



T.37/T.38 Fax Gateway

This document provides the required information for configuration of a T.37/T.38 Fax Gateway on a Voice Feature Card (VFC) installed in the Cisco AS5300 access server. Store-and-forward fax, previously documented in the *Cisco IOS Multiservice Applications Configuration Guide*, enables Cisco AS5300s to send and receive faxes across packet-based networks. This document includes the following sections:

- Feature Overview, page 1
- Supported Platforms, page 4
- Supported Standards, MIBs, and RFCs, page 4
- Prerequisites, page 5
- Configuration Tasks, page 13
- Configuration Examples, page 35

Feature Overview

When the Cisco AS5300 is equipped with VFCs, it supports carrier-class Voice over IP (VoIP) and fax over IP services. Since the Cisco AS5300 is H.323 compliant, it supports a family of industry-standard voice codecs and provides echo cancellation and Voice Activity Detection (VAD)/silence suppression. There is an Interactive Voice Response (IVR) application that provides voice prompts and digit collection in order to authenticate the user and identify the call destination.

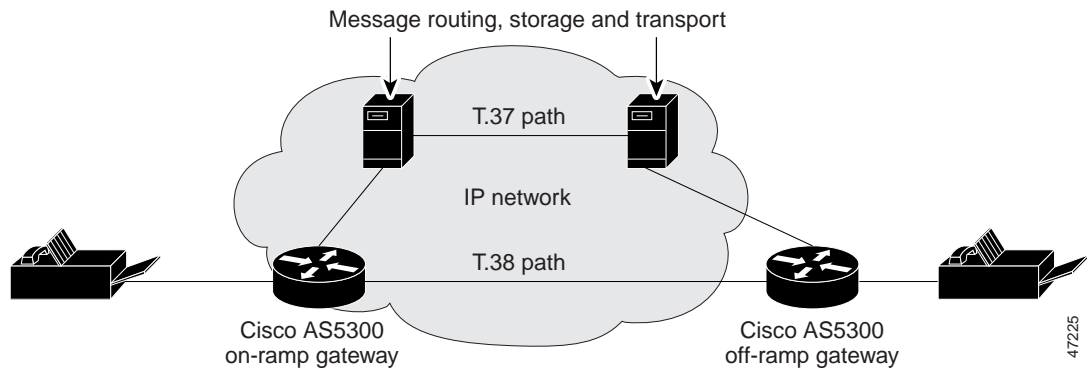
The VFC is a co-processor card with a powerful Reduced Instructions Set Computing (RISC) engine and dedicated, high-performance Digital Signal Processors (DSPs) to ensure predictable, real-time voice processing. The design enables steamlined packet forwarding. The Cisco AS5300 supports two VFCs that are scalable up to 96 E1 or 120 T1 voice connections within a single chassis.

Previously store-and-forward fax was supported only on modem cards while 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:

- Voice, fax relay, and 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 store-and-forward fax).

Figure 1 highlights the real-time (T.38 path) versus the store-and-forward processing (T.37 path) for fax transactions over IP networks.

Figure 1 Real-time versus Store-and-Forward Fax Processing



Previously, 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 Extended Simple Mail Transfer Protocol (ESMTP) store and forward method. The on-ramp gateway router accepted fax data from the PSTN fax machine.

It converted the fax data into a TIFF attachment in a MIME e-mail message and transmitted it to a store and forward SMTP server. These servers would deliver the faxmail message to the off-ramp gateway router. Once the off-ramp gateway router received the faxmail message, it processed the message and initiated a session with the destination fax machine.

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



Note

It is strongly recommended that the Cisco AS5300 access server packet filters be configured to accept only incoming SMTP connections from trusted mailers (off-ramp gateway).

To configure store-and-forward fax, the VoIP software component must be installed and functional on the Cisco AS5300.

Using Interactive Voice Response for Call Processing

IVR applications control calls in the T.37/T.38 Fax Gateway. They can be assigned to specific ports or invoked based on DNIS and accommodate many gateway services by customizing the presentation of the interfaces to callers.

IVR uses Tool Control 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.



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.

Benefits

Cost Savings and Port Density

The cost of maintaining two architectures, one for voice and one for fax, is eliminated. Service providers can use a single port for both voice, fax relay, and store-and-forward fax. For smaller POPs, the single-port configuration for both technologies is even more significant because mixed traffic can be handled more efficiently (only a single pool of ports versus splitting traffic across two pools).

