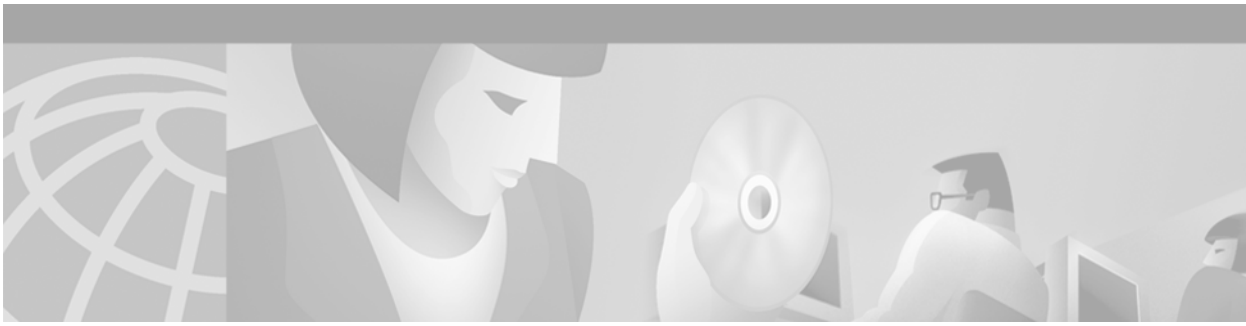


Configuring Fax Applications

This chapter describes T.37 Store and Forward Fax and T.38 Fax Gateway concepts and describes how to configure the fax applications for Cisco AS5300 universal access server access servers. The applications are T.37 Store and Forward Fax, T.38 Fax Relay for Voice over IP (VoIP) H.323, Fax Relay Packet Loss Concealment, and T.37/T.38 Fax Gateways. The applications enable the Cisco AS5300 universal access server to send and receive faxes across packet-based networks, using modems or voice feature cards (VFCs).

This chapter includes the following sections:

For a complete description of the commands used in this chapter, 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.

To identify the hardware platform or software image information mentioned in this chapter, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the "Identifying Supported Platforms" section in the "Using Cisco IOS Software" chapter.

Fax Applications Overview

Fax applications enable Cisco AS5300 universal access servers to send and receive faxes across packet-based networks using modems or VFCs. Some of the benefits of the Fax Gateway are as follows:

- Universal inbox for fax and e-mail—Faxes and e-mails can go to the same mailbox using direct inward dialing (DID) numbers. E-mail and fax recipients can be combined.
- Toll bypass—In an enterprise environment in which offices in different cities are connected using a WAN, toll charges can be bypassed by transmitting faxes over the network connection. Because a fax message is stored on the mail server until Simple Mail Transfer Protocol (SMTP) forwards messages to the recipient, SMTP can forward fax e-mail attachments during off-peak hours (for example, during evenings and weekends), thereby reducing long-distance charges.
- Broadcast to multiple recipients—E-mail fax attachments can be sent to multiple recipients simultaneously.

- Improve robustness—The Fax Relay Packet Loss Concealment feature improves the robustness of the facsimile relay. It eliminates fax failures and lost data caused by excessive page errors. Field diagnostics and troubleshooting capabilities are improved by available debug commands. Statistics give better visibility into the real-time fax operation in the gateway, allowing for improved field diagnostics and troubleshooting.
- Cost savings and port density using T.37/T.38 Fax Gateway—The cost of maintaining one architecture (either fax or voice) is eliminated. Service providers can do the following:
  - Use a single port for voice, fax relay, and Store and Forward Fax. For smaller points of presence (POPs), the single-port configuration for these technologies is even more significant because mixed traffic can be handled more efficiently requiring only a single pool of ports versus splitting traffic across two pools.
  - Offer the new service of a single number for subscriber voice and fax access. The applications that use a single number for voice and fax require only half as many dialed number identification service (DNIS) numbers and dial peers as would be required with separate voice and fax applications.
  - Offer applications that require toggling from voice to fax. Applications such as never-busy fax service can be addressed once the gateway can dynamically switch from fax relay to fax store and forward.
- Interoperability with T.37 fax relay for VoIP H.323—The Cisco 2600 and 3600 series routers and Cisco MC3810 multiservice concentrator gateways with International Telecommunication Union Telecommunication (ITU-T) T.38 fax relay capability can interoperate with third-party gateways and gatekeepers over an IP H.323 network. The goal is to work with third-party gateways and gatekeepers to provide ITU-T standards-based T.38 fax relay services for multivendor networks.

The Cisco 2600 and 3600 series routers and Cisco MC3810 multiservice concentrator gateways provide standards-based toll bypass for fax and voice calls. In addition to existing voice and fax toll bypass capabilities, the multiservice gateways provide toll bypass for fax relay with the standards-based ITU-T T.38 fax relay implementation.

On-Ramp Gateway

The Cisco AS5300 universal access server acts as an on-ramp gateway to receive faxes from end users and uses call discrimination to determine call type and destination. It converts the faxes into TIFF files, creates standard Multipurpose Internet Mail Extension (MIME) e-mail messages, attaches the TIFF files to e-mail messages, and forwards the fax-mail messages to the messaging infrastructure of a designated SMTP server, where fax-mail messages are stored.

The on-ramp gateway uses the sending Message Transfer Agent (MTA) and dial peers to receive the faxes. The sending MTA, the Cisco AS5300 universal access server, defines delivery parameters associated with the e-mail message to which the fax TIFF file is attached. These delivery parameters include defining a return e-mail path or designating a destination mail server.

The on-ramp plain old telephone service (POTS) dial peers define the call as a fax transmission and identify the DNIS of the incoming fax call. The on-ramp Multimedia Mail over IP (MMoIP) dial peer defines the destination fax telephone number and the session target, which in this case is the SMTP server.

The configuration of the on-ramp gateway involves the following:

- Called subscriber number—Displayed number in the liquid crystal display (LCD) of the fax device sending a fax to a recipient. With a standard Group 3 fax device, this is the telephone number associated with the receiving fax device.

- Sending MTA—Contains the following elements in the e-mail message to which the fax TIFF file is attached:
  - Subject
  - Destination
  - Return path
  - Postmaster
  - Any additional identifying e-mail header information
  - Address to which any disposition notices are sent
- POTS dial peer—Defines the characteristics of the Public Switched Telephone Network (PSTN) connection between the sending fax device and the on-ramp gateway. The on-ramp gateway uses these characteristics to determine the call type and call destination using call discrimination.
- MMoIP dial peer—Describes the line characteristics generally associated with a packet network connection. With T.37 Store and Forward Fax, this is the IP network connection between the on-ramp gateway and the SMTP server. On-ramp MMoIP dial peers do the following:
  - Define the destination fax telephone number
  - Specify a destination e-mail address, which identifies the SMTP server
  - Define the image encoding and resolution specifics for the associated fax-mail TIFF files
  - Request DSNs, MDNs, or both.

    If DID is enabled, the incoming called number for the on-ramp POTS dial peer should match the destination pattern of the on-ramp MMoIP dial peer. If DID is not enabled, a redialer must be configured and enabled. In this case, the destination pattern must match the forwarded dialed digits from the redialer.

Off-Ramp Gateway

Off-ramp faxing requires that the Cisco AS5300 universal access server act as an off-ramp gateway and dial POTS and communicate with a remote Group 3 fax device using standard fax protocols. It uses call discrimination to determine call type and destination.

Off-ramp faxing activities are not mutually exclusive. An e-mail can be sent as a fax, and a TIFF file can be attached to it. When the Cisco AS5300 universal access server converts the e-mail to fax format, it also converts the attached TIFF file to standard Group 3 fax format.

The off-ramp gateway does the following:

- Converts a fax-mail TIFF file or plain text file into a standard format and delivers it to the recipient. Store and Forward Fax does not alter the TIFF or plain text file in any way from its original format when converting it into a standard fax format. The off-ramp gateway uses the receiving MTA and dial peers to perform the conversion.
- Delivers an e-mail message as a standard fax transmission. The Cisco AS5300 universal access server generates information that is appended to the top of each faxed page (text-to-fax pages) and creates a fax cover sheet. The off-ramp gateway uses the receiving MTA and dial peers to deliver e-mail messages as fax transmissions.
- Uses only POTS dial peers to define the line characteristics between the forwarding off-ramp gateway and the fax device. The dial peers also define the telephone number of the destination fax device. Number expansion can be used because the destination pattern is defined. As an option, the

MMoIP dial peers can be configured, but MMoIP dial peers has limited functionality. They only define fax compression schemes and resolution and is useful only if those parameters are to be altered for the received fax-mails.

- Defines the parameters associated with the AS5300 SMTP server using the receiving MTAs. The MTAs can be SMTP host aliases, which can be different from the normal Domain Name System (DNS) host names, or an internal Cisco IOS host name.

The configuration of the on-ramp gateway involves configuring the following:

- Transmitting subscriber number—Displayed number in the LCD of the receiving fax device. Typically, with a standard Group 3 fax device, this is the telephone number associated with the transmitting or sending fax device.
- Fax transmission speed—Transmission speed of the fax device; this should be set to the speed of the other devices, if possible. This functionality is particularly helpful if the off-ramp gateway is sending faxes into an area where the fax transmission speed is always negotiated down to a slower speed.
- Receiving MTA—Accepts incoming mail (from the Cisco AS5300 universal access server to the SMTP server) if the destination host name of the incoming mail matches one of the aliases configured by the **mta receive aliases** command.
- Off-ramp POTS dial peer—Defines the line characteristics between the off-ramp gateway forwarding the converted e-mail message and the receiving fax device.
- Off-ramp MMoIP dial peer—Specifies a particular resolution for the fax transmission or defines an encoding type, which is optional. If the MMoIP dial peer is configured, the incoming called number must match the destination pattern telephone number of the corresponding on-ramp POTS dial peer.
- Faxed header information—Information appended to the top of each cover and text page indicates the telephone number of the sending fax device, the date, and the time of transmission. The header information is required.
- Fax cover page—Captures information taken from the originating e-mail messages. The destination address of an e-mail message controls the generation of a cover page on a per-recipient basis.

Call Discrimination Process

When the on-ramp gateway receives a call, it immediately identifies whether the call is being delivered using a PRI or T1 channel associated signaling (CAS) interface. If the call is on a T1-CAS interface, the gateway checks the service type field of the CAS group configuration. If the service type of the CAS group is fax, the interface forwards the fax to the MMoIP dial peer. If the gateway determines that the call is on a PRI interface, then the on-ramp gateway looks at several POTS dial peer data fields to determine what kind of call it has received.

POTS Dial Peers

The on-ramp gateway looks at the incoming called number field of each POTS dial peer listed in the dial peer lookup table. It compares the number configured as the incoming called number to the number received and selects the first POTS dial peer whose data matches. If the on-ramp router does not find a match, it assumes that the incoming call is a data call and processes it accordingly.

If the on-ramp router does find a match, it will then look at the service type field of the POTS dial peer to determine whether this is a voice or fax call. If this call has been flagged as a voice call, the on-ramp gateway will process it appropriately as a voice call.

If the call has been flagged as a fax call, the on-ramp gateway checks to see whether DID has been enabled. If DID has been enabled, the gateway concludes that the telephone number it has received is the destination directory number (DN) and forwards the call to be matched with the appropriate on-ramp MMoIP dial peer.

If DID has not been enabled, the on-ramp gateway assumes that the telephone number it received is the access DN. In this case, the on-ramp gateway provides a secondary dial tone and collects another telephone number from the redialer at the other end of the connection that the gateway will use as the destination DN. After the gateway has received this number from the redialer, the number is forwarded and matched to the appropriate on-ramp MMoIP dial peer.

A redialer is an interface hardware device that connects a fax device to the PSTN network. The user enters the complete telephone number into the fax device and the attached redialer captures and stores those dialed digits. It dials the on-ramp Cisco AS5300 universal access server that provides a secondary dial tone. Use a redialer when one of the following is true:

- Provisioning a DID service is not possible.
- User information, such as a personal ID number (PIN) from the redialer, is required.
- T1-CAS is in use.

The redialer should be programmed to wait two seconds and then send the PIN with destination digits to the on-ramp gateway.

The fax protocol starts after 52 digits have been detected or the interdigit timeout has exceeded 5 seconds. If the **debug fax receive** command is enabled, the digits are displayed as received by the on-ramp gateway. If a dial peer is matched, the fax proceeds. If a dial peer is not matched, the fax fails.

By default, DID is disabled, which means that the on-ramp gateway assumes that the fax call was placed using a redialer. When the call arrives, the gateway collects digits until it can identify the destination. Once the destination is identified, the gateway forwards the call to the next call leg (MMoIP dial peer).

If DID is enabled, the on-ramp gateway uses the called number (DNIS) to find a dial peer for the outgoing call leg. DID enables the gateway to match the incoming called number with a dial peer and then directly place the outbound call. With DID, the server does not present a dial tone to the fax machine and does not collect digits. It forwards the call directly to the configured destination.

