cisco IOS Security Configuration Guide

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Configuring T.37 Store-and-Forward Fax

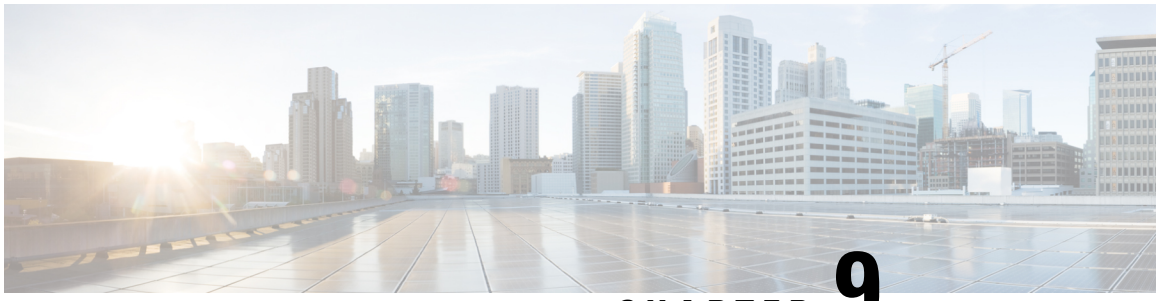
The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 7: Feature Information for Configuring T.37 Store-and-Forward Fax

Feature Name	Releases	Feature Information
Extended Simple Mail Transfer Protocol (ESMTP) Accounting in Store-and-Forward Fax	12.2	The SMTP facilitates the store-and-forward fax functionality, along with an additional functionality that provides confirmation of delivery using existing SMTP mechanisms, such as ESMTP.
T.37 Store-and-Forward Fax	12.0(7)T 12.1(5)T) 12.2(8)T 12.2(15)T 12.2(2)XB 12.3(14)T	Fax pass-through is a method for sending faxes over IP networks. The following command was modified: **service fax_on_vfc_onramp_app out-bound**.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.
© 2004-2011 Cisco Systems, Inc. All rights reserved.



CHAPTER 9

Configuring Fax Detection

Configuring Fax Detection

This chapter describes configuration for the fax detection (single-number voice and fax) feature on an IP network. Fax detection is the capability to detect automatically whether an incoming call is voice or fax.

History for the Fax Detection Feature

Release	Modification
12.1(5)XM	This feature was introduced on the Cisco AS5300.
12.2(2)XB	This feature was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(8)T	This feature was integrated into this release and implemented on the Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.
12.2(11)T	This feature was implemented on the Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.4(4)T	This feature was integrated into Cisco IOS release 12.4(4)T.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn . You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring Fax Detection

Before you configure fax detection, perform the following tasks:

- Configure your IP network and ensure that it is operational.
- Install a voice server and ensure that it is working on the IP network; for example, install an H.323 voice-mail server on your network and configure the corresponding outgoing dial peer for VoIP.
- Install fax service and ensure that it is working on the IP network. The fax service can be T.38 fax relay, T.37 store-and-forward fax, or both. By making sure that the fax service is operational before beginning to configure the fax detection application, you can keep fax configuration issues separate and make troubleshooting easier.
  - For information about T.38 fax relay, see the chapter “Configuring T.38 Fax Relay.”
  - For more information about T.37 store-and-forward fax, see the chapter “Configuring T.37 Store-and-Forward Fax.”

Restrictions for Configuring Fax Detection

The restrictions for fax detection are as follows:

- Prior to TCL IVR script app_fax_detect.2.1.2.3.tcl (dated April 3, 2009), Cisco’s fax detection TCL-IVR scripts only support T.37 store-and-forward fax. Beginning with TCL IVR script app_fax_detect.2.1.2.3.tcl (dated April 3, 2009), T.38 fax relay is also supported.

Note Although the TCL-IVR scripts have built-in customization options, we recommend that you contact Cisco Developer Support before you add specific IVR prompts. For more information, see the "Developer Support" section on page 23 .

- For TI-549 DSPs, only high-complexity VCWare is supported.
- Cisco’s fax detection feature relies on the originating gateway’s ability to detect the fax identifying either the CNG tone from the called fax machine or a user-initiated action, such as the caller pressing a DTMF digit, to identify a fax call. The following are known issues with fax machines that support fax detection:
  - Certain fax machines, produced before 1995, do not produce the required tone.
  - Fax machines that allow callers to talk before sending a fax temporarily stop the CNG detection when voice is heard. If the tone is not played every 3.5 seconds, the fax detection script on the originating gateway might not detect the fax and the call is not transferred to the terminating fax device.
  - If a single number script call is answered by a person instead of a fax machine, the fax might not be detected and is not transferred.
  - Certain routing schemes, such as call forwarding, might impact the success of fax detection.

Information About Fax Detection

Voice gateway dial peers for the fax detection application include an inbound dial peer to receive calls from the PSTN and at least two outbound dial peers, one for voice calls and one for fax, as explained in the following paragraphs.

The inbound dial peer describes the inbound call leg from the telephony connection to the gateway, and is called a plain old telephone service (POTS) dial peer. POTS dial peers define the characteristics of the telephony (PSTN) connection between the sending fax device or voice instrument and the gateway to the IP network. In general, the gateway uses the line characteristics defined by POTS dial peers to determine call type and call destination. The gateway then finds an outbound dial peer whose configured parameters match these attributes and routes the call to it. You can establish more than one POTS dial peer if you want different incoming calls to receive different handling. The fax detection application is enabled on the inbound dial peer.

One of the two types of outbound dial peers in the gateway router is the outbound Voice-over-IP (VoIP) dial peer, which describes the VoIP call leg from the router to the voice-mail server or voice path. You configure this dial peer exactly as you would configure an ordinary VoIP dial peer for voice calls.

The second type of outbound dial peer on the on-ramp gateway must be a fax dial peer. The fax dial peer can be either a Multimedia Mail over IP (MMoIP) dial peer, which describes an IP call leg for store-and-forward fax, or a VoIP dial peer configured for T.38 fax relay. The MMoIP dial peer is configured with the fax_on_vfc_onramp_app IVR application in the outbound mode, just the same as the standard configuration for store-and-forward fax. The VoIP dial peer for fax is configured exactly the same as the standard configuration for fax relay; no IVR application is required on this dial peer.

Fax Detection Modes

Fax detection supports the use of a single E.164 number for both voice mail and fax mail by providing the capability to detect automatically whether an incoming call is voice or fax. Fax detection can be configured to use the distinctive fax calling tones (CNG), a manually dialed digit, or both to distinguish fax calls from voice calls. Fax detection supports the following modes of operation:

The fax detection modes are explained in the following sections.

Connect-First Mode

(Default) When you configure connect-firstmodeon the gateway, incoming calls are connected immediately to the voice-mail server, which plays a greeting, or audio prompt, based upon the number called. Because this greeting is generated by the voice-mail application rather than by the gateway, each E.164 number can have its own custom prompt.

The gateway listens for distinctive CNG (fax) tones during the prompt and for the remainder of the call. If the gateway hears CNG at any time, the voice-mail application is disconnected and the call is passed on to the fax relay or store-and-forward fax application, depending on which was configured on the gateway. Note that non-CNG faxes are not supported in this mode.

If any dialed digits, or DTMF tones, are detected during the call, they are relayed to the voice-mail server using the DTMF signaling protocol configured on the dial peer. The gateway does not listen for DTMF and does not interpret DTMF.

The connect-first mode is useful when you expect that most incoming calls will be voice. The cost of this mode is the added load on the voice-mail application, which is now required to answer fax calls also.

This mode is the default if no mode is configured.

Listen-First Mode

When listen-first mode is configured on the gateway and an incoming call is received, the gateway can play a configurable audio prompt to greet the caller or provide instructions.

Note If an audio file for this prompt has not been specified during configuration, the caller hears 9 seconds of silence. We recommend configuring a prompt.

The gateway listens for CNG for 9 seconds before passing the call to an application or server. If CNG is detected, the call is passed to the fax relay or store-and-forward fax application, whichever is configured on the gateway. If CNG is not heard during the first 9 seconds, the call is passed to the voice-mail server. Non-CNG faxes are not supported in this mode.

If any DTMF tones are detected, the call is connected to the voice server. Once a call is connected to the voice server, DTMF tones are relayed using the DTMF signaling protocol that has been configured on the dial peer.

In listen-first mode, CNG fax calls are never automatically connected to the voice-mail server, so this mode is useful when CNG fax calls constitute a significant proportion of the calls to this E.164 number.

Default-Voice Mode

When default-voice mode is configured on the gateway and an incoming call is received, the gateway can play a configurable audio prompt to greet the caller or provide instructions.

Note If the audio file for this prompt has not been specified during configuration, the caller hears 9 seconds of silence. We recommend configuring a prompt.

In default-voice mode, during configuration you can specify a DTMF digit for incoming callers to press to manually select the voice-mail server and another digit that they can press to select the fax application. When the gateway detects either of these configured DTMF digits, the call is connected as requested.

The gateway listens for CNG for 9 seconds before passing the call to an application. If CNG is detected, the call is passed to the fax relay or store-and-forward fax application, whichever is configured on the gateway. If CNG is not heard during the first 9 seconds, the call is passed to the voice-mail server.

If any DTMF tones are detected, the gateway interprets the DTMF. If the tones match the DTMF digit configured for voice, the call is passed to the voice-mail server. If the tones match the DTMF digit configured for fax, the call is passed to the fax application. If the tones do not match either the voice or fax digit, the prompt is replayed. Once a call has been connected to the voice server, subsequent DTMF tones are relayed using the DTMF signaling protocol that has been configured on the dial peer.