Single Number for Voice and Fax Access

Service providers can 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 DNIS numbers and dial peers as would be required with separate voice and fax applications.

Switch from Fax Relay to Store-and-Forward Fax

Service providers can 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 store-and-forward fax.

Restrictions

The Cisco AS5300 access server must be equipped with 128 MB of Random Access Memory (RAM) in the following situations:

- When a maximum of 120 store-and-forward fax simultaneous sessions is required.
- If IVR Version 2.0 is required.

Related Features and Technologies

Store-and-forward fax and fax relay make use of and are related to the following features and technologies:

- Dial peers
- Destination patterns and prefixes
- Number expansion
- Cisco VoIP
- IVR
- Authentication, Authorization, and Accounting (AAA) security services
- RADIUS security server protocol

Related Documents

For related information on this feature, refer to the following documents:

- New feature documentation for Cisco IOS Release 12.1(1)T, *Store and Forward Fax with ESMTP*
- New feature documentation for Cisco IOS Release 12.0(3)T *Voice over IP for the Cisco AS5300*
- *Cisco IOS Multiservice Applications Configuration Guide*, Release 12.1
- *Cisco IOS Multiservice Applications Command Reference*, Release 12.1
- *Cisco IOS Security Configuration Guide*, Release 12.1
- *Cisco IOS Security Command Reference*, Release 12.1
- Cisco AS5300 Universal Access Server Software Configuration Guide
- Cisco AS5300 Universal Access Server Module Installation Guide

Supported Platforms

- Cisco AS5300

Supported Standards, MIBs, and RFCs

Standards

- ITU-T.37—*Procedures for the Transfer of Facsimile Data Via Store-and-forward on the Internet*, June 1998
- ITU-T.38—*Procedures for Real-time Group 3 Facsimile Communication over IP Networks*, June 1998
- ITU-T.38—*Procedures for Real-time Group 3 Facsimile Communication over IP Networks, Amendment 1*, April 1999
- ITU-T.38—*Revised Annex B of Recommendation T.38*, November 1998

MIBs

For descriptions of supported MIBs and how to use MIBs, see the Cisco MIB web site on CCO at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

RFCs

- RFC 821, *Simple Mail Transfer Protocol*
- RFC 822, *Standard for the Format of ARPA Internet Text Messages*
- RFC 1652, *SMTP Service Extension for 8bit-MIME Transport*
- RFC 1869, *SMTP Service Extensions*
- RFC 1891, *SMTP Service Extension for Delivery Status Notifications*
- RFC 1892, *The Multipart/Report Content Type for the Reporting of Mail System Administrative Messages*
- RFC 1893, *Enhanced Mail System Status Codes*

- RFC 1894, *An Extensible Message Format for Delivery Status Notifications*
- RFC 1896, *The Text/Enriched MIME Content-Type*
- RFC 2034, *SMTP Service Extension for Returning Enhanced Error Codes*
- RFC 2045, *Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies*
- RFC 2046, *Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types*
- RFC 2047, *MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text*
- RFC 2197, *SMTP Service Extension for Command Pipelining*
- RFC 2298, *An Extensible Message Format for Message Disposition Notifications*
- RFC 2301, *File Format for Internet Fax*
- RFC 2302, *Tagged Image File Format (TIFF) - Image/TIFF MIME Sub-Type Registration*
- RFC 2303, *Minimal PSTN Address Format in Internet Mail*
- RFC 2304, *Minimal Fax Address Format in Internet Mail*
- RFC 2305, *A Simple Mode of Fax Using Internet Mail*
- RFC 2532, *Extended Facsimile Using Internet Mail*

Store-and-forward fax is also compliant with the SMTP requirements in RFC 1123, *Requirements for Internet Hosts—Application and Support*.

Prerequisites

Before configuring the T.37/T.38 Fax Gateway on a Cisco AS5300 VFC, the following tasks must be completed:

- Downloading VCWare to the VFC
- Copying Flash Files to the VFC
- Unbundling VCWare
- Configuring the Fax Gateway to Support IVR

These tasks are described in the following sections.