The off-ramp gateway looks at the destination-pattern field of each POTS dial peer listed in the dial peer lookup table. It compares the number configured as the destination pattern with the destination DN portion of the fax-mail address and selects the first match.

After the off-ramp gateway has identified the appropriate POTS dial peer, it matches call type information. If the call type is identified as fax, it forwards the fax-mail message to off-ramp services. If the off-ramp router does not find a match, the recipient identified by the given address is not accepted by the off-ramp router.

MMoIP Dial Peers

The MMoIP function in the call discrimination process determines the fax-mail destination, which is the off-ramp gateway over which the fax-mail is sent to the destination fax machine. The on-ramp gateway looks at the destination pattern field of each MMoIP dial peer listed in the dial peer lookup table. It compares the number configured as the destination pattern with the number received and selects the first MMoIP dial peer whose the data matches.

The on-ramp gateway then looks at the session target field for the selected MMoIP dial peer in order to identify the destination of the fax-mail message. This value could be a specific off-ramp gateway or, if the fax is being delivered as an e-mail message, an e-mail address for a specific mail server.

The resolution of a fax image can be increased or decreased using the MMoIP dial peer configuration. Pass-through is the default: the image is sent exactly as it is received. Depending on the capacity of the fax machines in the network, a different image encoding (compression) scheme could be required for the fax TIFF image. The encoding default is pass-through.

On-Ramp Gateway Security

On-ramp gateway security controls who can send fax messages to the network. It is 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 the authentication server, whether it is RADIUS or TACACS+. User information is forwarded to the AAA interface, and the authentication request is forwarded to the security server.

Authentication must be completed before the first page of faxed material is accepted from the modem 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 feature card (VFC) disconnects the call.

The on-ramp gateway inserts whatever value was configured in the "X-account-ID" field of the e-mail header that is used for authentication and accounting by the on-ramp gateway.

Attribute-Value Pairs for AAA

RADIUS attributes define specific AAA elements in a user profile, which 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.

Table 50 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.

Table 50 Vendor-Specific RADIUS 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 the **mmoip aaa send-id** command.
4	Cisco-Fax-Msg-Id=	Unique fax message identification number.
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. True means a cover page was generated and false means it was not.
7	Cisco-Fax-Modem-Time	Number of seconds it takes to send fax data (x) and to complete the entire fax session (y) in the form x/y. For example, 10/15 means that the transfer time took 10 seconds and the full fax session took a total of 15 seconds.
8	Cisco-Fax-Connect-Speed	Modem speed. Possible values are 1200, 4800, 9600, and 14400.
9	Cisco-Fax-Recipient-Count	Number of recipients. Until e-mail servers support session mode, the number should be 1.
10	Cisco-Fax-Process-Abort-Flag	True/false flag indicating that fax session was aborted or successful. True is aborted and false is processed.

Table 50 Vendor-Specific RADIUS Attributes (continued)

Subtype Number	Attribute	Description
11	Cisco-Fax-Dsn-Address	Address to which DSNs are sent.
12	Cisco-Fax-Dsn-Flag	True/false flag to indicate if DSN is enabled. True is enabled and false is disabled.
13	Cisco-Fax-Mdn-Address	Address to which MDNs are sent.
14	Cisco-Fax-Mdn-Flag	True/Flash flag to indicate if MDN is enabled. True is enabled and false is disabled.
15	Cisco-Fax-Auth-Status	Authentication status—successful, failed, bypassed, or unknown.
16	Cisco-Email-Server-Address	E-mail server IP address handling the on-ramp fax-mail message.
17	Cisco-Email-Server-Ack-Flag	Acknowledgement that the e-mail server accepted the message.
18	Cisco-Gateway-Id	Processing gateway name in this 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.
21	Cisco-Abort-Cause	System component that signalled an abort.

Access Control Lists

Incoming Access Control Lists (ACLs) can be used on Ethernet or FastEthernet interfaces to filter SMTP fax traffic. It is recommended that ACLs be configured to restrict access to the SMTP port (port 25) to only trusted e-mail servers. Creating ACLs is beyond the scope of this document. For information, refer to the *Cisco IOS Security Configuration Guide*.

ESMTP Accounting Services

Accounting information can be collected about fax services in two ways:

- Using RADIUS accounting
- Collecting the accounting information using SMTP

The extended simple mail transfer protocol (ESMTP) accounting feature enables the collection of accounting information as part of the SMTP session. This functionality is activated through the use of an intelligent fax client or MTA. In ESMTP accounting, the off-ramp gateway acting as an ESMTP server advertises capabilities to the MTA, which is acting as an e-mail client.

One of the capabilities the off-ramp gateway advertises is “xaccounting,” which supports ESMTP accounting. If the MTA recognizes the xaccounting service extension, the MTA (acting as the client) accepts the ESMTP accounting information sent from the off-ramp gateway. If the MTA does not recognize the xaccounting service extension, it does not send the **xact** command to the off-ramp gateway. In that case, the off-ramp gateway does not respond with ESMTP accounting data.

To use SMTP to collect accounting data, the MTA must be configured to explicitly request accounting information as part of the e-mail session. The MTA must be able to do the following:

- Recognize the xaccounting service extension during the extended hello (ehlo) transaction
- Send the **xact** command to the off-ramp gateway to activate the ESMTP accounting feature

Message Delivery Notifications

Described in RFC 2298, an message delivery notification (MDN) is a message that is sent to the originator of an e-mail message indicating that the e-mail message was received. MDN elements must be configured for both the on-ramp and off-ramp gateways. MDN requests as part of the on-ramp MMoIP dial peer configuration must be enabled. For complete instructions on how to configure MDNs, see the "Configuring MDNs" section on page 699.

Delivery Status Notifications

Delivery status notifications (DSNs) are messages or responses that are automatically generated and sent to the sender or originator of an e-mail message by the SMTP server, notifying the sender of the status of the e-mail message. DSNs must be configured for both the on-ramp and off-ramp gateways.

Three different states can be reported back to the sender as follows:

- Delay—Delivery of the message was delayed.
- Success—Delivery of the message was successful.
- Failure—Message was undeliverable to the SMTP server.

Because the delivery states are not mutually exclusive, messages for all or any combination of these events can be generated.

DSN requests can be enabled as part of the on-ramp MMoIP dial peer configuration. For complete instructions on how to configure DSNs, refer to the "Configuring DSNs" section on page 700.

T.37 Store and Forward Fax

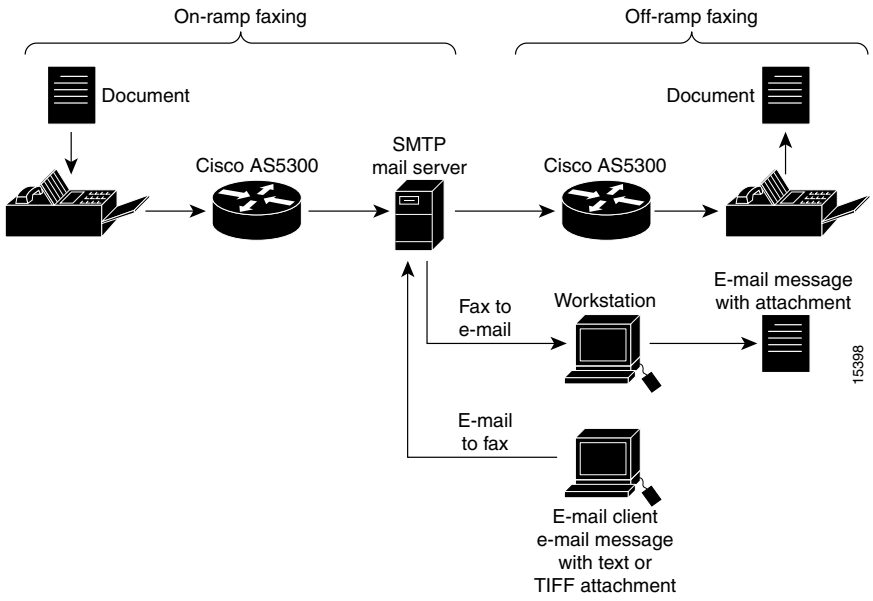
T.37 Store and Forward Fax is an implementation of the RFC 2305 proposed standard from the IETF and is the same as the T.37 recommendation of the International Telegraph Union (ITU). T.37 Store and Forward Fax enables the access server to become a multiservice platform, supplying both data and fax communication using modems.

T.37 Store and Forward Fax enables the following:

- Sending and receiving faxes to and from Group 3 fax devices
- Receiving faxes that are delivered as an e-mail attachment
- Creating and sending a standard e-mail message that is delivered as a fax to a standard Group 3 fax device

The basic functionality is facilitated through SMTP with additional functionality that provides confirmed delivery using existing SMTP mechanisms, such as ESMTP. Figure 117 shows a simple network topology using T.37 Store and Forward Fax.

Figure 117 T.37 Store and Forward Fax Functionality



The messaging infrastructure performs message routing, storage, and transport, and can be a standard Internet MTA—for example, UNIX sendmail or custom T.37 Store and Forward Fax software. The responsibility of delivering the fax-mail message falls to SMTP and the mail server.

Modem Pooling

As a default, T.37 Store and Forward Fax receives faxes on modems that are in the on-ramp gateway default modem pool. These modems are available for both fax and data calls. The on-ramp gateway determines the call type using DNIS and compares the DNIS number to the configured value for the incoming called-number POTS dial-peer configuration command.

If the DNIS number matches the incoming called number, DNIS treats the call as a fax transmission. If it does not find a match in its dial peer lookup table, it treats the call as a data call.

The incoming fax calls can be configured to bypass the default modem pool by defining a named modem pool. This is particularly useful if the calls have Modem ISDN channel aggregation (MICA) and Microcom faxes, because it diverts fax traffic from MICA modems that do not support fax transmission.

Fax Relay Packet Loss Concealment

Fax relay packet loss concealment improves the current real-time fax over IP (commonly known as fax relay) implementation in Cisco gateways, enabling fax transmissions to work reliably under higher packet loss conditions.

In addition, this feature includes enhanced real-time fax debug capabilities and statistics for improved field diagnostics and troubleshooting. The capabilities and statistics give better visibility into the real-time fax operation in the gateway.

One improvement is fax relay Error Correction Mode (ECM) on the VoIP dial peer. When used, the DSP fax relay firmware disables ECM through modification of the DIS T.30 message in both directions.

ECM provides for error-free page transmission. It is available on fax machines that include memory for storage of the page data (usually high-end fax machines). The page is transmitted in a series of blocks. After receiving the complete page data, the receiving fax indicates any frames with errors. The transmitting fax then retransmits those frames. This process is repeated until all frames have been received without errors. If the receiving fax is not able to receive an error-free page, the fax transmission may fail, and one of the fax machines may disconnect. With packet-loss levels greater than 2 percent, fax transmissions consistently fail between page transmissions when ECM is enabled.

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

- Respond to page reception with the **ReTrain Positive** command. This 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 causes the transmitting fax to go through the TCF process with a lower modulation scheme.
- Disconnect immediately.

Note ECM disable is recommended when there is a known lossy network (especially with packet loss at 2 percent or greater) and if fax traffic is anticipated for the dial peer.

Handling of Enclosures

All Cisco fax applications can process e-mail with the following MIME media content types:

- Text (plain type)
- Text (enriched type)
- Image or TIFF (“Profile S” described in RFC 2301)

Further, all Cisco fax applications support the following content transfer encodings:

- Seven bit
- Eight bit
- Base 64
- Quotable-printable

These content transfer encodings can be wrapped in any multipart/* content type. When messages with multiple sections are received, the first part of the multipart message is processed, and a count of what is and is not successfully sent is stored. The rest of the message is discarded. For example, if a multipart, alternative message has a plain text part and an enriched, html text part and the plain text is first, the the plain text part is the only part processed.

Note The TIFF file format must conform to RFC 2301 (*File Format for Internet Fax*). Store and forward fax does not support uuencoded text, JPEG or JBIG files, or multiraster content.

Caution The Cisco AS5300 universal access server recognizes only the listed file attachment types. If it receives a file format different from one of the defined acceptable formats, the data is discarded.

T.37/T.38 Fax Gateway

When the Cisco AS5300 universal access server is equipped with VFCs, it supports carrier-class Voice over IP (VoIP) and Fax over IP services. Since the Cisco AS5300 universal access server is H.323 compliant, it supports a family of industry-standard voice codecs and provides echo cancellation and voice activity detection (VAD)/silence suppression.