Non-CNG-compliant faxes are supported in the default-voice mode when the caller manually selects the fax application by pressing the keypad key to send the DTMF digit designated for fax.

Default-Fax Mode

When default-fax mode is configured on the gateway and an incoming call is received, the gateway can play a configurable audio prompt to greet the caller or provide instructions.

Note If the audio file for this prompt has not been specified during configuration, the caller hears 9 seconds of silence. We recommend configuring a prompt.

During configuration you can specify a DTMF digit that incoming callers can press to manually select the voice-mail server and another digit that they can press to select the fax application. When the gateway detects either of these configured DTMF digits, the call is immediately connected as requested.

The gateway listens for CNG for 9 seconds before passing the call to an application. If CNG is detected, the call is passed to the fax relay or store-and-forward fax application, whichever is configured on the gateway. If CNG is not heard during the first 9 seconds, the call is passed to the fax relay or store-and-forward fax application.

If any DTMF tones are detected, the gateway interprets the DTMF. If the tones match the DTMF digit configured for voice, the call is passed to the voice-mail server. If the tones match the DTMF digit configured for fax, the call is passed to the fax application. If the tones do not match either the voice digit or the fax digit, the prompt is replayed. Once a call has been connected to the voice server, subsequent DTMF tones are relayed using the DTMF signaling protocol that has been configured on the dial peer.

The default-fax mode is useful when fax calls constitute a significant proportion of the calls. In addition, this mode supports non-CNG-compliant faxes, without requiring the manual activation of a DTMF tone.

Audio Prompts

All of the fax detection modes except connect-first require you to install audio prompt files, or greetings, to tell callers how to send voice or fax to the called number. Default audio prompt files are included in the same zip file on Cisco.com that contains the TCL script. You may also create your own audio prompts to customize the greeting. In either case, the audio files must be installed in a location that is accessible by the gateway. The wording of the default gateway prompts is shown in the table below.

Table 8: Fax Detection Default Prompts

Mode	Default Prompt	Audio Filename
listen-first	To send a fax, press the **Start** key on your fax machine now. For voice calls, press any key or stay on the line.	• en_listen_first.au (English) • en_Uone_listen-first.au (English; same voice as prompts for Cisco uOne voice messaging service) • ch_listen_first.au (Mandarin) • sp_listen_first.au (Spanish)
default-voice	To send a fax, press **2**, then press the **Start** key on your fax machine. For voice calls, press **1** or stay on the line.	• en_default_voice.au (English) • en_Uone_default-voice.au (English; same voice as prompts for Cisco uOne voice messaging service) • ch_default_voice.au (Mandarin) • sp_default_voice.au (Spanish)

Mode	Default Prompt	Audio Filename
default-fax	For voice calls, press **1**. To send a fax, press the **Start** key on your fax machine now.	• en_default_fax.au (English) • en_Uone_default-fax.au (English; same voice as prompts for Cisco uOne voice messaging service) • ch_default_fax.au (Mandarin) • sp_default_fax.au (Spanish)

How to Download the Fax-Detection Application and Default Audio-Prompt Files

This section describes how to download the TCL script and default audio prompt files used with the fax detection application. You must download these files before you can configure the fax detection application. The script and the prompts are contained in a single zip file on Cisco.com.

The Cisco IOS File System (IFS) reads the files, so any IFS-supported URL can be used as a location for the files. URLs can include TFTP, FTP, or a pointer to a device on the router. For more information, see the *TCL IVR API Version 2.0 Programmer's Guide*.

SUMMARY STEPS

1. Log in to the Cisco website and go to http://www.cisco.com/cgi-bin/tablebuild.pl/tclware.
2. Select and download the following zip file which contains the fax detection application.
3. Unzip the file.
4. Move the application script file (app_fax_detect.2.1.2.3.tcl) and audio prompt files (*.au) to a location that can be accessed by your gateway using a URL address.
5. If you create your own audio files, ensure that they are in the proper format.

DETAILED STEPS

Step 1 Log in to the Cisco website and go to http://www.cisco.com/cgi-bin/tablebuild.pl/tclware.

When you are logged in to the Cisco website, you can navigate to the TCLWare page from the Cisco home page by following this path: Technical Support / Software Center / Access Software / TCLWare.

Step 2 Select and download the following zip file which contains the fax detection application.

You are asked for the following information:

- Cisco Connection Online (CCO) server nearest your physical location
- Where to save the files on your disk

Step 3 Unzip the file.

The zip file that you download includes the following files:

- Fax detection application TCL script file (app_fax_detect.2.1.2.3.tcl or a later version)

- Default audio prompt files.
- README file

Step 4 Move the application script file (app_fax_detect.2.1.2.3.tcl) and audio prompt files (*.au) to a location that can be accessed by your gateway using a URL address.

The URL of a TCL script or audio prompt is a standard URL that points to the location of the script. Examples include the following:

- flash:myscript.tcl--The script called myscript.tcl is located in Flash memory on the router.
- slot0:myscript.tcl--The script called myscript.tcl is located in a device in slot 0 on the router.
- tftp://BigServer/myscripts/MouseTrap.tcl--The script called MouseTrap.tcl is located in a server called BigServer in a directory within the tftpboot directory called myscripts.

Step 5 If you create your own audio files, ensure that they are in the proper format.

The IVR prompts require an audio file format (.au) with 8-bit, u-law, and 8-kHz encoding. To encode the audio files, it is recommended that one of the following two audio tools (or a similar tool of comparable quality) be used:

- Cool Edit, manufactured by Syntrillium Software Corporation.
- AudioTool, manufactured by Sun Microsystems.

The default files supplied by Cisco are in the proper format.

Note Flash memory is limited to 32 entries, which may prevent your loading all TCL and audio files there.

How to Load the Fax Detection Application

Fax detection is an IVR application that is written in a TCL script. The script must be downloaded from Cisco.com and installed on your network before the fax detection application can be loaded on the gateway. After you have installed the script at a location that is accessible by the gateway, load it using a name of your choice.

Note All subsequent commands that refer to the fax detection application use the name that you select when you load the application on the gateway.

Before you begin

This section describes the prerequisites for configuring fax detection.

- Download the fax detection application script named app_fax_detect.2.1.2.3.tcl to your TFTP server.

The app_fax_detect.2.1.2.3.tcl script is used to automatically route single-number fax calls to an MMoIP dial peer when configured in a T.37 fax store-and-forward environment or to a VoIP dial peer in a T.38 fax relay environment. The script automatically appends a prefix to the dialed digits for the fax call, allowing the router to match the call to the appropriate user-defined dial peer based on its "new" destination pattern.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **application**
4. **service** *service-name location*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**application** **Example:** `Router(config)# application`	Enters application configuration mode to configure voice applications and services.
Step 4	**service** *service-name location* **Example:** `Router(config-app)# service fax_detect flash:app_fax_detect.2.1.2.2.tcl`	Loads a VoiceXML document or Tcl script and defines its application name. • *service name location* --Directory and filename of the Tcl script or VoiceXML document in URL format. For example, Flash memory (flash:filename), a TFTP (tftp://../filename) or an HTTP server (http://../filename) are valid locations.

How to Configure Fax Detection for a Voice Gateway

Use the following tasks to configure the fax detection application on the voice gateway:

Note Starting with Cisco IOS Release 12.3(14)T, the **call application voice** configuration commands were restructured. This application guide uses the new command structure.

Note These configuration tasks assume that your network uses separate routers for a voice gateway running a TCL IVR script and for a remote, terminating gateway. For smaller networks that use a single router for both of these functions, configure the following tasks on the same router.

Configuring Fax Detection on the Voice Gateway Running a TCL IVR Script

Perform the following task to configure fax detection on the voice gateway running a TCL IVR script.

Note The commands in this section configure an IVR application, and they are not supported by Cisco IOS help. If you type **param mode ?**, for example, the Cisco IOS help does not supply a list of entries that are valid in place of the question mark, because the IVR application commands pass parameters to the named TCL script, rather than to the Cisco IOS software.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **application**
4. **service** *service-name location*
5. **param mode** {**connect-first** | **default-fax** | **default-voice** | **listen-first**}
6. **param prompt** *prompt-url*
7. **param voice-dtmf** {**0**|**1**|**2**|**3**|**4**|**5**|**6**|**7**|**8**|**9**|*|#}
8. **param fax-dtmf** {**0**|**1**|**2**|**3**|**4**|**5**|**6**|**7**|**8**|**9**|*|#}
9. **param fax-prefix** {**0**|**1**|**2**|**3**|**4**|**5**|**6**|**7**|**8**|**9**|*|#}
10. **param account-id-method** {**none** | **ani** | **dnis** | **gateway**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**application** **Example:** `Router(config)# application`	Enters application configuration mode to configure voice applications and services.
Step 4	**service** *service-name location* **Example:** `Router(config-app)# service fax_detect flash:app_fax_detect.2.1.2.2.tcl`	Loads a VoiceXML document or Tcl script and define its application name. • *service-name* --Name that identifies the voice application. This is a user-defined name and does not have to match the script name.