Note

Before using SMTP in Cisco gateways, configure the domain name and host name configured.

VFCs for the Cisco AS5300 come with a single bundled image of VCWare stored in VFC Flash memory. Table 1 shows the extension types defined for these embedded firmware files.

Table 1 VFC Firmware Extensions

Firmware	Filenames	Description
VCWare	vcw-vfc-*	Latest version of VCWare stores in Flash memory, including: <ul style="list-style-type: none"> • Datapath engine • Message dispatcher • DSP manager • VC manager • Process scheduler
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 into 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 filenames indicating which files are initially loaded into DSP upon bootup, and the capability list defines the set of codecs that can be negotiated for a voice call.

VFC management enables:

- Adding versions of VCWare to Flash memory (downloads and unbundles files).
- Erasing files contained in Flash memory.
- Adding files to the default file and capability lists.
- Deleting files from the default file lists and capability lists.

These tasks are described in the following sections:

- Downloading VCWare to the VFC
- Copying Flash Files to the VFC
- Unbundling VCWare
- Adding Files to the Default File List
- Adding Codecs to the Capability List
- Deleting Files from VFC Flash Memory
- Erasing the VFC Flash Memory
- Configuring the Fax Gateway to Support IVR

Downloading VCWare to the VFC

Before downloading VCWare to the VFC, determine that 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.

These are required tasks:

- Determine the Number of VFCs
- Identify the VFC Mode
- Download the Software in VCWare Mode
- Download the Software in ROM Monitor Mode

Determine 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# <code>show vfc slot directory</code>	Determines the number of installed VFCs and their location.

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

Identify the VFC Mode

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


Command	Purpose
Router# <code>show vfc slot board</code>	Determines whether your VFC is operating in VCWare mode or ROM Monitor mode.

If the mode is VCWare, the VFC status is “VCWARE running.” If the mode is ROM Monitor, the VFC status will be “ROMMON.”

Download the Software in VCWare Mode

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

	Command	Purpose
Step 1	Router# <code>erase vfc slot</code>	Erases the Flash memory.
Step 2	Router# <code>show vfc slot directory</code>	Verifies that the VFC Flash memory is indeed empty.

	Command	Purpose
Step 3	Router# <code>copy tftp: vfc:</code> or Router# <code>copy flash: vfc:</code>	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# <code>clear vfc slot</code>	Reboots the VFC.
Step 5	Router# <code>show vfc slot board</code>	Checks whether the VFC is back up in VCWare mode.
Step 6	Router# <code>show vfc slot directory</code>	Verifies that VCWare is in the VFC Flash.
Step 7	Router# <code>unbundle vfc slot</code>	Unbundles the DSPWare from the VCWare and configures the default file list and the capability list.
Step 8	Router# <code>show vfc slot directory</code>	Verifies that the DSPWare has been unbundled.
Step 9	Router# <code>show vfc slot default-list</code>	Verifies that the default file list has been populated.
Step 10	Router# <code>show vfc slot cap-list</code>	Verifies that the capability list has been populated.


Reboot the Cisco AS5300 for these changes to 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-.”

Download the Software in ROM Monitor Mode

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

	Command	Purpose
Step 1	Router# <code>clear vfc slot purge</code>	Erases the VFC Flash memory.
Step 2	Router# <code>copy tftp: vfc:</code> or Router# <code>copy flash: vfc:</code>	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# <code>clear vfc slot</code>	Reboots the VFC.
Step 4	Router# <code>show vfc slot board</code>	Checks whether the VFC is back up in VCWare mode.
Step 5	Router# <code>show vfc slot directory</code>	Verifies that VCWare is in the VFC Flash.

	Command	Purpose
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	Verifies that the DSPWare has been unbundled.
Step 8	Router# show vfc slot default-list	Verifies that the default file list has been populated.
Step 9	Router# show vfc slot cap-list	Verifies that the capability list has been populated.

Reboot the Cisco AS5300 for these changes to 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 enables two different ways to copy new versions of VCWare to the VFC Flash memory by:

- Downloading from the AS5300 Motherboard
- Downloading from a TFTP Server


Downloading from the AS5300 Motherboard

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

	Command	Purpose
Step 1	Router# copy flash vfc:	Downloads (copies) the Flash file from the AS5300 motherboard to the Flash memory on the VFC.
		 Note The colon in this command is 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 command in privileged EXEC mode:

	Command	Purpose
Step 1	Router# <code>copy flash vfc:</code>	Downloads (copies) the Flash file from a TFTP server to the Flash memory on the VFC.  Note The colon in this command is required.
Step 2	Router# <code>clear vfc slot</code>	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 1 shows the files associated with each firmware file.