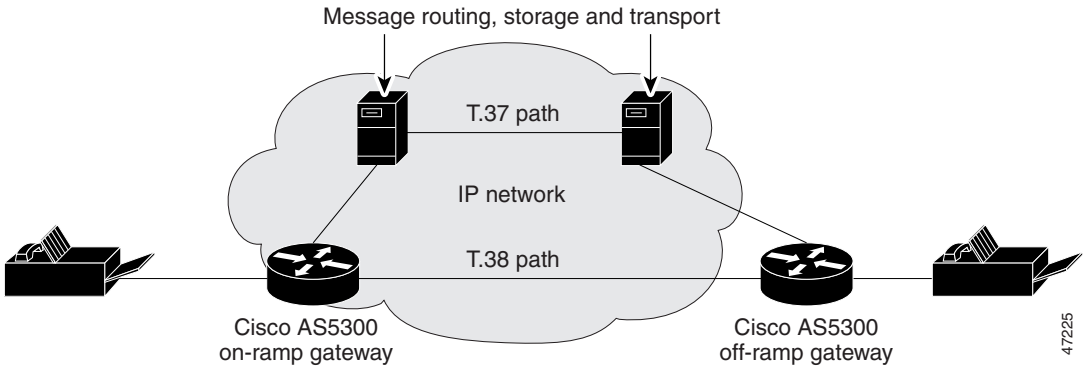
The VFC is a coprocessor card with a powerful reduced instructions set computing (RISC) engine and dedicated, high-performance DSPs to ensure predictable, real-time voice processing. The design enables streamlined packet forwarding. The Cisco AS5300 universal access server supports two VFCs that are scalable up to 96 E1 or 120 T1 voice connections within a single chassis.

T.37 Store and Forward Fax was supported by modem cards while the voice applications ran on the C542 digital signal processing module (DSPM) and C549 DSPMs that populated Cisco AS5300 VFCs. Each type of call required different technologies. With this software release, a single DSPM technology supports the following:

- Voice, fax relay, and T.37 Store and Forward Fax on both the C542 and C549 DSPM and the same voice port
- Dynamic switching from one application to another in the same call (IVR, voice, Fax Relay, and T.37 Store and Forward Fax)

Figure 118 highlights the real-time (T.38 path) versus the T.37 Store and Forward processing (T.37 path) for fax transactions over IP networks.

Figure 118 Real-Time Versus T.37 Store and Forward Fax Processing



Fax over IP used a proprietary protocol and an H.323 connection, represented by the T.37 path in the diagram. The T.37 path used the ESMTP T.37 Store and Forward method. The on-ramp gateway router accepted fax data from the PSTN fax machine.

The fax data was converted into a TIFF attachment in a MIME e-mail message and transmitted to a T.37 Store and Forward SMTP server. The server would deliver the fax-mail message to the off-ramp gateway. Once the off-ramp gateway received the fax-mail message, it processed the message and initiated a session with the destination fax machine.

With this software release, the T.38 path takes precedence over the T.37 path whenever possible. This means that as a fax session is being set up, the sending gateway first communicates using the T.38 path. If the communication fails, the sending gateway rolls over to the Cisco T.37 path if it is configured to rollover.

Using Interactive Voice Response

Interactive voice response (IVR) applications control calls by using voice prompts and digit collection in order to authenticate the user and identify the call destination. The applications are assigned to specific ports or invoked based on DNIS. They accommodate many gateway services by customizing the presentation of the interfaces to callers.

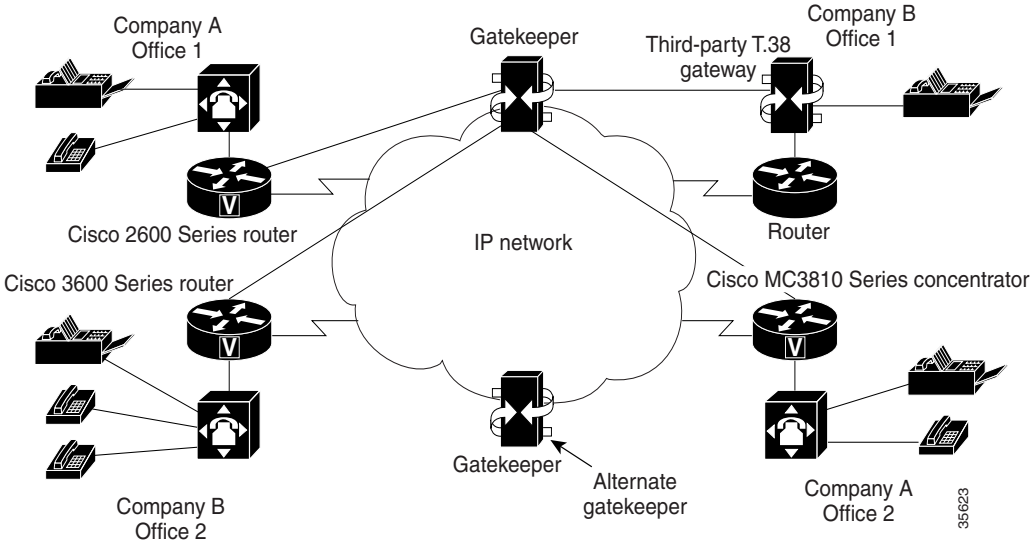
IVR uses Tool Command Language (TCL) scripts to gather information. For example, a TCL script plays when the caller receives a voice prompt to enter a specific type of information, such as a PIN. After the caller inputs the PIN, TCL collects the digits and forwards the digits to the server for storage and retrieval.

T.38 Fax Relay for VoIP H.323

The T.38 Fax Relay for VoIP H.323 feature provides standards-based fax relay protocol support on the Cisco 2600 and 3600 series routers and the Cisco MC3810 multiservice concentrator gateways. The Cisco proprietary fax relay solution is sometimes not an ideal solution for Enterprise and Service Provider customers who have implemented a mixed-vendor network. Because the T.38 fax relay protocol is standards based, Cisco gateways and gatekeepers can interoperate with third-party T.38-enabled gateways and gatekeepers in a mixed-vendor network when real-time fax relay capabilities are required.

 shows an IP H.323 network with Cisco and third-party gateways and gatekeepers using T.38 fax relay functionality. By using T.38 fax relay, all gateways and gatekeepers in this network are able to send faxes to other remote offices or to the offices of another company on the IP network.

Figure 119 IP Network for T.38 Fax Relay



For example, when a fax is sent from the originating gateway, a voice call is established. The terminating gateway detects the fax tone generated by the answering fax machine. The VoIP H.323 call stack then starts a T.38 mode request using H.245 procedures. If the opposite end of the call acknowledges the T.38 mode request, the initial audio channel is closed and a T.38 fax relay channel is opened. When the fax transmission is completed, the call reverts to voice mode.

Fax Applications Prerequisites

The following sections describe prerequisite tasks to perform before configuring all of the available fax applications:

Note If you are using modem cards, only T.37 Store and Forward Fax is supported. If you are using VFCs, T.37 Store and Forward Fax and T.38 Fax Relay and real-time fax are supported.

T.37 Store and Forward Fax Prerequisites

Before the T.37 Store And Forward Fax can be configured, the following tasks are required:

- Install a modem card into the appropriate slot of the Cisco AS5300 universal access server. Both MICA and Microcom modem cards support Store and Forward Fax, although MICA modem cards support only off-ramp faxing. For more information about installing Microcom and MICA modem cards, refer to the *Cisco AS5300 Universal Access Server Module Installation Guide* and the *Cisco AS5300 Universal Access Server Chassis Installation Guide*.
  - Update the Cisco AS5300 universal access server software configuration if modem cards are added or removed.
  - Download and install the V.90n firmware for the Microcom modem card and the standard portware with fax transmission capabilities for the MICA modem card.
- Establish a working IP network. For more information about configuring IP, refer to the "IP Overview," "Configuring IP Addressing," and "Configuring IP Services" chapters in the *Cisco IOS IP Routing Configuration Guide*.
- Complete the basic configuration for the Cisco AS5300 universal access server that includes, as a minimum, the following tasks:
  - Configure a host name and password for the Cisco AS5300 universal access server.
  - Configure the Ethernet 10Base T/100Base T interface so that the Cisco AS5300 universal access server can be recognized as a device on the Ethernet LAN.
  - Configure the Cisco AS5300 universal access server interfaces for ISDN PRI or T1 lines.
  - Configure the ISDN D channels for each ISDN PRI or T1 line.

  For more information about any of the these configuration tasks, refer to the *Cisco AS5300 Universal Access Server Software Configuration Guide*.

Note VoIP need not be configured for T.37 Store and Forward Fax to function.

The following sections describe specific prerequisite tasks to configure T.37 Store and Forward Fax:

Configuring the SMTP Server

Note Before using SMTP in Cisco gateways, be sure to configure the domain name and host name.

Although it is not required, configuring the SMTP server enhances functionality. To configure the SMTP server, perform the following tasks:

- Edit the SMTP server alias file to include an alias for fax transmissions. The alias is an e-mail address that has the "fax=" prefix included in it. For example, fax=5551212, user@hostname.com. In this example, the on-ramp gateway automatically forwards the incoming fax to the mailbox for user@hostname.com.
  - If aliases are used to forward faxes, configure the on-ramp multimedia over IP (MMoIP) dial peer **session-target** command as **session target mailto: d@***hostname.com*. The **d** wildcard specifies that the destination fax machine telephone number is inserted in the to: field of the fax-mail that gets sent to the SMTP server.
- Modify parameters involving SMTP delivery requirements. Failure to do so can result in a monopoly of bandwidth and fax resources.

  Fax transmission has delivery requirements that are different from those of e-mail transmission. For example, in certain countries, it is illegal to try to send a fax more than three times in a row if transmission fails.

  SMTP mail delivery requirements are not governed by such strict regulations. In general, if an e-mail message cannot be delivered, the SMTP server is supposed to continue trying every 30 minutes for up to 5 days. To avoid any complications arising from the difference between the SMTP e-mail and fax delivery requirements, modify the following parameters:
  - Delivery to one recipient
  - Message priority
  - Connection cache size
  - Minimum queue age

Configuring the MTAs

MTAs, such as sendmail, Post.Office, and others, are normally configured to provide fast and reliable service for transferring e-mail. However, the needs of fax users are different. The best example of differing fax requirements is retry timeouts.

A typical MTA configuration will retry sending failed message transmissions every 30 minutes for up to 5 days. Resending e-mail every 30 minutes is usually unacceptable to fax users—they want retries more often than every 30 minutes and usually want transmission aborted well before the typical 5-day retry limit. Although a typical unmodified MTA can be used with the Cisco AS5300 universal access server for off-ramp operations, the MTA may need to be fine-tuned for fax operation.

Configuring Fax Operation

The Cisco AS5300 universal access server off-ramp accepts only one e-mail recipient per SMTP transaction because the SMTP server does not do the following:

- Queue messages in the Cisco AS5300 universal access server memory. The reason is the size of the messages and the lack of sufficient nonvolatile storage.
- Include a mechanism to enable the receiving MTA to indicate the success or failure of each delivery. It indicates the success or failure of the entire transaction.

The Cisco AS5300 universal access server prevents one SMTP transaction from going to multiple recipients by responding to the second and subsequent RCPT commands with a "450" reply code. Because of the typical mailer configuration, this causes a 30-minute delay for each recipient: immediate delivery for the first recipient, 30-minute delay for the second recipient, 60-minute delay for the third recipient, etc.

Configuring All Mail Through One Mailer

To simplify system administration, have all mail to the Cisco AS5300 universal access server go through one mailer by setting up a DNS MX record for the Cisco AS5300 universal access server. The record points to and sets up the mailer to skip MX record processing for the Cisco AS5300 universal access server. For example, the following two records would exist in DNS:

```
sj-offramp  in mx 10 sj-mailer
sj-offramp  in mx 20 sj-offramp
sj-offramp  in a  1.2.3.4
```

Configure ACLs to block incoming mail from other mailers. This prevents unauthorized use of the fax off-ramp and forces all mail to go through one mailer.

If ACLs have been set up on the router, the second MX record should *not* be placed in the DNS. For more information about ACLs, refer to the *Cisco IOS Security Configuration Guide*.

Configuring Sendmail 8.8.5 for Single Recipients

Fine-tuning sendmail 8.8.5 for a single recipient enables the Cisco AS5300 universal access server to work faster with Store and Forward Fax off-ramps and reduce delays caused by attempting to send to multiple recipients. It is important that sendmail be configured to send to each recipient serially, but without a delay after each transmission. Parallel configuration of sendmail with a single recipient and multiple sendmail client processes would cause a single message to be returned through sendmail, perhaps on a different port. The parallel configuration is not within the intended scope of this document.

Caution Do not modify the sendmail configuration on any system without a full understanding of what mail that system is processing and without the approval of the postmaster of the site. Modifying a company mail system can cause a loss of mail service upon which many companies rely for day-to-day operation.