	Command or Action	Purpose
		• *location* --Directory and filename of the Tcl script or VoiceXML document in URL format. For example, Flash memory (flash:filename), a TFTP (tftp://../filename) or an HTTP server (http://../filename) are valid locations.
Step 5	**param mode** {**connect-first** | **default-fax** | **default-voice** | **listen-first**} **Example:** `Router(config-app)# param mode default-fax`	(Optional) Sets the mode of the fax detection application to one of the four available modes. • **connect-first** --Connects the call to the voice application and then listens for CNG. This is the default. • **default-fax** --Listens for CNG or DTMF and then connects; defaults to fax if no CNG or DTMF is heard • **default-voice** --Listens for CNG or DTMF and then connects; defaults to voice if no CNG or DTMF is heard • **listen-first** --Listens for CNG; if not detected, connects to voice.
Step 6	**param prompt** *prompt-url* **Example:** `Router(config-app)# param prompt tftp://BigServer/myscripts/detect.au`	(Optional) Specifies the audio file to use when the fax detection application is called. • *prompt-url* --URL or IFS on the TFTP server of the audio file containing the prompt. **Note** The audio file is used only in listen-first, default-voice, and default-fax modes.
Step 7	**param voice-dtmf** {**0**|**1**|**2**|**3**|**4**|**5**|**6**|**7**|**8**|**9**|*|#} **Example:** `Router(config-app)# param voice-dtmf 3`	(Optional) Specifies the key that a calling party should press to indicate a voice call when the fax detection application is operating in default-voice or default-fax mode. • **0** through **9**, *, #--Key to dial for a voice call. The default key is 1. **Note** This key must be different than the key configured for fax calls.
Step 8	**param fax-dtmf** {**0**|**1**|**2**|**3**|**4**|**5**|**6**|**7**|**8**|**9**|*|#} **Example:** `Router(config-app)# param fax-dtmf 4`	(Optional) Specifies the key that a calling party should press to indicate a fax call when the fax detection application is operating in default-voice or default-fax mode. • **0** through **9**, *, #--Key to dial for a fax call. The default key is 2.

	Command or Action	Purpose
		Note This key must be different than the key configured for voice calls.
Step 9	**param fax-prefix** {**0**|**1**|**2**|**3**|**4**|**5**|**6**|**7**|**8**|**9**|*|#} **Example:** `Router(config-app)# param fax-prefix 3`	(Optional) Specifies the key that is to be added to the called telephone number (DNIS) by the fax detection application when you want to direct a fax call as a T.38 fax relay session instead of a T.37 onramp session.
Step 10	**param account-id-method** {**none** | **ani** | **dnis** | **gateway**} **Example:** `Router(config-app)# param account-id-method ani`	(Optional) Specifies the method to assign an account identifier for the fax detection application. • **none** --No account identifier is assigned. This is the default. • **ani** --Calling telephone number is the account identifier. • **dnis** --Called telephone number is the account identifier. • **gateway** --Gateway host and domain names form the account identifier.

Configuring Dial Peers on the Voice Gateway Running a TCL IVR Script

Configuration of dial peers for fax detection is described in the following sections:

Configuring One or More Inbound POTS Dial Peers

The purpose of configuring inbound POTS dial peers on the on-ramp gateway is to associate a destination pattern and call type with each incoming call so that the call is properly routed to an outbound dial peer. The fax detection application is enabled on inbound POTS dial peers to assign call types by distinguishing between fax and voice calls.

Note When configuring store-and-forward fax on on-ramp gateways that have voice DSPs, do not configure the **information-type fax** command on the POTS dial peer. If this command is configured, fax calls fail.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **pots**
4. **application** *application-name*
5. **direct-inward-dial**
6. **incoming called-number** *string*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **pots** **Example:** `Router(config)# dial-peer voice 77 pots`	Enters dial-peer configuration mode and defines a local dial peer that directs traffic to or from a POTS interface. • *tag* --Dial-peer identifier that consists of one or more digits. Range: 1 to 2147483647. • **pots** --Specifies that this dial peer directs traffic to or from a POTS interface.
Step 4	**application** *application-name* **Example:** `Router(config-dial-peer)# application detect-app`	Associates the fax detection application with the dial peer.
Step 5	**direct-inward-dial** **Example:** `Router(config-dial-peer)# direct-inward-dial`	Enables the Direct Inward Dialing (DID) call treatment for incoming called numbers, in which the entire incoming dial string is used to find a matching outbound dial peer. The gateway does not present a dial tone to the caller and does not collect digits; the setup message contains all the digits necessary to route the call.
Step 6	**incoming called-number** *string* **Example:** `Router(config-dial-peer)# incoming called-number 14085557896`	Defines the called number (dialed number identification service or DNIS) string. The called number is used to match the incoming call leg to an inbound dial peer. • *string* --Incoming called telephone number. Valid entries are any series of digits that specify the E.164 telephone number.

Configuring One or More Outbound VoIP Dial Peers for Voice

The purpose of configuring an outbound VoIP dial peer is to provide call handling for voice calls that enter the packet network. The outbound VoIP dial peer for voice defines the characteristics of the IP connection between the gateway and the voice messaging application or IP voice path.

Note If you already configured an outgoing VoIP dial peer for voice calls with the appropriate destination pattern when you set up your VoIP network, you do not have to configure another dial peer for voice calls; there are no different parameters for the fax detection application.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **voip**
4. **destination-pattern** [+]*string*[**T**]
5. **dtmf-relay h245-signal**
6. **fax rate disable**
7. **session target** {**ipv4:** *destination-address* | **dns:**{**d.**| **e.** | **s.** | **u.**}*host-name*} | **ras**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 37 voip`	Enters dial-peer configuration mode and defines a dial peer that directs traffic to or from a packet network. • *tag* --Dial-peer identifier that consists of one or more digits. Range: 1 to 2147483647. • **voip** --Calls from this dial peer use voice encapsulation on the packet network.
Step 4	**destination-pattern** [+]*string*[**T**] **Example:** **Example:** `Router(config-dial-peer)# destination-pattern 14085556688`	Specifies a pattern that represents either the prefix or the full E.164 telephone number (depending on your dial plan) that identifies the destination telephone number. This pattern of numbers should fall within the pattern of numbers that was configured as the incoming called number on the inbound POTS dial peer. • + --(Optional) Plus sign indicates that an E.164 standard number follows. The plus sign (+) is not supported on the Cisco MC3810.

	Command or Action	Purpose

		• *string* --E.164 or private dialing plan telephone number. Valid entries are the digits 0 through 9, the letters A through D, and the following special characters:
		  • Asterisk (*) and pound sign (#) that appear on standard touch-tone dial pads. These characters cannot be used as leading characters in a string (for example, *650).
		  • Comma (,), which inserts a pause between digits.
		  • Period (.), which matches any entered digit (this character is used as a wildcard). The period cannot be used as a leading character in a string (for example, .650).
		• **T** --(Optional) Timer, or control, character indicates that the destination-pattern value is a variable-length dial string. Instructs the router to collect dialed digits until the interdigit timer expires (10 seconds, by default) or until a termination character (#, by default) is dialed. The timer character must be a capital T.

Step 5	**dtmf-relay h245-signal** **Example:** `Router(config-dial-peer)# dtmf-relay h245-signal`	Forwards dual tone multifrequency (DTMF) tones by using the H.245 "signal" User Input Indication method to compress the tones at one end of the call and decompress them at the other end. Supports tones 0 through 9, *, #, and A through D.
Step 6	**fax rate disable** **Example:** `Router(config-dial-peer)# fax rate disable`	Disables fax relay transmission capability on this dial peer.
Step 7	**session target** {**ipv4:** *destination-address* | **dns:**{**d.**| **e.** | **s.** | **u.**}*host-name*} | **ras**} **Example:** `Router(config-dial-peer)# session target dns: $d$.faxserver.abcinc.com`	Designates a network-specific address to receive calls from this dial peer. • **ipv4:** --Argument that follows is an IP address. • *destination-address* --String that contains the IP address of the network-specific address to receive calls from this dial peer. • **dns:** --Argument that follows is a router host name to be resolved by the domain name server. • **d.** --Wildcard to be replaced by the destination (called) number, followed by a period (.). • **e.** --Wildcard to be replaced by the digits in the called number in reverse order with periods added between the digits, followed by a period (.).

	Command or Action	Purpose
		• **s.** --Wildcard to be replaced by the source destination pattern, followed by a period (.). • **u.** --Wildcard to be replaced by the unmatched portion of the destination pattern (such as a defined extension number), followed by a period (.). • *host-name* --String that contains the host name of the network-specific address to receive calls from this dial peer. • **ras** --(H.323 only) Registration, Admission, and Status (RAS) signaling function protocol is being used, and a gatekeeper should be consulted to translate the E.164 address into an IP address.

Configuring One or More Outbound VoIP Dial Peers for T.38 Fax Relay

The purpose of configuring an outbound VoIP dial peer for T.38 fax relay is to enable call handling from the voice gateway running a TCL IVR script to a destination in the packet network. For fax relay, this destination is typically an incoming dial peer on a remote, terminating gateway. If you are configuring T.38 fax relay as the fax component of your fax detection application, see the "Configuring One or More Individual VoIP Dial Peers for T.38 Fax Relay" section on page 10 .

Configuring One or More Outbound MMoIP Dial Peers for T.37 Store-and-Forward Fax

The purpose of configuring an outbound MMoIP dial peer for store-and-forward fax is to enable call handling from the voice gateway running a TCL IVR script to a destination in the packet network. For store-and-forward fax, this destination is typically an SMTP or ESMTP server.

Terminating a Fax Detection Call

The fax detection application requires that you configure a remote, terminating gateway if you are handling calls that exit the packet network to the PSTN, as follows:

- Voice calls--If you have voice calls that are not terminated on the packet network, configure inbound dial VoIP dial peers and outbound POTS dial peers on a gateway using standard commands for voice networks.
- Fax relay calls--If you have fax relay calls that are exiting the packet network to the PSTN, follow the instructions for configuring a gateway in the chapter “Configuring T.38 Fax Relay.”
- Store-and-forward fax calls--If you have store-and-forward fax calls that are exiting the packet network to the PSTN, follow the instructions for configuring an off-ramp gateway in the chapter “Configuring T.37 Store-and-Forward Fax.”