Table 2 VFC Firmware Filenames

Firmware	Filenames
VCWare	vcw-vfc-mz.c542.t1.6
DSPWare Initialization and Static Files	bt1-vfc-1.0.1.bin btj-vfc-1.0.1.bin jbc-vfc-1.3.0.bin cor-vfc-hc-1.3.4.241.bin
DSPWare Overlay Files	bas-vfc-hc-1.3.4.241.bin fax-vfc-hc-1.3.4.241.bin cdc-g711-hc-1.3.4.241.bin cdc-g726-hc-1.3.4.241.bin cdc-g729-hc-1.3.4.241.bin cdc-g728-hc-1.3.4.241.bin cdc-g723.1-hc-1.3.4.241.bin

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

Command	Purpose
Router# <code>unbundle vfc slot</code>	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 that version of VCWare. The default file list indicates which files are initially loaded into DSP at startup. 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 can be added from those stored in VFC Flash memory 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 default for that 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 <i>filename</i> vfc <i>slot-number</i>	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 <i>file-name</i> vfc <i>slot</i>	Deletes the specified file from VFC Flash memory.

Erasing the VFC Flash Memory

When upgrading 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 <i>slot</i>	Erases the Flash memory on the VFC.

For more information about VFC management commands, refer to the *Cisco IOS Multiservice Applications Command Reference* publication.

Configuring the Fax Gateway to Support IVR

Before configuring the Cisco gateway to support IVR, perform the following:

- 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 classic or TCL IVR script from the CCO Software Support Center. 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 9.
- 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, it is recommended that one of these two audio tools (or a similar tool of comparable quality) be used:
 - 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 VSAs, which are implemented by using IETF RADIUS Attribute 26.

Configuration Tasks

The configuration tasks that must be performed are:

- Specifying the Interface Type for Fax Calls
- Configuring IVR Functionality
- Configuring the On-Ramp Gateway
- Configuring the Off-Ramp Gateway
- Configuring the Gateway Security
- Configuring MDN
- Configuring DSN

Specifying the Interface Type for Fax Calls

To select the VFC, use the following command in global configuration mode:

Command	Purpose
Router(config)# fax interface-type vfc	Specifies a VFC. On the Cisco AS5300 access server, the keyword vfc maps to the fax-mail keyword. If you enter the show run command, the fax-mail keyword will display.

Configuring IVR Functionality

To configure IVR functionality using either classic or TCL scripts, perform the following:

- Create an application that interacts with the appropriate classic or TCL script. Use **show call application voice** to view the contents of the TCL IVR script.
- Define and pass the defined parameter values to the application. Depending on the selected TCL script, these values can include the language of the audio file and the location of the audio file. Table 3 on page 15 lists the required TCL scripts and the parameter values.
- Associate the application to the incoming POTS dial peer.
- Define the appropriate method lists using AAA so that RADIUS is identified as the security protocol performing accounting.

To configure IVR functionality, use the following commands, beginning in privileged EXEC mode:


	Command	Purpose
Step 1	Router# configure terminal	Enters global configuration mode.
Step 2	Router(config)# call application voice <i>application-name location</i>	Defines the name to be referenced and indicates the URL of the IVR script to be used.  Note The <i>application-name</i> 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 3	Router(config)# call application voice <i>application-name language language</i>	(Optional) Defines the language of the audio file and passes that information to the application.
Step 4	Router(config)# call application voice <i>application-name pin-length number</i>	(Optional) Defines the number of PIN characters and passes that information to the application.
Step 5	Router(config)# call application voice <i>application-name retry-count number</i>	(Optional) Defines the number of times a caller is permitted to reenter the PIN and passes that information to the application.
Step 6	Router(config)# call application voice <i>application-name uid-length number</i>	(Optional) Defines the number of UID characters and passes that information to the application.
Step 7	Router(config)# call application voice <i>application-name set-location language category location</i>	(Optional) Defines the location, language, and category of the audio files and passes that information to the application.
Step 8	Router(config)# aaa new-model	Enables AAA security and accounting services.
Step 9	Router(config)# gw-accounting h323	Enables gateway-specific H.323 accounting.
Step 10	Router(config)# aaa authentication login h323 radius	Defines a method list called h323 where RADIUS is defined as the only method of login authentication.
Step 11	Router(config)# aaa accounting connection h323 start-stop radius	Defines a method list called h323 where RADIUS is used to perform connection accounting, providing start-stop records.
Step 12	Router(config)# radius-server host <i>ip-address</i> auth-port <i>number</i> acct-port <i>number</i>	Identifies the RADIUS server and the ports that will be used for authentication and accounting services.
Step 13	Router(config)# radius-server key <i>key</i>	Specifies the password used between the gateway and the RADIUS server.
Step 14	Router(config)# dial peer voice <i>number</i> pots	Changes mode to dial peer configuration.
Step 15	Router(config-dial-peer)# port <i>port number</i>	Defines the voice port associated with the POTS dial peer.
Step 16	Router(config-dial-peer)# ctrl + z	Exits to privileged EXEC mode.

Table 3 lists the required TCL scripts for fax applications on VFCs.

Table 3 Required TCL Scripts 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

Use the following commands to verify the IVR configuration:

- **Show running configuration** – verifies the configuration parameters.
- **Show call application summary** – displays a list of all voice applications.
- **Show call application voice** – shows the contents of the script.
- **Show dial-peer voice** – verifies that dial peer is operational.

Configuring the On-Ramp Gateway

When acting as the on-ramp gateway, the Cisco AS5300 receives faxes from end users, converts them into TIFF files, creates standard MIME e-mail messages, attaches the TIFF files to the e-mail messages, and forwards the fax-mail messages to the designated SMTP server for storage.

The gateway uses the sending MTA and dial peers to complete these tasks. The sending MTA, which is the Cisco AS5300, defines delivery parameters associated with the e-mail message to which the fax TIFF file is attached. The delivery parameters include defining a return e-mail path or designating a destination mail server.



Note

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

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

- Configuring the Called Subscriber Number
- Configuring the Sending MTA
- Configuring the POTS Dial Peer
- Configuring the MMoIP Dial Peer
- Verifying the On-Ramp Gateway Configuration
- Verifying the On-Ramp Gateway Configuration

Configuring the Called Subscriber Number

The called subscriber number is the number displayed in the LCD of the fax device when a fax is sent to a recipient. Typically, with a standard Group 3 fax device, this is the telephone number associated with the receiving fax device. To configure the called subscriber number, use the following commands beginning in privileged EXEC mode:

	Command	Purpose
Step 1	Router# configure terminal	Enters global configuration mode.
Step 2	Router(config)# fax receive called-subscriber { \$d\$ <i>string</i> }	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

MTAs define the elements of the e-mail message to which the fax TIFF file is attached, which includes:

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



Note

The **mta send mail-from username** and **mta send mail-from hostname** commands configure the From: username. The To: address is configured with **session target** and is the on-ramp gateway MMoIP dial peer.

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

	Command	Purpose
Step 1	Router(config)# mta send mail-from <i>hostname string</i>	Specifies the originator (host name) of the e-mail fax message. This information appears in the RFC 822 From: field and the RFC 821 MAIL FROM field of the e-mail fax message. This information is also used for generating DSNs. When the mta send mail-from hostname command is configured, the configured host name is used with the mta send mail-from username command to form a complete e-mail address, like <code>faxuser@onramp-gateway.com</code> .
Step 2	Router(config)# mta send mail-from { <i>username string</i> username <i>\$\$</i> }	Specifies the originator (username portion) of the e-mail fax message. This information appears in the RFC 822 From: field and the RFC 821 MAIL FROM field of the e-mail fax message. This information is also used for generating DSNs. When the mta send mail-from username command is configured, the configured username is used with the mta send mail-from hostname command to form a complete e-mail address, like <code>faxuser@onramp-gateway.com</code> .
Step 3	Router(config)# mta send server { <i>host-name</i> <i>IP-address</i> }	Specifies the destination server. 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 <i>string</i>	Defines the text that appears in the Subject field of the e-mail fax message.
Step 5	Router(config)# mta send postmaster <i>e-mail-address</i>	Defines address to be used as the mta send mail-from address if the evaluated string is blank. An address such as <code>fax-administrator@example.com</code> is recommended (where <code>company.com</code> is replaced with the domain name, and <code>fax-administrator</code> is aliased to the person responsible for the operation of the Cisco AS5300 fax functions). At some sites this may be the same person as the e-mail postmaster, but at most sites this is likely to be a different person.
Step 6	Router(config)# mta send origin-prefix <i>string</i>	(Optional) Defines additional identifying information to be prepended to the e-mail header.
Step 7	Router(config)# mta send return-receipt-to { <i>hostname string</i> <i>username string</i> }	(Optional) Specifies the address where MDNs are sent.