To configure sendmail 8.8.5 to send to a single recipient, perform the following tasks:

- Modify the sendmail configuration file (usually named /etc/sendmail.cf) to the following:

```
Kmailertable hash /etc/mailertable
```

Note The line could already exist, but be commented out.

- If Kmailertable already exists in the configuration file, determine the name of the source text file used to build the mailertable.db file and edit it in or the existing mailertable.db of the site will be overwritten. If Kmailertable does not exist, add the line in toward the top of the configuration file with other "K" settings. The mailer table usually displays like this:

```
# not local -- try mailer table lookup
R$* <@ $+ > $*          $: < $2 > $1 < @ $2 > $3       extract host name
R< $+ . > $*            $: < $1 > $2                   strip trailing dot
R< $+ > $*              $: < $(mailertable $1 $) > $2  lookup
R< error : $- $+ > $*   $#error $@ $1 $: $2            check -- error?
R< $- : $+ > $*         $# $1 $@ $2 $: $3              check -- resolved?
R< $+ > $*              $: $>90 <$1> $2                try domain
```

Note A rewrite rule must be specified that causes a matching of the hosts in the mailer table. Ensure that the rewrite rules (starting with "R") for mailer table are not commented out.

  If the mailer table cannot be found, place the lines in Ruleset 0, which starts at the line containing "S0," before the rules that deliver local mail (R$=L $#local ...).

- Create a new mailer specification line in the section with other mailer specifications toward the bottom of the file as follows:

```
Mfaxofframp,    P=[IPC], F=DFMuXa0, S=11/31, R=21, E=\r\n, L=2040,
T=DNS/RFC822/SMTP,
A=IPC $h
```

  Ensure that the S and R values are the same as those for the existing mailer specifications for mail relaying. The existing S and R values are the lines beginning with an uppercase "M," usually toward the end of the sendmail.cf file.

  The S and R values control sendmail rewrite rules as applied to the Sender and Recipient addresses of the message. The rules and rule numbers must be different on each system, especially at sites that have complex sendmail configurations.

  It is important to omit the "F=m" flag and include the "F=0" (zero) flag as shown. The "m" flag causes delivery to multiple recipients (which is unwanted) and the "0" (zero) flag disables MX lookups (which are desired). The "0" (zero) flag is available only in sendmail version 8.8 or later. If an earlier version of sendmail is configured, omit the "0" and use [ ] in the mailer table.

- Create a file (/etc/mailertable.txt) with one line for each fax off-ramp device, listing the host name, white space, then the string "faxofframp:" and the host name again. For example, the hosts offramp-seattle.cisco.com and as5300-denver.cisco.com would be inputted as follows:

```
offramp-seattle.cisco.com  faxofframp:offramp-seattle.cisco.com
as5300-denver.cisco.com    faxofframp:as5300-denver.cisco.com
```

  If prior version of sendmail 8.8 is configured, use brackets around the right-side host name as follows:

```
offramp-seattle.cisco.com  faxofframp:[offramp-seattle.cisco.com]
```

- Input the following line to compile the new mailertable.txt using makemap (sometimes located in /usr/sbin):

```
/usr/sbin/makemap hash /etc/mailertable.db < mailertable.txt
```

Note If the system does not have makemap, sendmail will not support "hash." In this case, point sendmail at the mailertable.txt file by using "text" instead of "hash" on the Kmailertable line.

- Close and restart sendmail as follows:

```
ps -e | grep sendmail
kill pid                    # using PID indicated by above output
/usr/lib/sendmail -bd
```

- In DNS, set up A and MX records:

```
as5300-hostname     in a   a.b.c.d
in mx  10  sendmail-system
in mx  20  as5300-hostname
```

  This causes mail to be delivered to the sendmail-system first. Because the sendmail configuration disables MX lookups ("F=0") for the Cisco AS5300 universal access server, sendmail delivers directly to the IP address of the Cisco AS5300 universal access server. Also, if the sendmail system is down or otherwise unavailable, mail is queued directly to the Cisco AS5300 universal access server. Alternatively, use the following configuration:

```
as5300-hostname     in a   a.b.c.d
in mx  10  sendmail-system
in mx  20  backup-mta
```

  In this example, backup-mta is another sendmail (or other) mailer.

- Fine-tune the following parameters to control sendmail and provide near-real-time delivery of messages:
  - "O MinQueueAge" controls how long an entry must be in the queue before an attempt is made to process it. Reduce this setting for use with Cisco fax off-ramps (the normal value is 30 minutes).
  - "-q" switch starts sendmail and controls how often the queue is checked for reprocessing entries.
  - "O Timeout.queuereturn" controls the lifetime of a message in the queue.
  - "O Timeout.queuewarn" controls when sendmail issues a warning that the message has not been successfully relayed.
  - "O QueueSortOrder=XXX" controls how sendmail sorts the queue for processing. The string XXX should be one of these: host, priority, or time.
  - "O QueueLA" and "O QueueFactor" control the system load average, which causes sendmail to queue new messages instead of delivering them.
  - "O ConnectionCacheSize" and "O ConnectionCacheTimeout" processes more than one mail transaction in one TCP session with the fax off-ramp.
- Set the "O DoubleBounceAddress" parameter to the local postmaster or other administrative human address.

Note If the sending MTA supports the X-SESSION SMTP service extension, the Cisco AS5300 universal access server will support multiple recipients in one SMTP transaction and will store only one copy of each fax data page in its memory.

Configuring the Redialers

Perform the following tasks to enable a redialer:

- Program the redialer to dial the Cisco AS5300 universal access server acting as the on-ramp gateway and capture the dialed digits.
- Configure an MMoIP dial peer to match the forwarded dialed digits from the redialer.

Note Only the Mitel and Telecom Research redialers are supported on the Cisco AS5300 universal access server.

Fax Relay Packet Loss Concealment Prerequisite Tasks

VCWare 7.04 or higher version must be running before configuring fax relay packet loss concealment.

T.37/T.38 Fax Gateway Prerequisite Tasks

To enable the T.37/T.38 Fax Gateway for the Cisco AS5300 universal access server, perform the following tasks:

- Downloading VCWare to the VFC, page 682
- Copying Flash Files to the VFC, page 685
- Unbundling VCWare, page 686
- Adding Files to the Default File List, page 687
- Adding Codecs to the Capability List, page 687
- Deleting Files from VFC Flash Memory, page 688
- Erasing the VFC Flash Memory, page 688
- Configuring IVR, page 688

Downloading VCWare to the VFC

VFCs for the Cisco AS5300 universal access server come with a single bundled image of VCWare stored in VFC Flash memory. Table 51 shows the extension types defined for these embedded firmware files.

Table 51 VFC Firmware Extensions

Firmware	Filenames	Description
VCWare	vcw-vfc-*	Latest version of VCWare stored in Flash memory, including the following: • Datapath engine • Message dispatcher • DSP manager • VC manager • Process scheduler

Table 51 VFC Firmware Extensions (continued)

Firmware	Filenames	Description
DSPWare	btl-vfc-*	DSP bootloader
	cor-vfc-*	Core operating system and initialization
	bas-vfc-*	Base voice
	cdc-*-*	Voice codec files
	fax-vfc-*	Fax relay files

DSPWare is stored as a compressed file within VCWare. VCWare must be unbundled to install DSPWare in Flash memory. During the unbundling process, two default lists (default file and capability) are automatically created, populated with default files from that version of VCWare, and stored in VFC Flash memory. The default file list contains the names of the files that are initially loaded into DSP upon boot up, and the capability list defines the set of codecs that can be negotiated for a voice call.

VFC management enables the following functionality:

- Adding versions of VCWare to Flash memory by downloading and unbundling the files
- Erasing files contained in Flash memory
- Adding files to the default file and capability lists
- Deleting files from the default and capability lists

Before downloading VCWare to the VFC, determine whether or not the version of VFC ROM Monitor software is compatible with the installed Cisco IOS image. VFC ROM version 1.2 requires Cisco IOS image 0.14.1 (1.6 NA1) or later. VFC ROM Monitor version 1.2 can be made to work with Cisco IOS image 0.13 (or later) by appending the suffix ".VCW" to the VCWare image stored in VFC Flash memory.

The required tasks are as follows:

- Determining the Number of VFCs
- Identifying the VFC Mode
- Downloading the Software in VCWare Mode
- Downloading the Software in ROM Monitor Mode

Determining the Number of VFCs

To determine the number of installed VFCs and their location, use the following command in privileged EXEC mode:

Command	Purpose
`Router# show vfc slot directory`	Determines the number of installed VFCs and their location.

For each VFC identified and located, upgrade the system software on that VFC.

Identifying the VFC Mode

To identify the mode (whether VCWare or ROM Monitor), use the following command in privileged EXEC mode:

Command	Purpose
`Router# show vfc slot board`	Determines whether the VFC is operating in VCWare mode or ROM Monitor mode.

If the mode is VCWare, the VFC status will be "VCWARE running." If the mode is ROM monitor, the VFC status will be "ROMMON."

Downloading the Software in VCWare Mode

To download VFC software to the VFC while in VCWare mode, use the following commands in privileged EXEC mode:

	Command	Purpose
Step 1	`Router# erase vfc slot`	Erases the Flash memory.
Step 2	`Router# show vfc slot directory`	Displays that the VFC Flash memory is empty.

Step 3	`Router# copy tftp: vfc:`
	or
	`Router# copy flash: vfc:`
		Downloads the VCWare from a TFTP Boot server into VFC Flash memory
		or
		Downloads the VCWare from the VFC motherboard into VFC Flash memory.
		Note The colons in this command are required.

Step 4	`Router# clear vfc slot`	Reboots the VFC.
Step 5	`Router# show vfc slot board`	Checks whether the VFC is back up in VCWare mode.
Step 6	`Router# show vfc slot directory`	Displays that VCWare is in the VFC Flash memory.
Step 7	`Router# unbundle vfc slot`	Unbundles the DSPWare from the VCWare and configures the default file list and the capability list.
Step 8	`Router# show vfc slot directory`	Displays that the DSPWare has been unbundled.
Step 9	`Router# show vfc slot default-list`	Displays that the default file list has been populated.
Step 10	`Router# show vfc slot cap-list`	Displays that the capability list has been populated.

The Cisco AS5300 universal access server must be rebooted before these changes can take effect.

Note If the VFC ROM is version 1.1, the image name must end in ".VCW." If the VFC ROM is version 1.2, the image name must start with "vcv-."

Downloading the Software in ROM Monitor Mode

To download VFC software while in ROM monitor mode, use the following commands in privileged EXEC mode:

	Command	Purpose
Step 1	`Router# clear vfc slot purge`	Erases the VFC Flash memory.

Step 2	`Router# copy tftp: vfc:`
	or
	`Router# copy flash: vfc:`
		Downloads the VCWare from a TFTP server into VFC Flash memory.
		or
		Downloads the VCWare from the VFC motherboard into VFC Flash memory.
		Note The colons in this command are required.

Step 3	`Router# clear vfc slot`	Reboots the VFC.
Step 4	`Router# show vfc slot board`	Checks whether the VFC is back up in VCWare mode.
Step 5	`Router# show vfc slot directory`	Displays that VCWare is in the VFC Flash memory.
Step 6	`Router# unbundle vfc slot`	Unbundles the DSPWare from the VCWare and configures the default file list and the capability list.
Step 7	`Router# show vfc slot directory`	Displays that the DSPWare has been unbundled.
Step 8	`Router# show vfc slot default-list`	Displays that the default file list has been populated.
Step 9	`Router# show vfc slot cap-list`	Displays that the capability list has been populated.

The Cisco AS5300 universal access server must be rebooted before these changes can take effect.

Note The image name must start with “vcw-.”

Copying Flash Files to the VFC

Each VFC comes with a single bundled image of VCWare stored in Flash memory. VoIP for the Cisco AS5300 universal access server enables two different ways to copy new versions of VCWare to the VFC Flash memory by:

- Downloading from the Cisco AS5300 Motherboard, page 686
- Downloading from a TFTP Server, page 686

Downloading from the Cisco AS5300 Motherboard

To download from the AS5300 motherboard to Flash memory, use the following commands in privileged EXEC mode:

	Command	Purpose
Step 1	`Router# copy flash: vfc:`	Downloads (copies) the Flash file from the Cisco AS5300 motherboard to the Flash memory on the VFC. **Note** The colons in this command are required.
Step 2	`Router# clear vfc slot`	Reboots the VFC.

Downloading from a TFTP Server

To download the latest version of VCWare from a TFTP server, ensure that the file is stored on the TFTP server. If a copy of the current version of VCWare is resident on disk, store that image on a TFTP server or the file cannot be downloaded into VFC memory. To copy the Flash file from a TFTP server, use the following commands in privileged EXEC mode:

	Command	Purpose
Step 1	`Router# copy tftp: vfc:`	Downloads (copies) the Flash file from a TFTP server to the Flash memory on the VFC. **Note** The colons in this command are required.
Step 2	`Router# clear vfc slot`	Reboots the VFC.