Troubleshooting Tips

Use the following tips to help resolve problems that keep fax detection from working correctly.

- Ensure that you are using a Cisco IOS software release that supports fax detection. For more information, see Cisco Feature Navigator at http://www.cisco.com/go/fn.

- Before configuring fax detection, make sure that your voice application is functional by putting a series of calls through.
- Before configuring fax detection, make sure that your fax application is functional by sending a series of faxes.
- After configuring fax detection, issue the **debug voip ivr script** command to display debug information from the fax detection script. Then, put through a series of voice calls and fax calls to ensure correct operation. The debug output that is displayed when you put calls through is indispensable for diagnosing failing calls and finding the source of a problem. It is the only way to verify that parameters are set to the values that you want and that they are actually taking effect. Also note that mistakes such as typing errors in command-line interface (CLI) parameters (for example, typing "moode" for "mode") are not recognized as errors by Cisco IOS software. They are accepted without complaint when typed, yet cannot have the desired effect during operation. It is only by watching the debug output during operation that you find these mistakes.
- Make sure that you have configured different DTMF digits for fax and for voice. If you configure both to be the same number, you are not notified immediately as with other Cisco IOS command errors. You find this error only if the **debug voip ivr script** command is enabled before a failing call comes in.

Use the following **show** commands to troubleshoot fax detection:

- **show dial-peer voice** [*tag*] [**summary**]--Displays configuration information for MMoIP, VoIP, and POTS dial peers to help you verify that dial peers are properly configured for all legs of voice and fax calls.
- **show call application voice summary** --Lists all voice applications that are loaded on the router to help you confirm that the scripts that you are interested in are loaded.
- **show call application voice** *application-name* --Displays the line-by-line contents of the TCL script associated with the specified application.

Configuration Example for Fax Detection

Fax Detection Example

This example uses both fax relay and store-and-forward fax on different dial peers. It is a basic configuration for T1 fax detection for incoming calls to any 4-digit DNIS with the leading digit 7. The mode is default-fax, an audio file that contains a voice prompt and DTMF digits to select voice and fax routing is specified, and the application is called fax_detect on the gateway. The account identifier is the router-specific name derived from the host name and domain name. Two fax applications have been configured, and calls are routed to one or the other based on dialed number (DNIS). One fax application is fax relay, which is configured on an outbound VoIP dial peer; the other is store-and-forward fax, which has been configured on an outbound MMoIP dial peer.

A gateway with this configuration handles voice and fax calls as follows:

- Answers all calls to 7xxx (4-digit DNIS starting with 7) with the fax_detect application.
- Routes voice calls with 4-digit DNIS of 7xxx to VoIP dial peer 2 (voice).
- Routes fax calls with 4-digit DNIS of 71xx to MMoIP dial peer 3 (store-and-forward).
- Routes fax calls with 4-digit DNIS of 72xx to VoIP dial peer 4 (fax relay).

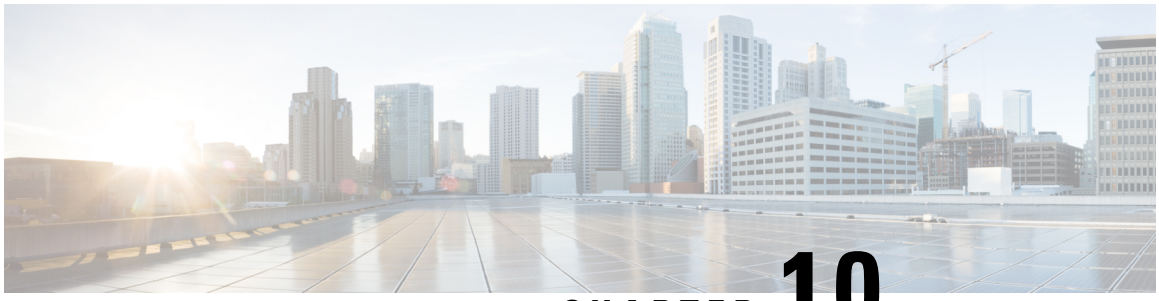
This example includes configuration of a unified communications (UC) server and a gatekeeper, which is described in the *Cisco IOS H.323 Configuration Guide* .

```
!
version 12.1
service timestamps debug datetime localtime
service timestamps log datetime localtime
no service password-encryption
!
hostname zebra
!
!
resource-pool disable
!
!
clock timezone AEST 10
ip subnet-zero
ip domain-name cisco.com
!
isdn switch-type primary-5ess
call rsvp-sync
!
! IVR script configuration for fax detection
application
service
application voice fax_detect tftp://10.1.1.1/eng/tcl/app_fax_detect.2.1.2.3.tcl
call application voice fax_detect prompt tftp://10.1.1.1/eng/prompts/en_default_fax.au
call application voice fax_detect mode default-fax
call application voice fax_detect voice-dtmf 1
call application voice fax_detect fax-dtmf 2
call application voice fax_detect account-id-method gateway
cns event-service server
!
!
fax receive called-subscriber $d$
fax send transmitting-subscriber $s$
fax send left-header $s$
fax send center-header $t$
fax send right-header Page $p$
fax send coverpage enable
fax send coverpage email-controllable
fax send coverpage comment Cisco cover page comment
fax interface-type vfc
mta send server 172.16.1.25
mta send subject Test Message
mta send origin-prefix Cisco Fax
mta send postmaster postmaster@mail-server.unified-messages.com
mta send mail-from hostname zebra.unified-messages.com
mta send mail-from username $s$
mta send return-receipt-to username $s$
mta receive aliases sydney.com
mta receive maximum-recipients 120
mta receive generate-mdn
!
!
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 pri-group timeslots 1-24
!
controller T1 1
 framing esf
```

```
 clock source line secondary 1
 linecode b8zs
 pri-group timeslots 1-24
!
controller T1 2
 framing esf
 clock source line secondary 2
 linecode b8zs
 pri-group timeslots 1-24
!
controller T1 3
 clock source line secondary 3
!
controller T1 4
 clock source line secondary 4
!
controller T1 5
 clock source line secondary 5
!
controller T1 6
 clock source line secondary 6
!
controller T1 7
 clock source line secondary 7
!
!
interface Ethernet0
 ip address 10.2.14.90 255.0.0.0
!
interface Serial0
 no ip address
 no ip mroute-cache
 shutdown
 no fair-queue
 clockrate 2015232
!
interface Serial1
 no ip address
 shutdown
 no fair-queue
 clockrate 2015232
!
interface Serial2
 no ip address
 shutdown
 no fair-queue
 clockrate 2015232
!
interface Serial3
 no ip address
 shutdown
 no fair-queue
 clockrate 2015232
!
interface Serial0:23
 no ip address
 ip mroute-cache
 isdn switch-type primary-5ess
 isdn incoming-voice modem
 isdn T203 10000
 no cdp enable
!
interface Serial1:23
 no ip address
```

```
 isdn switch-type primary-5ess
 isdn incoming-voice modem
 no cdp enable
!
interface Serial2:23
 no ip address
 isdn switch-type primary-5ess
 isdn incoming-voice modem
 isdn guard-timer 3000
 isdn T203 10000
 no cdp enable
!
interface FastEthernet0
 ip address 172.16.14.90 255.255.0.0
 duplex auto
 speed auto
 h323-gateway voip interface
 h323-gateway voip h323-id 5300-voip
 h323-gateway voip tech-prefix 2#
!
ip classless
no ip http server
!
!
voice-port 0:D
!
voice-port 1:D
!
voice-port 2:D
!
! POTS dial-peer configuration for fax detection
dial-peer voice 1 pots
 application fax_detect
 incoming called-number 7...
 direct-inward-dial
!
! Voice dial-peer configuration for fax detection
dial-peer voice 2 voip
 destination-pattern 7...
 session target ras
 tech-prefix 5#
 dtmf-relay h245-signal
 codec g711ulaw
 fax rate disable
 no vad
!
! Store-and-forward fax dial-peer configuration for fax detection
dial-peer voice 3 mmoip
 application fax_on_vfc_onramp_app out-bound
 destination-pattern 71..
 information-type fax
 session target mailto:$d$@mail-server.unified-messages.com
!
! Fax relay dial-peer configuration for fax detection
dial-peer voice 4 voip
 destination-pattern 72..
 session target ras
 tech-prefix 3#
!
gateway
!
!
line con 0
 exec-timeout 0 0
```

```
 transport input none
line aux 0
line vty 0 4
 login
!
ntp clock-period 17180419
ntp source Ethernet0
ntp server 10.1.1.1
end
```



CHAPTER 10

Configuring Fax Rollover

Configuring Fax Rollover

This chapter describes configuration for fax rollover on an IP network. Fax rollover occurs when a T.38 fax is configured to roll over to a T.37 fax session when the far end is busy or unreachable.

History for the Fax Rollover Feature

Release	Modification
12.0(7)T	This feature was implemented for VoIP on the Cisco AS5300 and Cisco AS5800.
12.2(4)T	Keywords were added for more disconnect cause codes.
12.3(14)T	A new command-line interface structure for configuring Tcl and IVR applications was introduced and affected the commands for configuring this feature.
12.4(4)T	This feature was integrated into Cisco IOS release 12.4(4)T.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn . You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring Fax Rollover

This section describes prerequisites for configuring fax rollover.