Unbundling VCWare

VCWare must be unbundled before DSPWare can be loaded in Flash memory. The default file and capability lists are created and populated with the appropriate default files for that version of DSPWare. Table 52 shows the files associated with each firmware file.

Table 52 VFC Firmware Filenames

Firmware	Filenames
VCWare	vcw-vfc-mz.c542.t1.6
DSPWare Initialization and Static Files	btl-vfc-l.0.1.bin btj-vfc-l.0.1.bin jbc-vfc-1.3.0.bin cor-vfc-hc-1.3.4.24l.bin
DSPWare Overlay Files	bas-vfc-hc-1.3.4.24l.bin fax-vfc-hc-1.3.4.24l.bin cdc-g711-hc-1.3.4.24l.bin cdc-g726-hc-l.3.4.24l.bin cdc-g729-hc-1.3.4.24l.bin cdc-g728-hc-l.3.4.24l.bin cdc-g723.1-hc-l.3.4.24l.bin

To unbundle the current running image of VCWare, use the following command in privileged EXEC mode:

Command	Purpose
`Router# unbundle vfc slot`	Unbundles the current image of VCWare.

Adding Files to the Default File List

After the VCWare is unbundled, the default file list is automatically created and populated with the default files for VCWare. The default file list indicates which files are initially loaded into DSP at boot up. The following example shows the output from the **show vfc def** command, which displays the contents of the default file list:

```
Router# show vfc 1 def

Default List for VFC in slot 1:
1. btl-vfc-1.0.13.0.bin
2. cor-vfc-1.0.1.bin
3. bas-vfc-1.0.1.bin
4. cdc-g729-1.0.1.bin
5. fax-vfc-1.0.1.bin
6. jbc-vfc-1.0.13.0.bin
```

Under most circumstances, these default files should be sufficient. If needed, files from those stored in VFC Flash memory can be added to the default file list or existing files replaced from the default file list. When a specific file is added to the default file list, it replaces the existing file with the same extension type.

To add a file to the default file list, use the following command in global configuration mode:

Command	Purpose
`Router(config)# default-file filename vfc slot`	Selects a file stored in the Flash memory to be added to the default file list.

Adding Codecs to the Capability List

The capability list defines the set of codecs that can be negotiated for a voice call. Like the default file list, the capability list is created and populated when VCWare is unbundled and DSPWare added to VFC Flash memory. The following example shows the output from the **show vfc cap** command, which displays the contents of the capability list:

```
Router# show vfc 1 cap

Capability List for VFC in slot 1:
1. fax-vfc-1.0.1.bin
2. bas-vfc-1.0.1.bin
3. cdc-g729-1.0.1.bin
4. cdc-g711-1.0.1.bin
5. cdc-g726-1.0.1.bin
6. cdc-g728-1.0.1.bin
7. cdc-gsmfr-1.0.1.bin
```

Codec files can be added, using VFC management, if needed for a specific telephony network.

Note The capability list does not indicate codec preference: it only reports available codecs. The session application decides which codec to use.

To add a codec overlay file to the capability list, use the following command in global configuration mode:

Command	Purpose
`Router(config)# cap-list filename vfc slot-number`	Selects a codec overlay file to be added to the capability list.

Deleting Files from VFC Flash Memory

In some instances, a file may need to be deleted from the default file or capability lists. To delete a file from VFC Flash memory, use the following command in privileged EXEC mode:

Command	Purpose
`Router# delete file-name vfc slot`	Deletes the specified file from VFC Flash memory.

Erasing the VFC Flash Memory

When upgrading the Cisco AS5300 universal access to a more current version of VCWare, new files are stored in VFC Flash and do not overwrite existing files. The contents of VFC Flash memory must be erased to free memory space. To erase the Flash memory of a specific VFC, use the following command in privileged EXEC mode:

Command	Purpose
`Router# erase vfc slot`	Erases the Flash memory on the VFC.

Configuring IVR

Before configuring the Cisco gateways to support IVR, perform the following tasks:

- Configure VoIP to support H.323 compliant gateways, including specific devices in the network to act as gateways, such as configuring dial peers and voice ports.
- Configure a TFTP server to perform storage and retrieval of the required audio files.
- Download the appropriate TCL IVR script from the Cisco.com. Use the **copy** command to copy the audio file (.au file) to Flash memory, and the **audio-prompt load** command to read it into RAM. For more information about copying files into Flash memory, refer to "Copying Flash Files to the VFC" section on page 685.
- Ensure that the audio files are in the proper format. The IVR prompts require audio file (.au) format with 8-bit, u-law, and 8-Khz encoding. To encode the audio files, one of these two audio tools (or a equivalent tool) is recommended:
  - Cool Edit, manufactured by Syntrillium Software Corporation
  - AudioTool, manufactured by Sun Microsystems

- Ensure that the access platform has a minimum of 16 MB of Flash memory and 64 MB of DRAM.
- Install and configure the appropriate RADIUS security server in the network. The version of RADIUS must be able to support IETF-supported Vendor-Specific Attributes (VSAs), which are implemented by using IETF RADIUS Attribute 26.

T.38 Fax Relay for VoIP H.323 Prerequisites

Ensure that the following have been performed or checked before configuring VoIP H.323 for the T.38 fax relay:

- Cisco IOS Release 12.1(3)T is running on the Cisco AS5300 universal access server.
- There is a working VoIP H.323 network for voice calls.
- There has been complete voice interoperability testing with third-party gateways and gatekeepers.
- There is a minimum of 64 MB RAM.

Note Although 96 to 128 MB RAM is recommended, the memory requirement is dependent on the platform and the anticipated number of calls to be made through the system.

Fax Applications Configuration Tasks List

The configuration tasks for fax applications are described in the following sections:

Configuring the On-Ramp Gateway

To configure the on-ramp gateway, perform the tasks described in the following sections:

- Configuring the Called Subscriber Number, page 690 (Required)
- Configuring the Sending MTA, page 690 (Required)
- Configuring POTS Dial Peers, page 691 (Required)
- Configuring MMoIP Dial Peers, page 691 (Required)

Note Before using SMTP in Cisco gateways, be sure to configure the domain name and host name.

Configuring the Called Subscriber Number

To configure the called subscriber number, use the following commands in global configuration mode:

Command	Purpose
`Router(config)# fax receive called-subscriber {$d$ | string}`	Defines the number that is displayed in the LCD of the sending fax machine. This parameter defines the called subscriber identification (CSI).

Configuring the Sending MTA

Defining the originator of the e-mail fax, the destination mail server, the subject of the message, and the postmaster, which is the default mail station for undeliverable e-mail message, is required (Steps 1 through 5). Steps 6 and 7 are optional.

Note The To: address of the fax-mail comes from the **session target** command configured for the MMoIP dial peer for the on-ramp gateway.

To configure the sending MTA, use the following commands in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# mta send mail-from hostname string`	Specifies the originator host name of the e-mail fax message. Use this command with the **mta send mail-from username** command for a complete address.
Step 2	`Router(config)# mta send mail-from {username string | username $s$}`	Specifies the originator username of the e-mail fax message. Use this command with **mta send mail-from hostname** command for a complete address. The keyword **username s** is the calling number.
Step 3	`Router(config)# mta send server {host-name | IP-address}`	Specifies the destination server. **Note** DNS MX records are not used to determine the IP address of the host specified with the **mta send server** command.
Step 4	`Router(config)# mta send subject string`	Defines the text that appears in the subject field of the e-mail fax message.
Step 5	`Router(config)# mta send postmaster e-mail-address`	Defines sending address as the **mta send mail-from** address if the evaluated string is blank.
Step 6	`Router(config)# mta send origin-prefix string`	(Optional) Defines additional identifying information to be prepended to the e-mail header.
Step 7	`Router(config)# mta send return-receipt-to {hostname string username string}`	(Optional) Specifies the address where MDNs are sent, if MDNs are requested.

Configuring POTS Dial Peers

To configure the on-ramp gateway POTS dial peers, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# dial-peer voice number pots`	Defines the POTS dial peer tag number and enters dial-peer configuration mode.
Step 2	`Router(config-dial-peer)# application name`	Associates a specific IVR application with this dial peer. **Note** The **out-bound** keyword is not used with the POTS dial peers, but is used in the MMoIP dial peer configuration.
Step 3	`Router(config-dial-peer)# information-type fax`	Identifies calls associated with this dial peer as being fax transmissions, as opposed to being voice calls.
Step 4	`Router(config-dial-peer)# direct-inward-dial`	(Optional) Specifies DID. If a redialer is not used, DID must be enabled.
Step 5	`Router(config-dial-peer)# incoming called-number string`	Defines the telephone number associated with the POTS dial peer. If DID is enabled, the incoming called number (DNIS number) is used to match the destination pattern of outgoing MMoIP dial peers.
Step 6	`Router(config-dial-peer)# max-conn number`	(Optional) Defines the maximum number of on-ramp connections used simultaneously on this Cisco AS5300 to send fax-mail.

Note E.164 e-mail addresses that are compliant with RFC 2304 use this format: fax=+d@your.hostname.com format. If the off-ramp gateway receives the correct format, it strips the + and matches an off-ramp POTS dial peer with the remaining digits. The number contained in "d" must be a fully qualified E.164 telephone number (that is, it must include the country code) and it must not include an access code (such as "9" to get an outside line).

Configuring MMoIP Dial Peers

To configure the on-ramp gateway MMoIP dial peers, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# dial-peer voice number mmoip`	Defines the MMoIP dial peer tag number and enters dial-peer configuration mode.
Step 2	`Router(config-dial-peer)# application name [out-bound]`	Associates a specific IVR application with this dial peer. If the **out-bound** keyword is used, the named application handles the MMOIP dial peer in the outgoing mode.

	Command	Purpose
Step 3	`Router(config-dial-peer)# destination-pattern [+]string`	Identifies the destination fax telephone number. If DNIS has been enabled, this number should be the same as the configured incoming called number. If DNIS is not enabled, this should be the number from the redialer DNIS.
Step 4	`Router(config-dial-peer)# session target {mailto:{name | $d$}@domain-name | ipv4:destination-address | dns:[$s$. | $d$. | $u$. | $e$.] host-name| loopback:rtp |loopback:compressed | loopback:uncompressed}`	Defines the destination e-mail address for the fax-mail, meaning the e-mail address identifying the SMTP server.
Step 5	`Router(config-dial-peer)# session protocol smtp`	Identifies the session protocol being used between the on-ramp gateway and the remote mail server as SMTP.
Step 6	`Router(config-dial-peer)# image encoding {mh | mr | mmr | passthrough}`	Selects a specific encoding method for the fax-mail messages forwarded via this dial peer.
Step 7	`Router(config-dial-peer)# image resolution {fine | standard | super-fine | passthrough}`	Selects a specific resolution for the TIFF images attached to the fax-mail message forwarded by this dial peer.
Step 8	`Router(config-dial-peer)# max-conn number`	(Optional) Defines the maximum number of connections used simultaneously to send fax-mail.
Step 9	`Router(config-dial-peer)# dsn {delay | failure | success}`	(Optional) Requests that a delivery status notification be generated by the last-hop mailer if the delivery was successful. This DSN is sent to the address specified by the **mta send mail-from** command. Three types of DSNs can be requested: delay, failure, and success. **Note** DSN must be supported by the remote mail server.
Step 10	`Router(config-dial-peer)# mdn`	(Optional) Requests that a message disposition notification be generated by the mail user agent when the message 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. **Note** Return receipt must be supported or initiated by the receiving e-mail client.

Verifying the Gateway Configuration

To verify the gateway configuration, perform the following tasks:

- Verify the configured called-subscriber number using the **debug fax receive called-number** command.
- Check the configured called subscriber number by sending a fax and checking the number in the sending machine LCD.
- Verify that the dial peers have been configured correctly using the **show dialplan number fax** command.

- Display Class 2 fax tracing information on all on-ramp fax connections using the **debug fax receive all** command.
- Display output for all of on-ramp client connections (messages exchanged; for example, the handshake) between the e-mail server and the on-ramp gateway using the **debug mta send all** command.
- Display output for a specific on-ramp SMTP client connection during e-mail transmission using the **debug mta send rcpt-to** command.
- Test connectivity between the on-ramp gateway and the e-mail server by sending a test e-mail to a specified e-mail address and using the **debug mmoip send email** command.
- Make a POTS call to the on-ramp gateway and listen for a secondary dial tone to ascertain if DID is enabled or disabled.