- Configure your IP network and ensure that it is operational.
- Text fax relay and ensure that it is operational on the IP network. By making sure that fax relay is operational before beginning to configure the fax rollover application, you can keep fax configuration issues separate and make troubleshooting easier.
- Test the store-and-forward fax application and ensure that it is operational on the IP network with a Simple Mail Transfer Protocol (SMTP) or an Extended Simple Mail Transfer Protocol (ESMTP) mail server.

Restrictions for Configuring Fax Rollover

The following restriction applies to fax rollover:

- For TI-549 DSPs, only high-complexity VCWare is supported.

Information About Fax Rollover

The on-ramp gateway receives fax calls at an E.164 number. The gateway attempts to route fax calls using fax relay. If the attempt fails, the call is forwarded to an SMTP server by a mail transfer agent (MTA) using T.37-standard protocols for store-and-forward fax.

Fax rollover is configured by installing the TCL IVR rollover application to the on-ramp gateway and adding the application to the POTS dial peer that answers T.38 calls.

The TCL IVR application has a procedure for setting up the call, waiting for success, and, upon receiving a busy or gateway-down message, setting up the same call again with new destination parameters. When the call is returned to the originating gateway, the gateway searches for a new VoIP dial peer with the same destination number, and a preference equal to or greater than the first dial peer that it found. If it finds one, it sets up the call again.

Dial peers for the fax rollover application include at least one inbound dial peer to receive calls from the PSTN and at least two outbound dial peers, one for fax relay and one for store-and-forward fax.

The inbound dial peer describes the inbound call leg from the telephony connection to the gateway and is called a plain old telephone service (POTS) dial peer. POTS dial peers define the characteristics of the telephony (PSTN) connection between the sending fax device or voice instrument and the gateway to the IP network. In general, the gateway uses the line characteristics defined by POTS dial peers to determine call type and call destination.

The gateway then finds an outbound dial peer whose configured parameters match these attributes and routes the call to it. You can establish more than one POTS dial peer if you want different incoming calls to receive different handling. The fax rollover application is enabled on the inbound dial peer.

One of the two types of outbound dial peers in the gateway router is the Voice-over-IP (VoIP) dial peer, which describes the fax relay call leg that is outbound from the router.

The second type of outbound dial peer on the on-ramp gateway is the Multimedia-Mail-over-IP (MMoIP) dial peer, which describes an IP call leg for store-and-forward fax. The MMoIP dial peer is configured with

the fax_on_vfc_onramp_app IVR application in the outbound mode, which is the standard configuration for store-and-forward fax.

How to Download the Fax Rollover Application File

This section describes how to download the TCL script and default audio prompt files used with the fax rollover application. You must download these files before you can configure the fax rollover application. The script is contained in a zip file on Cisco.com.

The Cisco IOS File System (IFS) reads the files, so any IFS-supported URL can be used as a location for the files. URLs can include TFTP, FTP, or a pointer to a device on the router. For more information, see the TCL IVR API Version 2.0 Programmer's Guide.

SUMMARY STEPS

1. Log in to the Cisco website and go to http://www.cisco.com/cgi-bin/tablebuild.pl/tclware.
2. Select and download this zip file: TCLware.2.0.1.zip.
3. Unzip the files.
4. Move the application script file to a location that can be accessed by your gateway using a URL address.

DETAILED STEPS

Step 1 Log in to the Cisco website and go to http://www.cisco.com/cgi-bin/tablebuild.pl/tclware.

When you are logged in to the Cisco website, you can navigate to the TCLWare page from the Cisco home page by following this path: Technical Support / Software Center / Access Software / TCLWare.

Step 2 Select and download this zip file: TCLware.2.0.1.zip.

When you are asked, provide the following information:

- Cisco Connection Online (CCO) server nearest your physical location
- Where to save the files on your disk

Step 3 Unzip the files.

The zip file that you download includes these files:

- Fax rollover application TCL script file
- README file

Step 4 Move the application script file to a location that can be accessed by your gateway using a URL address.

The URL of a TCL script is a standard URL that points to the location of the script. Examples include the following:

- flash:myscript.tcl--The script called myscript.tcl is located in Flash memory on the router.
- slot0:myscript.tcl--The script called myscript.tcl is located in a device in slot 0 on the router.
- tftp://BigServer/myscripts/MouseTrap.tcl--The script called MouseTrap.tcl is located in a server called BigServer in a directory within the tftpboot directory called myscripts.

Note Flash memory is limited to 32 entries, which may prevent your loading all TCL and audio files there.

How to Configure Fax Rollover

Use the following tasks to configure fax rollover on an on-ramp gateway:

Note The instructions in this chapter assume that your packet network includes separate routers for on-ramp and off-ramp functions. For smaller networks that use a single router for both on-ramp and off-ramp functionality, follow both the on-ramp and the off-ramp instructions on the same router.

Loading the Fax Rollover Application on the Gateway

Fax rollover is an IVR application that is written in a TCL script. The script must be downloaded from Cisco.com and installed on your network before the fax rollover application can be loaded on the gateway. See the How to Download the Fax Rollover Application File, on page 189.

Install the script at a location that is accessible by the gateway and load it using a name of your choice. All later commands that refer to the fax rollover application use the name you selected when loading the the application on the gateway.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **application**
4. **service** *service-name location*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**application** **Example:** `Router(config)# application`	Enters application configuration mode to configure voice applications and services.

	Command or Action	Purpose
Step 4	**service** *service-name location* **Example:** `Router(config-app)# service rollover-app tftp://BigServer/myscripts/fax_roll_2.1.2.0.tcl`	Indicates the location or URL of the TCL script to be used for the fax rollover application. • *service-name location* --Directory and filename of the Tcl script or VoiceXML document in URL format. For example, Flash memory (flash:filename), a TFTP (tftp://../filename) or an HTTP server (http://../filename) are valid locations.

Configuring Dial Peers

Configuration of dial peers for fax rollover is described in the following sections:

Configuring Inbound POTS Dial Peers

The inbound POTS dial peers associates a destination pattern and call type with each incoming call so that the call is properly routed to an outbound dial peer. The fax rollover application is enabled on the inbound POTS dial peer.

Note When configuring store-and-forward fax on on-ramp gateways with voice DSPs, do not configure the **information-type fax** command on the POTS dial peer. If this command is configured, fax calls fail.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **pots**
4. **application** *application-name*
5. **direct-inward-dial**
6. **incoming called-number** *string*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**dial-peer voice** *tag* **pots** **Example:** `Router(config)# dial-peer voice 77 pots`	Enters dial-peer configuration mode and defines a local dial peer that directs traffic to or from a POTS interface. • *tag* --Dial-peer identifier that consists of one or more digits. Valid entries are from 1 to 2147483647. • **pots** --This dial peer directs traffic to or from a POTS interface.
Step 4	**application** *application-name* **Example:** `Router(config-dial-peer)# application rollover-app`	Associates the fax rollover application with the dial peer. • *application-name* --Name that was defined for the fax rollover application in Loading the Fax Rollover Application on the Gateway, on page 190.
Step 5	**direct-inward-dial** **Example:** `Router(config-dial-peer)# direct-inward-dial`	Enables the Direct Inward Dialing (DID) call treatment for incoming called numbers, in which the entire incoming dial string is used to find a matching outbound dial peer. The gateway does not present a dial tone to the caller and does not collect digits; the setup message contains all the digits necessary to route the call.
Step 6	**incoming called-number** *string* **Example:** `Router(config-dial-peer)# incoming called-number 14085557896`	Defines the called number (dialed number identification service or DNIS) string. The called number is used to match the incoming call leg to an inbound dial peer. • *string* --Incoming called telephone number. Valid entries are any series of digits that specify the E.164 telephone number.

Configuring One or More Outbound VoIP Dial Peers for T.38 Fax Relay

The purpose of configuring an outbound VoIP dial peer for T.38 fax relay is to enable call handling from the on-ramp gateway to a destination in the packet network. For fax relay, this destination is typically an incoming dial peer on an off-ramp gateway. If you are configuring T.38 fax relay as the fax component of your fax detection application, see the "Configuring One or More Individual VoIP Dial Peers for T.38 Fax Relay" section on page 10 .

Configuring One or More Outbound MMoIP Dial Peers for T.37 Store-and-Forward Fax

The purpose of configuring an outbound MMoIP dial peer for store-and-forward fax is to enable call handling from the on-ramp gateway to a destination in the packet network. For store-and-forward fax, this destination is typically an SMTP or ESMTP server.

Troubleshooting Tips

Use the following commands to troubleshoot fax rollover:

- **show dial-peer voice** [*tag*] [**summary**]--Displays configuration information for MMoIP, VoIP, and POTS dial peers to help you verify that dial peers are properly configured for all legs of voice and fax calls.

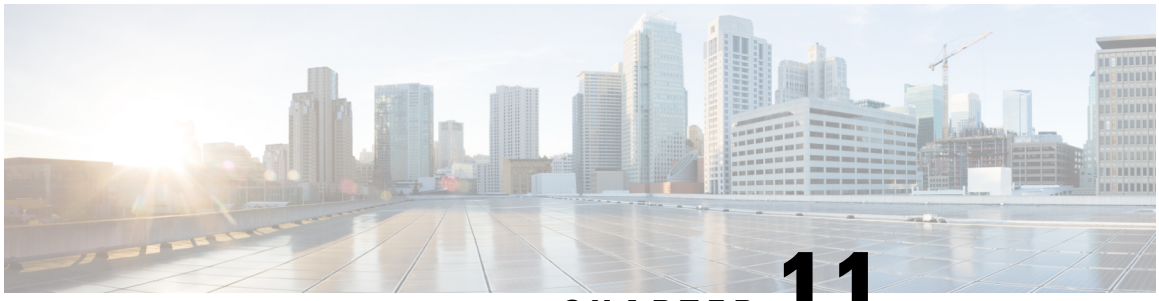
- **show call application voice summary** --Lists all voice applications that are loaded on the router to help you confirm that the scripts that you are interested in are loaded.

Configuration Example for Fax Rollover

T.38 Fax Rollover to T.37 Example

The following example shows dial peers configured for T.38 fax rollover to T.37 fax.

```
.
.
voice hunt user-busy
!
! Inbound peer for T.38/T.37 on-ramp rollover operation.
! This peer includes the TCL application for rollover operation.
dial-peer voice 70 pots
 application app_lib_rollover
 incoming called-number 5......
 port 1/1:0
!
! Outbound peer for T.38 ingress gateway.
! This peer requires a lower preference number than the next matching peer.
dial-peer voice 71 voip
 preference 1
 destination-pattern 5550119
 session target ipv4:10.14.120.109
 fax protocol t38 ls_redundancy 0 hs_redundancy 0
!
! Outbound peer for T.37 on-ramp operation.
dial-peer voice 72 mmoip
 preference 2
! The application name below must be exactly as shown!
 application fax_on_vfc_onramp_app out-bound
 destination-pattern 5550119
 session target mailto:$d$@mail-server.cisco.com
 information-type fax
```



CHAPTER 11

Monitoring of Modem Call Status

Monitoring of Modem Call Status

This appendix describes configuration for modem call status. Modem call status provides monitoring and maintaining of modem calls at digital signal level zero (DS-0), the PRI bearer channel level, and the modem level.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring Modem Call Status

Before configuring your access server or gateway to enable monitoring of modem call status, perform the following tasks:

- Install the SNMP manager on your workstation.
- Configure the SNMP agent on the access server with the following commands:

```
snmp-server
 community

public
 RO
snmp-server
 host

10.1.2.3
 public
```

Information about Modem Call Status

Modem call status is supported by:

- The generation of DS-0 busyout traps
- The generation of ISDN PRI-requested channel-not-available traps
- The generation of modem health traps
- Using the **show controllers** command
- DS-1 loopback traps

Monitoring and maintaining of modem call status offers the following benefits:

- Improved visibility into the line status of the access server for comprehensive status monitoring and notification capability
- Improved troubleshooting and diagnostics for large dial networks

DS-0 Busyout Traps

A DS-0 busyout trap is generated when one of the following conditions is met:

- A request occurs to busy out a DS-0
- A busyout is complete and the DS-0 is out of service
- A request occurs to take a DS-0 out of busyout mode

DS-0 busyout traps are generated at the DS-0 level for channel-associated signalling (CAS) and ISDN configured lines.

ISDN PRI-Requested Channel-Not-Available Traps

ISDN PRI-requested channel-not-available traps are generated when a requested DS-0 channel is not available or when there is no modem available to take an incoming call. This feature is available only on ISDN PRI interfaces.

Modem Health Traps

Modem health traps are generated when a modem port is bad, disabled, reflashed, or shut down, or when there is a request to busy out the modem.

show controllers timeslots Command

The **show controllers** command, with the keyword **timeslots,** displays the channel state in detail. This command shows whether the DS-0 channels of a particular controller are in idle, in-service, maintenance, or busyout states. The **show controllers** command applies to both CAS and ISDN PRI interfaces.

DS-1 Loopback Traps

DS-1 loopback traps are generated when a DS-1 line goes into loopback mode.

Configuring Modem Call Status

To configure modem call status on your access server or gateway, perform the following tasks, all of which are optional:

Note For a complete description of the commands, refer to the Cisco IOS Voice, Video, and Fax Command Reference. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

Enabling DS-0 Busyout Traps

To generate DS-0 busyout traps, use the following command in global configuration mode:

Command	Purpose
`Router(config)# snmp-server enable traps ds0-busyout`	Generates a trap when there is a request to busy out a DS-0 or when busyout finishes. DS-0 busyout traps are disabled by default. The **ds0-busyout** keyword specifies that DS-0 busyout traps be enabled.

Enabling ISDN PRI-Requested Channel-Not-Available Traps

To generate ISDN PRI-requested channel-not-available traps, use the following command in global configuration mode:

Command	Purpose
`Router(config)# snmp-server enable traps isdn chan-not-avail`	Generates a trap when the network access server (NAS) rejects an incoming call on an ISDN PRI interface because the channel is not available. ISDN PRI-requested channel-not-available traps are disabled by default. The **isdn chan-not-avail** keywords specify that ISDN PRI-requested channel-not-available traps be enabled.

Enabling Modem Health Traps

To generate modem health traps, use the following command in global configuration mode:

Command	Purpose
`Router(config)# snmp-server enable traps modem-health`	Generates a trap when a modem port is bad, disabled, or downloading firmware; when a download fails; when a modem is placed in loopback mode for maintenance; or when there is a request to busy out the modem. Modem health traps are disabled by default. The **modem-health**keyword specifies that modem health traps be enabled.

Enabling DS-1 Loopback Traps

To generate DS-1 loopback traps, use the following command in global configuration mode:

Command	Purpose
`Router(config)# snmp-server enable traps ds1-loopback`	Generates a trap when the DS-1 line goes into loopback mode. DS-1 loopback traps are disabled by default. The **ds1-loopback** keyword specifies that DS-1 loopback traps be enabled.

Verifying Enabled Traps

Use the **show running-config** command to verify that the traps are enabled. The following output indicates that all the traps are enabled:

```
.
Router(config)# show running-config
snmp-server enable traps ds0-busyout
snmp-server enable traps isdn chan-not-avail
snmp-server enable traps modem-health
snmp-server enable traps ds1-loopback
.
```

Troubleshooting Enabled Traps

To troubleshoot the traps, enable debugging for SNMP packets by entering the **debug snmp packets** command in privileged EXEC mode. Check the resulting output to see that the SNMP trap information packet is being sent. The output will vary according to the kind of packet sent or received.

The following example shows the **debug snmp packets**command followed by an excerpt from the debug output. The first and last lines of the sample output show SNMP trap packets that have been sent and received.

```
Router# debug snmp packets
SNMP: Packet received via UDP from 10.5.4.1 on Ethernet0
SNMP: Get-next request, reqid 23584, errstat 0, erridx 0
sysUpTime = NULL TYPE/VALUE
 system.1 = NULL TYPE/VALUE
 system.6 = NULL TYPE/VALUE
SNMP: Response, reqid 23584, errstat 0, erridx 0
 sysUpTime.0 = 2217027
 system.1.0 = Cisco Internetwork Operating System Software
 system.6.0 =
SNMP: Packet sent via UDP to 10.5.4.1
```

You can also use trap monitoring and logging tools such as **snmptrapd** with debugging flags turned on to monitor output.

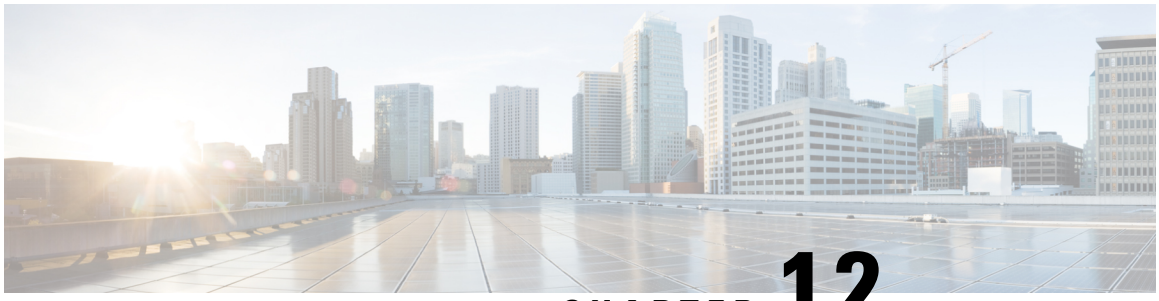
Modem Call Status Configuration Example

The following example shows modem call status configured with DS-0 busyout traps enabled:

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname router
!
aaa new-model
```

```
aaa authentication ppp default group radius
enable password <password>
!
spe 1/0 1/7
 firmware location system:/ucode/mica_port_firmware
spe 2/0 2/7
 firmware location system:/ucode/mica_port_firmware
!
resource-pool disable
!
clock timezone PDT -8
clock calendar-valid
no modem fast-answer
modem country mica usa
modem link-info poll time 60
modem buffer-size 300
ip subnet-zero
!
isdn switch-type primary-5ess
isdn voice-call-failure 0
!
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 pri-group timeslots 1-24
!
controller T1 1
 framing esf
 linecode b8zs
 ds0-group 0 timeslots 1-24 type e&m-fgb
 cas-custom 0
!
interface Loopback0
 ip address 10.5.4.1
!
interface Ethernet0
 no ip address
 shutdown
!
interface Serial0
 no ip address
 shutdown
!
interface Serial1
 no ip address
 shutdown
!
interface Serial0:23
 no ip address
 ip mroute-cache
 isdn switch-type primary-5ess
 isdn incoming-voice modem
 no cdp enable
!
interface FastEthernet0
 ip address 10.5.4.1
 duplex full
 speed auto
 no cdp enable
!
interface Group-Async1
 ip unnumbered FastEthernet0
 encapsulation ppp
```