Configuring the Off-Ramp Gateway

To configure the off-ramp gateway, perform the tasks in the following sections:

- Configuring the Transmitting Subscriber Number, page 693 (Required)
- Configuring the Fax Transmission Speed, page 693 (Required)
- Configuring the Receiving Mail Transfer Agent, page 694 (Required)
- Configuring POTS Dial Peers, page 691 (Required)
- Configuring MMoIP Dial Peers, page 691 (Required)
- Configuring the Faxed Header Information, page 695 (Required)
- Configuring the Fax Cover Page Information, page 696 (Required)

Configuring the Transmitting Subscriber Number

To configure the transmitting subscriber number, use the following command in global configuration mode:

Command	Purpose
`Router(config)# fax send transmitting-subscriber {$d$ | string}`	Defines the number that appears in the LCD of the receiving fax device. This parameter defines the transmitting subscriber identification (TSI).

Configuring the Fax Transmission Speed

To configure the fax transmission speed, use the following command in global configuration mode:

Command	Purpose
`Router(config)# fax send max-speed {12000 | 14400 | 2400 | 4800 | 7200 | 7600}`	Specifies the maximum fax speed.

Configuring the Receiving Mail Transfer Agent

To configure the receiving MTA, use the following commands in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# mta receive aliases` *string*	Defines a host name to be used as an alias for the off-ramp Cisco AS5300 universal access server device. Up to ten different aliases can be specified. The Cisco AS5300 universal access server SMTP server accepts only incoming mail if the destination host name of the incoming mail matches one of the aliases as configured by the **mta receive aliases** command. A domain IP address must be explicitly added by enclosing the address in brackets (for example, [xxx.xxx.xxx.xxx]).
Step 2	`Router(config)# mta receive generate-mdn`	(Optional) Configures the Cisco AS5300 universal access server to actually generate an MDN message when requested to do so. Some sites may want to enable or disable this feature depending on the types of mailers in use.
Step 3	`Router(config)# mta receive maximum-recipients` *number*	Defines the number of simultaneous SMTP recipients handled by this device. This is intended to limit the number of resources (modems) allocated for fax transmissions.

Configuring the POTS Dial Peer

To configure the POTS dial peer for the off-ramp gateway, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# dial-peer voice` *number* `pots`	Defines the POTS dial peer tag number and enter dial-peer configuration mode.
Step 2	`Router(config-dial-peer)# information-type fax`	Identifies calls associated with the dial peer as fax transmissions.
Step 3	`Router(config-dial-peer)# destination-pattern` [+]*string*	Identifies the destination fax telephone number.
Step 4	`Router(config-dial-peer)# prefix` *string*	(Optional) Specifies the prefix of the dialed digits associated with the dial peer. If a prefix is configured, the argument *string* is sent to the modem first, before the configured telephone number.

Configuring the MMoIP Dial Peer

To configure the off-ramp gateway MMoIP dial peer, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# dial-peer voice number mmoip`	Defines the MMoIP dial peer tag number and enters dial-peer configuration mode
Step 2	`Router(config-dial-peer)# information-type fax`	Identifies calls associated with this dial peer as being fax transmissions, as opposed to strictly being voice calls.
Step 3	`Router(config-dial-peer)# incoming called-number string`	Identifies the destination fax telephone number.
Step 4	`Router(config-dial-peer)# image resolution {fine | standard | super-fine | passthrough}`	Specifies the fax image resolution for TIFF files associated with this particular MMoIP dial peer. **Note** Only standard and fine fax resolutions are supported.
Step 5	`Router(config-dial-peer)# image encoding {mh | mr | mmr | passthrough}`	Specifies the type of encoding to be used for TIFF files associated with this MMoIP dial peer.
Step 6	`Router(config-dial-peer)# exit`	Exits dial-peer configuration mode.

Note When configuring the MMoIP dial peer, ensure that the **incoming called number** command value and the configured destination telephone number (corresponding on-ramp POTS dial peer) match.

Configuring the Faxed Header Information

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

To configure faxed header information, use the following commands in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# fax send center-header {$a$ | $d$ | $p$ | $s$ | $t$ | string}`	Specifies the header information to be displayed in the center position. The keywords and arguments are as follows: • **d**—Specifies the destination address. • **s**—Specifies the sender address. • **p**—Specifies the page count. • **t**—Specifies the transmission time. • *string*—Inserts a personalized text string.

	Command	Purpose
Step 2	`Router(config)# fax send right-header {$a$ | $d$ | $p$ | $s$ | $t$ | string}`	Specifies the header information to be displayed on the right. Use the *string* argument in this command to insert a personalized text string.
Step 3	`Router(config)# fax send left-header {$a$ | $d$ | $p$ | $s$ | $t$ | string}`	Specifies the header information to be displayed on the left. Use the *string* variable in this command to insert a personalized text string.

Configuring the Fax Cover Page Information

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

To configure fax cover page information, use the following commands in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# fax send coverpage enable`	Enables the off-ramp gateway to send a cover sheet with faxes that originate from e-mail messages.
Step 2	`Router(config)# fax send coverpage comment string`	(Optional) Adds personalized text in the title field of the fax cover sheet.
Step 3	`Router(config)# fax send coverpage show-detail`	(Optional) Prints all of e-mail header information as part of the fax cover sheet text.
Step 4	`Router(config)# fax send coverpage enable`	(Optional) Enables the off-ramp gateway to send a cover page with faxes that originate from e-mail messages.
Step 5	`Router(config)# fax send coverpage e-mail controllable`	(Optional) Configures the router to defer to the cover page setting in the e-mail header. For example, if the address has a parameter set to cover=no or cover=yes, it will override the setting for the **fax send coverpage enable** command.

Verifying the Gateway Configuration

To verify the gateway configuration, perform the following tasks:

- Use **debug fax send calling-number** to check the transmitting subscriber number configuration.
- Use **debug fax send all** to display Class 2 fax protocol tracing information for all off-ramp faxing activities.
- Use **debug mta receive all** to view output relating to the activity on the SMTP server (messages exchanged; for example, the handshake) between the e-mail server and the off-ramp gateway.
- Use **debug text-to-fax** to view information relating to the off-ramp text-to-fax conversion.
- Use **debug tiff reader** to display output about the on-ramp TIFF reader.
- Use **debug tiff writer** to display output about the on-ramp TIFF writer.
- Send an e-mail message to the off-ramp gateway to check whether the fax cover page generates correctly.
- Send a fax-mail using a mail client to the off-ramp gateway and request a return receipt in the e-mail message to check if the fax-mail is processed correctly. The destination e-mail address must have the appropriate fax=user@receive alias to be allowed.

Configuring Gateway Security

To configure gateway security, perform the tasks in the following sections:

- Configuring On-Ramp Gateway Security, page 697 (Required)
- Configuring Off-Ramp Gateway Security, page 698 (Required)
- Configuring the Gateway Security for TCL Application Files, page 699 (Required)

Configuring On-Ramp Gateway Security

To configure on-ramp security, use the following commands in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# aaa new model`	Enables AAA security services.
Step 2	`Router(config)# mmoip aaa method fax authentication` *method-list-name*	Defines the name of the method list to be used for Store and Forward Fax AAA authentication.
Step 3	`Router(config)# mmoip aaa method fax accounting` *method-list-name*	Defines the name of the method list to be used for Store and Forward Fax AAA accounting.
Step 4	`Router(config)# aaa authentication login {default | list-name} method1 [method2...]`	Creates a local authentication method list and enables authentication.
Step 5	`Router(config)# aaa accounting {system | network | exec | connection | commands level} {default | list-name} {stop-only} [method1 [method2...]]`	Creates an accounting method list and enables accounting. We recommend the following configuration: **aaa accounting connection** *list-name* **stop-only**.
Step 6	`Router(config)# mmoip aaa receive-id primary {ani | dnis | gateway | redialer-id | redialer-dnis}`	Specifies the primary location where AAA retrieves its identifying information for on-ramp faxing.
Step 7	`Router(config)# mmoip aaa receive-id secondary {ani | dnis | gateway | redialer-id | redialer-dnis}`	(Optional) Specifies the secondary location where AAA retrieves its identifying information for on-ramp faxing.
Step 8	`Router(config)# mmoip aaa receive-authentication enable`	Enables on-ramp AAA authentication services.
Step 9	`Router(config)# mmoip aaa receive-accounting enable`	Enables on-ramp AAA accounting services.
Step 10	`Router(config)# radius-server host {hostname | ip-address} [auth-port port-number] [acct-port port-number]`	Specifies the IP address or host name of the remote RADIUS server host and assigns authentication and accounting destination port numbers. Typical authentication and accounting destination ports are 1645 and 1646.
Step 11	`Router(config)# radius-server key string`	Specifies the shared-secret text string used between the router and the RADIUS server.
Step 12	`Router(config)# radius-server vsa send accounting`	Enables the network access server to recognize and use accounting VSAs as defined by RADIUS IETF attribute 26.
Step 13	`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.

Configuring Off-Ramp Gateway Security

Note It is recommended that the off-ramp gateway (the packet filters) be configured to accept only incoming SMTP connections (IP addresses) from trusted mailers when faxes are sent to the off-ramp gateway.

To configure off-ramp security, use the following commands in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# aaa new model`	Enables AAA security services.
Step 2	`Router(config)# mmoip aaa method fax authentication` *method-list-name*	Defines the name of the method list to be used for Store and Forward Fax AAA authentication.
Step 3	`Router(config)# mmoip aaa method fax accounting` *method-list-name*	Defines the name of the method list to be used for Store and Forward Fax AAA accounting.
Step 4	`Router(config)# aaa authentication login {default | list-name} method1 [method2...]`	Creates a local authentication method list and enables authentication.
Step 5	`Router(config)# aaa accounting {system | network | exec | connection | commands level} {default | list-name} {stop-only} [method1 [method2...]]`	Creates an accounting method list and enables accounting. It is recommended that **aaa accounting connection** *list-name* **stop-only** be used.
Step 6	`Router(config)# mmoip aaa send-id primary {account-id | envelope-from | envelope-to | gateway}`	Specifies the primary location where AAA retrieves its identifying information for off-ramp faxing.
Step 7	`Router(config)# mmoip aaa send-id secondary {account-id | envelope-from | envelope-to | gateway}`	(Optional) Specifies the secondary location where AAA retrieves its identifying information for off-ramp faxing.
Step 8	`Router(config)# mmoip aaa send-authentication enable`	Enables off-ramp AAA authentication services.
Step 9	`Router(config)# mmoip aaa send-accounting enable`	Enables off-ramp AAA accounting services.
Step 10	`Router(config)# radius-server host {hostname | ip-address} [auth-port port-number] [acct-port port-number]`	Specifies the IP address or host name of the remote RADIUS server host and assigns authentication and accounting destination port numbers. Typical authentication and accounting destination ports are 1645 and 1646.
Step 11	`Router(config)# radius-server key string`	Specifies the shared secret text string used between the router and the RADIUS server.
Step 12	`Router(config)# radius-server vsa send accounting`	Enables the network access server to recognize and use accounting VSAs as defined by RADIUS IETF attribute 26.
Step 13	`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.

Configuring the Gateway Security for TCL Application Files

To configure gateway security for the TCL application files that are used for fax calls on the T.37/T.38 Fax Gateway with a VFC, use the following commands in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# call application voice application-name accounting enable`	Enables AAA accounting services for the named application.
Step 2	`Router(config)# call application voice application-name accounting-list method-list-name`	Defines the name of the method list to be used for AAA accounting with fax applications on a VFC.
Step 3	`Router(config)# call application voice application-name authentication enable`	Enables AAA authentication services for the named application.
Step 4	`Router(config)# call application voice application-name authen-list method-list-name`	Specifies the name of an authentication method list for the named application.
Step 5	`Router(config)# call application voice application-name authen-method id`	Specifies the name of the authentication method for the named application. Valid authentication ids are prompt-user, gateway, ani, dnis, redialer-id, and redialer DNIS.

Verifying the Gateway Security Configuration

To verify the gateway security configuration, perform the following tasks:

- Use the **debug mmoip aaa** command to verify that the on-ramp security is configured correctly.
- Check the console log file, depending upon the RADIUS version used, to verify connection to the RADIUS server.
- Use the **debug aaa** command to verify AAA performance.

Configuring MDNs

Note The MDN elements must be configured for both the on-ramp and off-ramp gateways.

To configure the on-ramp gateway to support MDN, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# mta send return-receipt-to username string`	Specifies the username address. If this field is left blank, the on-ramp gateway inserts the postmaster address in this field as a default.
Step 2	`Router(config)# mta send return-receipt-to hostname string`	Specifies the host name address. If this field is left blank, the on-ramp gateway inserts the postmaster address in this field as a default.

	Command	Purpose
Step 3	`Router(config)# dial-peer voice number mmoip`	Defines the MMoIP dial peer tag number and enters dial-peer configuration mode.
Step 4	`Router(config-dial-peer)# mdn`	Sends the MDN to the destination defined by the **mta send return-receipt-to** command.