```
 ip tcp header-compression passive
 no ip mroute-cache
 async mode interactive
 peer default ip address pool swattest
 no fair-queue
 ppp authentication chap
 ppp multilink
 group-range 1 192
!
interface Dialer1
 ip unnumbered FastEthernet0
 encapsulation ppp
 ip tcp header-compression passive
 dialer-group 1
 peer default ip address pool swattest
 pulse-time 0
 no cdp enable
!
ip local pool swattest 10.5.4.1
ip default-gateway 10.5.4.1
ip classless
!
dialer-list 1 protocol ip permit
snmp-server engineID local 00000000DDDDDDDDFFFFFFFF
snmp-server community public RO
snmp-server packetsize 2048
snmp-server enable traps pop
snmp-server host 10.5.4.1 public
!
radius-server host 10.5.4.1 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key <password>
!
line con 0
 transport input none
line 1 192
 autoselect ppp
 modem InOut
 transport preferred none
 transport input all
 transport output none
line aux 0
line vty 0 4
end
```



CHAPTER 12

RADIUS Vendor-Specific Attributes

The table below lists the supported vendor-specific options (subtype numbers from 3 through 21) that use IETF RADIUS attribute 26 and the Cisco vendor-ID company code of 9. These attributes are used with store-and-forward fax.

For more information, refer to the RADIUS Vendor-Specific Attributes appendix of the*Cisco IOS Security Configuration Guide.*

Table 9: RADIUS Vendor-Specific Attributes

Subtype Number	Attribute	Description
3	Cisco-Fax-Account-Id-Origin	Account ID origin as defined by the system administrator for the **mmoip aaa receive-id** or **mmoip aaa send-id** command.
4	Cisco-Fax-Msg-Id=	Unique fax message identification number assigned by store-and-forward fax.
5	Cisco-Fax-Pages	Number of pages sent or received during a fax session including cover pages.
6	Cisco-Fax-Coverpage-Flag	True/false flag that indicates whether a cover page was generated by the off-ramp gateway for this fax session. True indicates that a cover page was generated, and false indicates that a cover page was not generated.
7	Cisco-Fax-Modem-Time	Number of seconds it takes to send fax data (x) and to complete the entire fax session (y), which includes both fax-mail and PSTN time, in the form x/y. For example, 10/15 means that the transfer time took 10 seconds and that the full fax session took 15 seconds.
8	Cisco-Fax-Connect-Speed	Modem speed at which this fax mail was initially sent or received. Possible values are 1200, 4800, 9600, and 14400.
9	Cisco-Fax-Recipient-Count	Number of recipients for this fax transmission. Until e-mail servers support session mode, the number should be 1.

Subtype Number	Attribute	Description
10	Cisco-Fax-Process-Abort-Flag	True/false flag that indicates whether the fax session was aborted or successful. True indicates that the session was aborted, and false indicates that the session was successful.
11	Cisco-Fax-Dsn-Address	Address to which DSNs are sent.
12	Cisco-Fax-Dsn-Flag	True/false flag to indicate whether DSN is enabled. True indicates that DSN is enabled, and false indicates that DSN is not enabled.
13	Cisco-Fax-Mdn-Address	Address to which MDNs are sent.
14	Cisco-Fax-Mdn-Flag	True/Flash flag to indicate whether MDN is enabled. True indicates that MDN is enabled, and false indicates that MDN is not enabled.
15	Cisco-Fax-Auth-Status	Indicates whether or not authentication for this fax session was successful. Possible values for this field are success, failed, bypassed, or unknown.
16	Cisco-Email-Server-Address	IP address of the e-mail server handling the on-ramp fax-mail message.
17	Cisco-Email-Server-Ack-Flag	Indicates that the on-ramp gateway has received a positive acknowledgment from the e-mail server accepting the fax-mail message.
18	Cisco-Gateway-Id	Name of the gateway that processed the fax session. The name appears in the following format: hostname.domain-name.
19	Cisco-Call-Type	Type of call activity: fax receive or fax send.
20	Cisco-Port-Used	Slot/port number used to send or receive this fax mail.
21	Cisco-Abort-Cause	If the fax session aborts, indicates the system component that signaled the abort. Examples of system components that could trigger an abort are FAP (Fax Application Process), TIFF (the TIFF reader or the TIFF writer), fax-mail client, fax-mail server, ESMTP client, or ESMTP server.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks

Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

- Finding Feature Information, on page 203
- RADIUS Vendor-Specific Attributes, on page 203

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

RADIUS Vendor-Specific Attributes

The table below lists the supported vendor-specific options (subtype numbers from 3 through 21) that use IETF RADIUS attribute 26 and the Cisco vendor-ID company code of 9. These attributes are used with store-and-forward fax.

For more information, refer to the RADIUS Vendor-Specific Attributes appendix of the*Cisco IOS Security Configuration Guide.*

Table 10: RADIUS Vendor-Specific Attributes

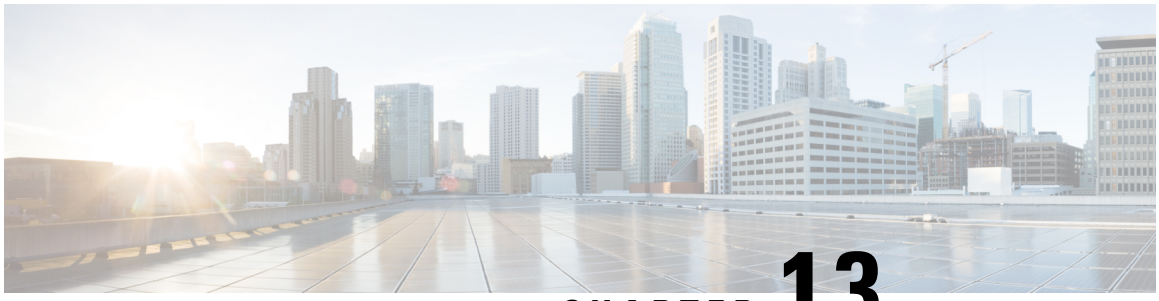
Subtype Number	Attribute	Description
3	Cisco-Fax-Account-Id-Origin	Account ID origin as defined by the system administrator for the **mmoip aaa receive-id** or **mmoip aaa send-id** command.
4	Cisco-Fax-Msg-Id=	Unique fax message identification number assigned by store-and-forward fax.
5	Cisco-Fax-Pages	Number of pages sent or received during a fax session including cover pages.
6	Cisco-Fax-Coverpage-Flag	True/false flag that indicates whether a cover page was generated by the off-ramp gateway for this fax session. True indicates that a cover page was generated, and false indicates that a cover page was not generated.
7	Cisco-Fax-Modem-Time	Number of seconds it takes to send fax data (x) and to complete the entire fax session (y), which includes both fax-mail and PSTN time, in the form x/y. For example, 10/15 means that the transfer time took 10 seconds and that the full fax session took 15 seconds.
8	Cisco-Fax-Connect-Speed	Modem speed at which this fax mail was initially sent or received. Possible values are 1200, 4800, 9600, and 14400.
9	Cisco-Fax-Recipient-Count	Number of recipients for this fax transmission. Until e-mail servers support session mode, the number should be 1.

RADIUS Vendor-Specific Attributes

Subtype Number	Attribute	Description
10	Cisco-Fax-Process-Abort-Flag	True/false flag that indicates whether the fax session was aborted or successful. True indicates that the session was aborted, and false indicates that the session was successful.
11	Cisco-Fax-Dsn-Address	Address to which DSNs are sent.
12	Cisco-Fax-Dsn-Flag	True/false flag to indicate whether DSN is enabled. True indicates that DSN is enabled, and false indicates that DSN is not enabled.
13	Cisco-Fax-Mdn-Address	Address to which MDNs are sent.
14	Cisco-Fax-Mdn-Flag	True/Flash flag to indicate whether MDN is enabled. True indicates that MDN is enabled, and false indicates that MDN is not enabled.
15	Cisco-Fax-Auth-Status	Indicates whether or not authentication for this fax session was successful. Possible values for this field are success, failed, bypassed, or unknown.
16	Cisco-Email-Server-Address	IP address of the e-mail server handling the on-ramp fax-mail message.
17	Cisco-Email-Server-Ack-Flag	Indicates that the on-ramp gateway has received a positive acknowledgment from the e-mail server accepting the fax-mail message.
18	Cisco-Gateway-Id	Name of the gateway that processed the fax session. The name appears in the following format: hostname.domain-name.
19	Cisco-Call-Type	Type of call activity: fax receive or fax send.
20	Cisco-Port-Used	Slot/port number used to send or receive this fax mail.
21	Cisco-Abort-Cause	If the fax session aborts, indicates the system component that signaled the abort. Examples of system components that could trigger an abort are FAP (Fax Application Process), TIFF (the TIFF reader or the TIFF writer), fax-mail client, fax-mail server, ESMTP client, or ESMTP server.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks

Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)



CHAPTER 13

V150.1 MER Modem Relay Support for TDM to SIP Gateway

V150.1 MER Modem Relay Support for TDM to SIP Gateway

The Cisco V.150.1 Minimum Essential Requirements feature complies with the requirements of the National Security Agency (NSA) SCIP-216 Minimum Essential Requirements (MER) for V.150.1 recommendation. This feature is added to support V.150.1 MER modem relay support on SIP gateways. This is of importance to establish secure calls as per V.150.1 MER specifications between two SIP gateways with the PSTN line side being T1/E1 CAS or PRI. Typically, specialized encryption-capable BRI/analog phones (STE) that can communicate over V.150.1 modem relay or over modem pass-through are used as endpoints.

Feature Information for Cisco V.150.1 MER Modem Relay Support for TDM to SIP Gateway

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Feature Name	Releases	Feature Information
V.150.1 MER Modem Relay Support for TDM to SIP Gateway	Cisco IOS 15.5(3)M	The V.150.1 MER Modem Relay Support for TDM to SIP Gateway feature is added to support V.150.1 MER modem relay support on SIP gateways with the PSTN line side being T1/E1 CAS or PRI. The following command was modified: **modem relay sse v150mer**.

Information on V150.1 MER Modem Relay Support for TDM to SIP Gateway

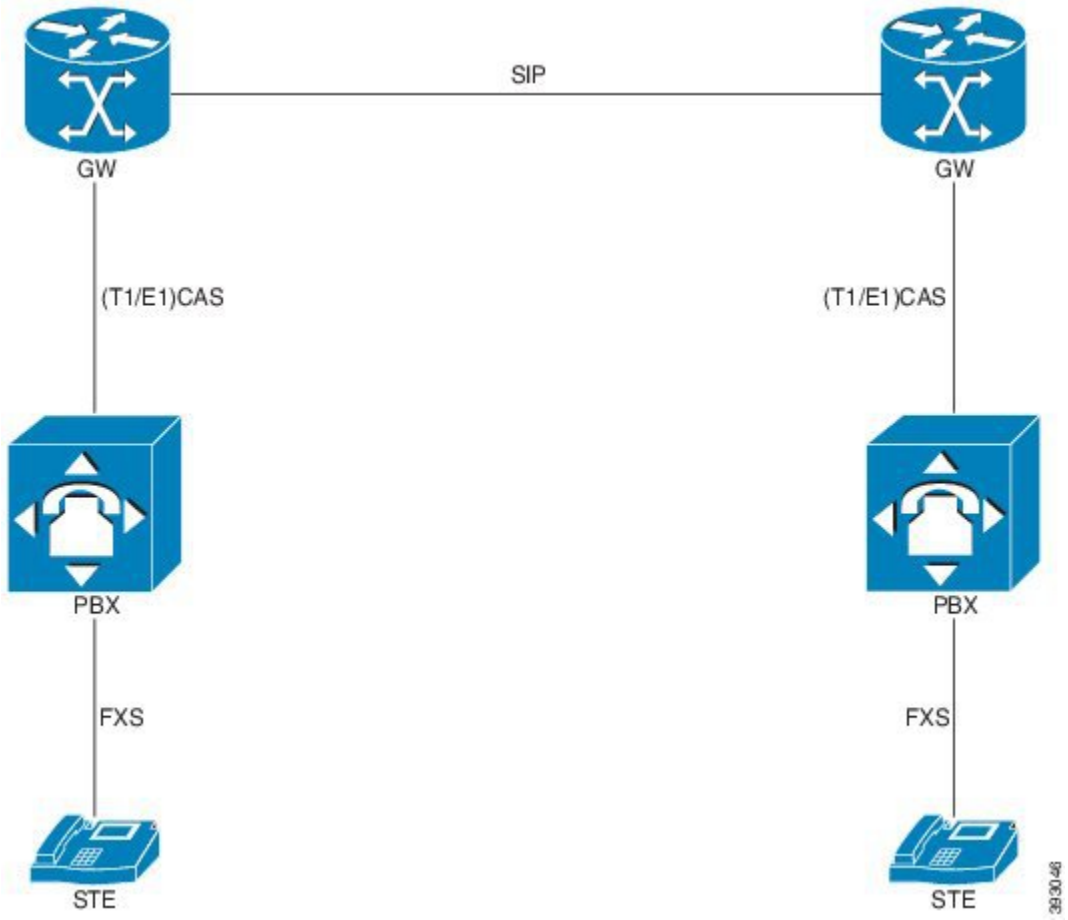
V150.1 MER Modem Relay Support for TDM to SIP Gateway

V.150.1 is an ITU standard for relaying modem or fax transmission that uses state signaling event (SSE) packets to trigger the transition from audio to modem-relay mode or fax-relay mode. The SSE headers are carried in the RTP packet. After call setup, in-band signaling through Simple Packet Relay Transport (SPRT) and SSE messages is used to transition from one state to another. SPRT packets (non-RTP packets) carry the data after the digital signal processor (DSP) transitions into modem relay mode.

In Cisco IOS Release 15.5(3)M, V150.1 MER Modem Relay support is provided on TDM to SIP gateways for placing secure calls between two SIP gateways with PSTN side being T1/E1 CAS or PRI. This feature provides only modem relay support as per the V.150.1 MER specifications.

Topology

Figure 9: Topology—V150.1 MER Modem Relay Support for TDM to SIP Gateway



Prerequisites for Cisco V.150.1 MER Modem Relay Support for TDM to SIP Gateway

- ISR-G2 routers must be installed on your network containing Cisco VWIC-xMFT-T1/E1 card for T1 PRI or CAS lines
- PVDM3 cards containing Dsp type: sp2600
- DTMF relay must be configured with RTP-NTE under dial-peer

Restrictions for Cisco V.150.1 MER Modem Relay Support for TDM to SIP Gateway

- V150.1 MER modem relay is supported only for TDM to SIP call flows
- V150.1 MER Modem relay is not supported with initial call being SRTP
- No-Audio codec and V150.1 MER compliance T.38 fax relay protocols are not supported
- VBD mode and other modulations like V.90 (apart from V.34 and V.32) are not supported
- SPRT with payload number 120 and SSE with payload number 118 values are fixed
- Audio to V150.1 MER modem relay transition is supported only for the following codecs: G.711, G.729, and G723
- Both NSE and SSE based modem relay should not be configured together

How to Configure V.150.1 MER Modem Relay Support for TDM to SIP Gateway

Configuring V.150.1 MER Modem Relay Support for TDM to SIP Gateway

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Configure SSE MER V.150.1 using the following commands:
   - **modem relay sse v150mer** in the dial-peer configuration mode
   - **modem relay sse v150mer** in the global VoIP configuration mode
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.
Step 2	**configure terminal**	Enters global configuration mode.
Step 3	Configure SSE MER V.150.1 using the following commands: • **modem relay sse v150mer** in the dial-peer configuration mode	

	Command or Action	Purpose

	• **modem relay sse v150mer** in the global VoIP configuration mode
	
	Example:
	In dial-peer configuration mode
	
	`! Configuring SSE V.150.1 MER for one dial peer only`
	`Device (config)# dial-peer voice 20 voip`
	`Device (config-dial-peer)# modem relay sse v150mer`
	
	`Device (config-dial-peer)# end`
	
	Example:
	In global VoIP SIP configuration mode
	
	`! Configuring SSE MER V.1501.1 globally`
	`Device (config)# voice service voip`
	`Device (config-voi-serv)# modem relay sse v150mer`
	`Device (config-serv-serv)# end`	

Step 4	**end**	Exits to privileged EXEC mode.

Verifying and Troubleshooting V.150.1 MER Modem Relay Support for TDM to SIP Gateway

To verify and troubleshoot the configuration of the Cisco V.150.1 MER Modem Relay Support for TDM to SIP feature, use the following **show** commands. The **show** commands provide information about the calls.

1. **show call active voice {brief/compact}**-This command displays details about the VoIP call legs on the voice gateway, and also the type of codec and modem relay (V.150.1 or NSE) used. Initially, when the call is audio, the command displays details about the audio codec. Once the modem call is established across gateway, the codec is displayed as modem relay.

   Example

   ```
   Router# show call active voice compact
    <callID>  A/O FAX T<sec> Codec       type        Peer Address       IP R<ip>:<udp>
    Total call-legs: 2
           38 ANS     T20    modem-relay VOIP        P      9.44.48.116:16422
           39 ORG     T20    modem-relay TELE        P2357
   ```

   Example

   ```
   Router# show call active voice | sec Modem
   Modem Relay Mode = signaling-assisted
   Modem Relay Local Rx Speed=31200 bps
   Modem Relay Local Tx Speed=31200 bps
   Modem Relay Remote Rx Speed=31200 bps
   Modem Relay Remote Tx Speed=31200 bps
   Modem Relay Phy Layer Protocol=v34
   Modem Relay Ec Layer Protocol=v14
   Modem RelayType=sse-v150-mer
   ```

2. **show modem relay statistics {sprt/all/v42}**-This command provides information on the various statistics for modem relay. The SPRT packets will increase for all the V.150.1 MER modem relay calls. Hence, this command is used to make sure that the call is using the V.150.1 MER modem relay method.

   Example