To configure the off-ramp gateway to support MDN, use the following command in global configuration mode:

Command	Purpose
`Router(config)# mta receive generate-mdn`	Specifies that the Cisco AS5300 universal access server acting as the off-ramp gateway will respond to a request for an MDN.

Verifying MDN Configuration

To verify the MDN configuration, perform the following tasks:

- Verify if DSN is enabled or disabled using the **show dial-peer voice** command and look at the disposition notification field.
- Verify that the **mta send return-receipt-to username**, **mta send return-receipt-to hostname**, and **mta receive generate-mdn** commands have been configured by using the **show running-config** command.
- Send a fax to the on-ramp gateway. When the destination e-mail account client opens and responds to the MDN request, check the return-receipt-to user account for the MDN response message.
- Send a fax to the off-ramp gateway with MDN requested (return receipt). After the off-ramp gateway has processed the fax-mail message, check the original From: user's account for the MDN response message.

Configuring DSNs

Note The DSN elements must be configured for both the on-ramp and off-ramp gateways.

To configure DSN, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# mta send mail-from {hostname string}`	Specifies the originator (host name portion) of the e-mail fax message. Use this command with the **mta send mail-from username** command to form a complete e-mail address (faxuser@onramp-gateway.com).

	Command	Purpose
Step 2	`Router(config)# mta send mail-from {username string | username $s$}`	Specifies the originator (username portion) of the e-mail fax message. The keyword **s** generates a transmission report that is sent to the originating fax machine. Use this command with the **mta send mail-from hostname** command to form a complete e-mail address (faxuser@onramp-gateway.com).
Step 3	`Router(config)# dial-peer voice number mmoip`	Defines the MMoIP dial peer tag number and enters dial-peer configuration mode.
Step 4	`Router(config-dial-peer)# dsn {delay | success | failure}`	Sends a DSN to the destination defined by the **mta send mail-from** command.

Verifying DSN Configuration

To verify the DSN configuration, perform the following tasks:

- Use the **show dial-peer voice** command and look at the delivery status notification field.
- Use the **show running-config** command to display the **mta send mail-from username** and **mta send mail-from hostname** configurations. If these commands are not configured, the DSN will be delivered to the postmaster defined by the **mta send postmaster** command.
- Use the **show running-config** command to display the **mta send return-receipt-to username**, **mta send return-receipt-to hostname**, and **mta receive generate-mdn** configurations.
- Send a fax to the on-ramp gateway. When the destination e-mail server receives the fax-mail message and responds to the DSN request, check the mail-from or postmaster user account for the DSN response message. (The mail-from or postmaster user account could be a fax machine.)
- Send a fax-mail message to the off-ramp gateway with DSN requested (rcpt to:<fax=555-1212@company.com> NOTIFY=SUCCESS, FAILURE, DELAY). After the off-ramp gateway has processed the fax-mail message, check the original From: user's account for the DSN response message.

Configuring T.37 Store and Forward Fax

The Cisco AS5300 universal access server supports only two modem cards: the Microcom modem card and the MICA technologies modem card. Microcom modem cards support both on-ramp and off-ramp fax activities. MICA technologies modem cards support only off-ramp faxing.

Store and forward fax on-ramp has been designed to work by using direct inward dial (DID) or a redialer. A redialer is a hardware interface device that interconnects between a fax device and the PSTN. If DID is disabled, a redialer must be configured and enabled on the originating fax machine before Store and Forward Fax is operational.

To configure the T.37 Store and Forward Fax application, configure the on- and off-ramp gateways, including gateway security, and perform the following tasks:

- Configuring On-Ramp Modem Pooling, page 702 (Required)
- Configuring ECM, page 702 (Required)

Configuring On-Ramp Modem Pooling

To configure on-ramp modem pooling, use the following commands in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# modem-pool name`	Creates a modem pool.
Step 2	`Router(config)# pool-range number-number`	Assigns a range of modems to the specified modem pool.

Configuring ECM

To configure ECM, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# dial-peer voice 99 voip`	Enters dial peer configuration mode for the VoIP dial peer.
Step 2	`Router(config-dial-peer)# fax-relay ecm disable`	Disables ECM. **Note** Use the **no fax-relay ecm disable** command to enable ECM.

Configuring the T.37/T.38 Fax Gateway

The Cisco AS5300 universal access server must be equipped with 128 MB of RAM in the following situations:

- When a maximum of 120 simultaneous Store and Forward Fax sessions is required
- If IVR Version 2.0 is required

To configure the T.37/T.38 Fax Gateway feature, configure the on- and off-ramp gateways, including gateway security and perform the following tasks:

- Specifying the Interface Type for Fax Calls, page 703 (Required)
- Configuring IVR Functionality, page 703 (Required)
- Configuring T.38 Fax Relay for VoIP H.323, page 705 (Required)

Specifying the Interface Type for Fax Calls

To select the interface type (modem or VFC), use the following command in global configuration mode:

Command	Purpose
`Router(config)# fax interface-type {modem | vfc}`	Specifies the interface type. **Note** On Cisco AS5300 access servers, the keyword **vfc** maps to the **fax-mail** keyword. If you enter the **show run** command, the **fax-mail** keyword will display. The defaults are determined as follows: •If the gateway has modem cards only, the default is the **modem** keyword. •If the gateway has voice cards only, the default is the **vfc** (**fax-mail)** keyword. The **modem** keyword is unavailable. This applies to all platforms except the Cisco AS5300 access server. •If the gateway has both modem and voice cards, the default is the **modem** keyword.

Configuring IVR Functionality

Note All IVR scripts are modified and secured with a proprietary Cisco locking mechanism. Only Cisco internal technical support personnel can open and modify these scripts. TCL must be installed before IVR functionality is configured.

To configure IVR functionality, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# call application voice` *application-name location*	Defines the name to be referenced and indicates the URL of the IVR script to be used. **Note** The *application-name* is a user-defined name which, once defined, is referenced in all other IVR commands except for **application** used with the on-ramp MMoIP dial peer.
Step 2	`Router(config)# call application voice` *application-name* **language** *language*	(Optional) Defines the language of the audio file and passes that information to the application.
Step 3	`Router(config)# call application voice` *application-name* **pin-length** *number*	(Optional) Defines the number of PIN characters and passes that information to the application.
Step 4	`Router(config)# call application voice` *application-name* **retry-count** *number*	(Optional) Defines the number of times a caller is permitted to reenter the PIN and passes that information to the application.
Step 5	`Router(config)# call application voice` *application-name* **uid-length** *number*	(Optional) Defines the number of UID characters and passes that information to the application.

	Command	Purpose
Step 6	`Router(config)# call application voice application-name set-location language category location`	(Optional) Defines the location, language, and category of the audio files and passes that information to the application.
Step 7	`Router(config)# aaa new-model`	Enables AAA security and accounting services.
Step 8	`Router(config)# gw-accounting h323`	Enables gateway-specific H.323 accounting.
Step 9	`Router(config)# aaa authentication login h323 radius`	Defines a method list called **h323** where in RADIUS is defined as the only method of login authentication.
Step 10	`Router(config)# aaa accounting connection h323 start-stop radius`	Defines a method list called **h323** where in RADIUS is used to perform connection accounting, providing start and stop records.
Step 11	`Router(config)# radius-server host ip-address auth-port number acct-port number`	Identifies the RADIUS server and the ports that will be used for authentication and accounting services.
Step 12	`Router(config)# radius-server key key`	Specifies the password used between the gateway and the RADIUS server.
Step 13	`Router(config)# dial peer voice number pots`	Changes mode to dial peer configuration.
Step 14	`Router(config-dial-peer)# port port number`	Defines the voice port associated with the POTS dial peer.
Step 15	`Router(config-dial-peer)# ctrl + z`	Exits to privileged EXEC mode.

Table 53 lists the TCL scripts required for fax applications on VFCs.

Table 53 TCL Scripts Required for VFCs

TCL Script Name	Description—Summary	Commands to Configure
app_libretto_onramp9.tcl	Authenticates the account and PIN using the following: prompt-user, ANI, DNIS, gateway ID, redialer ID, and redialer DNIS.	None
app_libretto_offramp5.tcl	Authenticates the account and PIN using the following: envelope-from, envelope-to, gateway ID, and x-account ID.	None
fax_rollover_on_busy.tcl	Used for on-ramp T.38 fax rollover to T.37 fax when the destination fax line is busy.	**voice hunt user-busy**

Verify the IVR Configuration

To verify the IVR configuration, perform the following tasks:

- Use the **show running-config** to verify the configuration parameters.
- Use the **show call application summary** to display a list of all voice applications.
- Use the **show call application voice** to display the contents of the script.
- Use the **show dial-peer voice** to verify that a dial peer is operational.

Configuring T.38 Fax Relay for VoIP H.323

Only User Datagram Protocol (UDP) is implemented for T.38 Fax Relay for VoIP H.323 gateway support on the multiservice gateways. Transmission Control Protocol (TCP) T.38 Fax Relay is not supported. For further information on T.38 protocol, refer to ITU-T Recommendation.

Voice interoperability testing with third-party gateways and gatekeepers must be completed before configuring the T.38 Fax Relay for VoIP H.323 in the network because different companies are allowed to select certain parts of H.323 and T.38 to implement into their gateways and gatekeepers.

T.38 Fax Relay interoperability requires H.323 Version 2. In addition, T.38 Fax Relay is not supported in the following:

- Cisco MC3810 multiservice concentrators with VCM (Voice Compression Module)
- T.38 Fax Relay is not supported by Multimedia Conference Manager (MCM) H.323 proxy
- T.38 Fax Relay is not supported in conjunction with Media Gateway Control Protocol (MGCP), Simple Gateway Control Protocol (SGCP), or Session Initiation Protocol (SIP)

Configure both the on-ramp and off-ramp gateways to enable T.38 Fax Relay for VoIP H.323. To specify the global default fax protocol for all the VoIP dial peers, use the global configuration mode. To specify the fax protocol for a specific VoIP dial peer, which takes precedence over the global configuration, use dial-peer configuration mode.

Configuring T.38 Fax Relay for VoIP H.323 Globally

To configure T.38 Fax Relay for VoIP H.323 for all the connections of a gateway, which is required, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# voice service voip`	Enters voice-service configuration mode.
Step 2	`Router(config-voi-serv)# fax protocol {cisco | t38 [ls_redundancy value] [hs_redundancy value]}`	Specifies the global default fax protocol. The keywords and arguments are as follows: • **cisco**—Selects the original Cisco proprietary fax protocol. • **t38**—Enables the T.38 Fax Relay protocol. • **ls_redundancy**—(Optional) Sends redundant T.38 fax packets in the low-speed V.21-based T.30 fax machine protocol. • *value*—Specifies redundancy from 0 to 5. The default is 0 (no redundancy). • **hs_redundancy**—Sends redundant T.38 fax packets in the high-speed V.17, V.27, and V.29 T.4 or T.6 fax machine image data. • *value*—Specifies redundancy from 0 to 2. The default is 0 (no redundancy). If set to a value greater than zero, network bandwidth could be increased or consumed.

Configuring T.38 Fax Relay for a Specific Dial Peer

To configure T.38 Fax Relay for VoIP H.323 for a specific dial peer, which is optional, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# dial-peer voice tag voip`	Enters dial-peer configuration mode.
Step 2	`Router(config-dial-peer)# fax protocol {cisco | t38 [ls_redundancy value] [hs_redundancy value] | system}`	Specifies the fax protocol for a dial peer. The keywords and arguments are as follows: • **cisco**—Selects the original Cisco proprietary fax protocol. • **t38**—Enables the T.38 Fax Relay protocol. • **ls_redundancy**—(Optional) Sends redundant T.38 fax packets in the low-speed V.21-based T.30 fax machine protocol. • *value*—Specifies redundancy from 0 to 5. The default is 0 (no redundancy).
		• **hs_redundancy**—Sends redundant T.38 fax packets in the high-speed V.17, V.27, and V.29 T.4 or T.6 fax machine image data. • *value*—Specifies redundancy from 0 to 2. The default is 0 (no redundancy). If set to a value greater than zero, network bandwidth could be increased or consumed. • **system**—Specifies the global default fax protocol used by a dial peer, set by the **fax protocol t.38** command.
Step 3	`Router(config-dial-peer)# fax rate {12000 | 14400 | 2400 | 4800 | 7200 | 9600} {disable | voice} [bytes bytes]`	Selects the maximum fax transmission speed.

Verifying T.38 Fax Relay for VoIP H.323

To verify the T.38 fax relay for VoIP H.323, perform the following tasks:

- Enter the **show running-config** command.
- Enter the **show dial-peer voice** command.

Troubleshooting Tips

To troubleshoot the T.38 Fax Relay for VoIP H.323 feature, perform the following steps:

- Ensure that a voice call can be made.
- Ensure that T.38 Fax Relay for VoIP H.323 is configured on both the on-ramp and off-ramp gateways.
- Ensure that the fax protocol is configured as T.38 in global configuration mode or dial-peer configuration mode for both the on-ramp and off-ramp gateways.

- Use the **debug vtsp session**, **debug cch323 session**, and the **debug cch323 h245** commands to debug a problem.
- Use the **debug voip ccapi inout** command to debug problems while making the call.

Monitoring and Maintaining T.38 Fax Relay for VoIP H.323

To monitor and maintain the T.38 fax relay for VoIP H.323, perform the following tasks:

- Use the **show running-config** command to display the current configuration.
- Use the **show dial-peer voice summary** command to display the configuration information for all dial peers.

Fax Applications Configuration Examples

Configuration examples are provided in the following sections:

- T.37 Store and Forward Fax Configuration Examples, page 707
- T.37/T.38 Fax Gateway Examples, page 714

T.37 Store and Forward Fax Configuration Examples

The following output sample is the configuration of a Cisco AS5300 universal access server acting as an on-ramp gateway in global configuration mode:

```
!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 where 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 5105551212
!
!(Optional) Define the maximum number of connections that will be used simultaneously
!to transmit fax-mail.
 max-conns 10
!
!
!Define an on-ramp MMoIP dial peer.
dial-peer voice 1001 mmoip
!
!Define the telephone number associated with this dial peer.
 destination-pattern 14085554321
!
!Define a destination e-mail address for this dial peer
 session-target mailto:$d$@abccompany.com
!
!(Optional) Request that DSNs be sent.
 dsn
!
!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
```

The following output sample is the configuration of a Cisco AS5300 universal access server acting as the off-ramp gateway beginning in global configuration mode:

```
!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 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 14085556789
!
!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
```

The following sample output is the configuration of the on-ramp and off-ramp gateway for security in global configuration mode:

```
!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 173.13.11.13 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
```

The following sample output is the configuration of the on-ramp modem pool that uses 24 Microcom and 60 MICA modems in global configuration mode:

Note Microcom modems are in slot 1 and MICA modems are in slot 2. The purpose of this named modem pool (mica-inbound) is to prevent fax calls from going to the MICA modems (modems 25 through 84).

```
modem-pool mica-inbound
pool-range 25-84
```

The following sample output is complete Cisco AS5300 universal access server configuration:

```
Router# show running-config

Building configuration...

Current configuration:
!
!Last configuration change at 19:20:39 PST Mon Jul 14 1997
!NVRAM config last updated at 19:11:04 PST Mon Jul 14 1997
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
service udp-small-servers
service tcp-small-servers
!
hostname mmoip-b
!
boot system tftp /auto/annex2/njoffe/c5300-is-mz 255.255.255.255
boot system flash c5300-is-mz
aaa new-model
aaa authentication login fax radius local
aaa accounting connection fax stop-only radius
!
username njoffe password 0 password
username jfitzhug password 0 password
username wooksong password 0 password
username gmercuri password 0 password
```

```
username faryaman password 0 password
username ilyau password 0 password
clock timezone PST -8
clock calendar-valid
!
modem-pool mica-inbound
modem poll time 2
ip subnet-zero
ip host mail-server 10.14.116.1
ip host keyer 223.255.254.254
ip host mail-server.cisco.com 10.14.116.1
ip domain-name cisco.com
ip name-server 10.14.116.1
!
isdn switch-type primary-5ess
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
mta send server mail-server.cisco.com
mta send subject mmoip-b subject line here
mta send origin-prefix Cisco Powered Fax System
mta send postmaster gmercuri@mail-server.com
mta send mail-from hostname mail-from-hostname.com
mta send mail-from username $s$
mta send return-receipt-to hostname mmoip-b.cisco.com
mta send return-receipt-to username $s$
mta receive aliases mmoip-b.cisco.com
mta receive aliases [1.2.3.4]
mta receive aliases cisco.com
mta receive maximum-recipients 24
mta receive generate-mdn
mmoip aaa send-id primary gateway
mmoip aaa receive-id primary gateway
mmoip aaa method fax authentication fax
mmoip aaa method fax accounting fax
mmoip aaa send-accounting enable
mmoip aaa send-authentication enable
mmoip aaa receive-accounting enable
mmoip aaa receive-authentication enable
!
controller T1 0
framing esf
clock source line primary
linecode b8zs
cablelength short 133
pri-group timeslots 1-24
!
controller T1 1
shutdown
framing esf
clock source line secondary 1
linecode b8zs
cablelength short 133
cas-group 0 timeslots 1-24 type e&m-fgb service fax
!
controller T1 2
shutdown
framing esf
linecode b8zs
```

```
cablelength short 133
cas-group 0 timeslots 1-24 type e&m-fgb
!
controller T1 3
shutdown
framing esf
linecode b8zs
cablelength short 133
pri-group timeslots 1-24
!
voice-port 0:D
timeouts call-disconnect 0
!
voice-port 1:0
timeouts call-disconnect 0
!
voice-port 2:0
timeouts call-disconnect 0
!
voice-port 3:D
timeouts call-disconnect 0
!
dial-peer voice 5 mmoip
destination-pattern 55508..
information-type fax
mdn
dsn success
dsn failure
session target mailto:$d$@mail-server.cisco.com
!
dial-peer voice 1001 pots
incoming called-number 571....
port 0:D
!
dial-peer voice 2 pots
incoming called-number 5550839
information-type fax
direct-inward-dial
!
dial-peer voice 1 pots
destination-pattern 5......
information-type fax
prefix 5
!
num-exp 01133...... 33.......
!
interface Loopback0
no ip address
no ip directed-broadcast
!
interface Tunnel1
no ip address
no ip directed-broadcast
!
interface Ethernet0
ip address 10.14.120.2 255.255.0.0
no ip directed-broadcast
!
interface Serial0:23
no ip address
no ip directed-broadcast
encapsulation ppp
no ip route-cache
dialer rotary-group 1
```

```
dialer-group 1
isdn switch-type primary-5ess
isdn tei-negotiation first-call
isdn incoming-voice modem
no fair-queue
!
interface Serial3:23
no ip address
no ip directed-broadcast
shutdown
isdn switch-type primary-5ess
isdn tei-negotiation first-call
no cdp enable
!
interface FastEthernet0
no ip address
no ip directed-broadcast
shutdown
!
interface Group-Async1
ip unnumbered Ethernet0
no ip directed-broadcast
encapsulation ppp
ip tcp header-compression
dialer in-band
dialer-group 1
async mode interactive
peer default ip address pool default
no fair-queue
ppp multilink
group-range 1 12
hold-queue 10 in
!
interface Dialer1
ip unnumbered Loopback0
no ip directed-broadcast
encapsulation ppp
dialer in-band
dialer-group 1
peer default ip address pool def
no fair-queue
ppp multilink
!
ip default-gateway 10.14.0.1
no ip http server
ip classless
ip route 223.255.254.0 255.255.255.0 10.14.0.1
!
dialer-list 1 protocol ip permit
snmp-server engineID local 00000009020000E01EA48784
snmp-server community public RW
radius-server host 10.14.116.1 auth-port 1645 acct-port 1646
radius-server key password
radius-server vsa send accounting
radius-server vsa send authentication
!
line con 0
exec-timeout 0 0
logging synchronous
transport input none
line 1 12
autobaud
autoselect ppp
modem InOut
```

```
modem autoconfigure type microcom_hdms
rotary 1
transport input all
line aux 0
line vty 0 4
exec-timeout 0 0
password password
!
exception core-file /auto/annex2/gmercuri/coredump
exception dump 223.255.254.254
ntp source Ethernet0
ntp update-calendar
ntp peer 223.255.254.254
scheduler heapcheck process
scheduler interval 1000
end
```

T.37/T.38 Fax Gateway Examples

The following output sample shows the configured VFCs on a Cisco AS5300 universal access server:

```
!version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
service udp-small-servers
service tcp-small-servers

hostname fax-gateway

aaa new-model
aaa authentication login fax group radius local
aaa authorization exec fax group radius
aaa accounting connection fax stop-only group radius
enable password lab

username betatest password 0 password

ip subnet-zero
ip host dirt 223.255.254.254
ip domain-name cisco.com
ip name-server 1.14.116.1

mgcp package-capability trunk-package
mgcp default-package trunk-package
isdn switch-type primary-5ess
isdn voice-call-failure 0
```

The following output sample shows the PSTN Fallback from the T.38 Gateway to the T.37 gateway after configuring the **voice hunt user-busy** command. The global service is displayed first as in the following example:

```
voice service voip
 fax protocol t38 ls_redundancy 0 hs_redundancy 0

call application voice app_libretto_offramp5
tftp://dirt/libretto-test/app_libretto_offramp5.tcl
call application voice app_libretto_offramp5 authen-list fax
call application voice app_libretto_offramp5 authen-method gateway
call application voice app_libretto_offramp5 accounting-list fax
```

```
call application voice app_onramp9 tftp://dirt/libretto-test/app_libretto_onramp9.tcl
call application voice app_onramp9 authen-list fax
call application voice app_onramp9 authen-method gateway
call application voice app_onramp9 language 1 en
call application voice app_onramp9 accounting-list fax
call application voice app_onramp9 set-location en 0 tftp://dirt/cchiu/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 Cisco cover page comment
fax interface-type vfc
mta send server 1.14.116.1
mta send subject faxmail subject line here
mta send origin-prefix Cisco Powered Fax System
mta send postmaster postmaster@mail-server.cisco.com
mta send mail-from hostname fax-gateway.com
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 mmoip-b.cisco.com
mta receive aliases cisco.com
mta receive aliases [1.14.120.2]
mta receive maximum-recipients 80
mta receive generate-mdn

controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 pri-group timeslots 1-24

interface Ethernet0
 ip address 1.14.120.2 255.255.0.0
 no ip directed-broadcast

interface Serial0:23
 no ip address
 no ip directed-broadcast
 no ip route-cache
 isdn switch-type primary-5ess
 isdn incoming-voice modem
 no fair-queue

interface FastEthernet0
 no ip address
 no ip directed-broadcast
 shutdown
 duplex auto
 speed auto

ip default-gateway 1.14.0.1
ip classless
ip route 223.255.254.0 255.255.255.0 1.14.0.1
no ip http server

radius-server host 1.14.116.1 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key password
radius-server vsa send accounting
```

```
radius-server vsa send authentication

voice-port 0:D
 no modem passthrough

!Inbound Peer of the T.37 On-Ramp Gateway
dial-peer voice 2 pots
    application app_onramp9
     incoming called-number 5......
     direct-inward-dial
!Outbound Peer of the T.37 On-ramp Gateway
dial-peer voice 3 mmoip
!MDN and DSN Configuration of the Outbound Peer
 application fax_on_vfc_onramp_app out-bound
     destination-pattern 57108..
     session target mailto:$d$@mail-server.cisco.com
!Inbound Peer of the T.37 Off-Ramp Gateway
dial-peer voice 21 mmoip
     application lib_off_app5
     incoming called-number 5......
     information-type fax
!Outbound Peer of the T.37 Off-Ramp Gateway
!POTS 20 peer has port 0:D which means that when this peer is matched, controller T1-0 is
!used for the outgoing call:
dial-peer voice 20 pots
     destination-pattern 5......
     port 0:D
     prefix 5
!Inbound Peer for T.38 On-ramp Gateway
dial-peer voice 50 pots
     incoming called-number 1800555....
!Outbound Peer for On-Ramp Gateway
    dial-peer voice 51 voip
     destination-pattern 57108..
     session target ipv4:12.22.95.20
!Inbound Peer for Off-Ramp Gateway
    dial-peer voice 61 voip
     incoming called-number 57108..
!Outbound Peer for Off-Ramp Gateway
    dial-peer voice 60 pots
     destination-pattern 57108..
     port 0:D
     prefix 57108
!On-Ramp T.38 Fax Rollover to T.37
!Voice hunt user-busy is set first.
!Inbound peer of the T.37/T.38 on-ramp gateway
    dial-peer voice 70 pots
     application app_lib_rollover15
     incoming called-number 5......
!Outbound peer of the T.38 on-ramp gateway:
    dial-peer voice 71 voip
     preference 1
     destination-pattern 3746096
     session target ipv4:1.14.120.109
     fax protocol t38 ls_redundancy 0 hs_redundancy 0
!Outbound peer of the T.37 on-ramp gateway:
    dial-peer voice 72 mmoip
     preference 2
    application fax_on_vfc_onramp_app out-bound
     destination-pattern 3746096
     session target mailto:$d$@mail-server.cisco.com

    line con 0
     exec-timeout 0 0
```

```
 transport input all
line aux 0
line vty 0 4
 exec-timeout 0 0
 password password
end
```

T.38 Fax Relay for VoIP H.323 Configuration Example

This section provides configuration examples of T.38 Fax Relay:

```
Router# show running-config
Building configuration...

Current configuration:
.
.
.
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
```