```
Router# show modem relay statistics sprt
ID:11E4
SPRT Layer Statistics
        sprt_info_frames_rcvd=0 sprt_xid_frames_rcvd=0
        sprt_tc0_explicit_acks_rcvd=0 sprt_tc1_explicit_acks_rcvd=0
 ---------------------------------
 ---------------------------------
        sprt_info_tframes_failed_to_consume=0
        sprt_info_bytes_rcvd=1637 sprt_info_bytes_sent=47
        sprt_pkts_dropped_intf_busy=0 sprt_min_rexmit_timeout=500
        sprt_max_rexmit_timeout=500

        Total Modem Relay Call Legs = 1
```

Troubleshooting V.150.1 MER Modem Relay Support for TDM to SIP Gateway

Use the following **debug** commands to troubleshoot V.150.1 MER modem relay support for TDM to SIP gateway:

- debug ccsip message
- debug ccsip error
- debug voip ccapi inout
- debug voip vtsp all
- debug vpm signal
- debug modem relay events
- debug modem relay errors

Use the following advanced **debug** commands to troubleshoot V.150.1 MER modem relay support for TDM to SIP gateway thoroughly:

- debug voip ccapi inout
- debug vpm signal
- debug voip vtsp all
- debug voip hpi all
- debug modem relay errors
- debug modem relay events
- debug modem relay packetizer
- debug voice dsm all
- debug voice dsmp all

- debug voip rtp session named-event
- debug voip dspapi all
- debug voip ccapi all
- debug ccsip verbose

INDEX

T

U

V