Configuring the POTS Dial Peer

To configure the POTS dial peer, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# dial-peer voice <i>number</i> pots	Defines the POTS dial peer tag number and enters dial-peer configuration mode.
Step 2	Router(config-dial-peer)# application <i>name</i>	Associates a specific IVR application with this dial peer. 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 you are not using a redialer, you must enable DID to use store-and-forward fax.
Step 5	Router(config-dial-peer)# incoming called-number <i>string</i>	Defines the telephone number associated with the POTS dial peer—in store-and-forward fax, 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 <i>number</i>	(Optional) Defines the maximum number of on-ramp connections used simultaneously on this Cisco AS5300 to send fax-mail.
Step 7	Router(config-dial-peer)# exit	Exits dial-peer configuration mode.

Configuring the MMoIP Dial Peer

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

	Command	Purpose
Step 1	Router(config)# dial-peer voice <i>number</i> mmoip	Defines the MMoIP dial peer tag number and enters dial-peer configuration mode.
Step 2	Router(config-dial-peer)# application <i>name</i> [out-bound]	Associates a specific IVR application with this dial peer. If the out-bound keyword is used, the named application will handle the MMoIP dial peer in the outgoing mode.
Step 3	Router(config-dial-peer)# destination-pattern <i>[+]string</i>	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: { <i>name</i> \$d\$ }@ <i>domain-name</i> ipv4: <i>destination-address</i> dns: { \$s\$. \$d\$. \$u\$. \$e\$.} <i>host-name</i> 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.

	Command	Purpose
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 vis this dial peer.
Step 8	Router(config-dial-peer)# max-conn <i>number</i>	(Optional) Defines the maximum number of connections used simultaneously on this Cisco AS5300 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. 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. Return receipt must be supported/initiated by the receiving e-mail client.
Step 11	Router(config-dial-peer)# exit	Exits the dial-peer configuration mode.

Verifying the On-Ramp Gateway Configuration

To verify the on-ramp gateway configuration, perform the following:

- Use **debug fax receive called-number** to verify the configured called-subscriber number.
- Check the configured called subscriber number by sending a fax and checking the number in the sending machine LCD.
- Use **show dialplan number fax** to verify that store-and-forward fax dial peers have been configured correctly.
- Use **debug fax receive all** to display Class 2 fax tracing information on all on-ramp fax connections.
- Use **debug mta send all** to display output for all of the on-ramp client connections (messages exchanged, for example, the handshake) between the e-mail server and the on-ramp gateway.
- Use **debug mta send rcpt-to** to display output for a specific on-ramp SMTP client connection during e-mail transmission.
- 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 **debug mmoip send email**.
- Make a POTS call and listen for a secondary dial tone to determine if DID is enabled or disabled. If DID is disabled, the server presents a dial tone to collect the digits.

Configuring the Off-Ramp Gateway

Off-ramp faxing requires that the Cisco AS5300 act as an off-ramp gateway to dial the POTS and communicate with a remote fax machine (Group 3 fax device), using standard fax protocols. The off-ramp gateway:

- 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 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, dial peers, and commands specific to formatting the appended information and generating a fax cover sheet 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. As an option, the MMoIP dial peers can be configured, but MMoIP dial peers has limited functionality. It only defines 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. This can be its SMTP host aliases, which can be different than its normal DNS host names, or internal Cisco IOS host name.

**Note**

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 converts the e-mail to fax format, it also converts the attached TIFF file to standard Group 3 fax format.

The off-ramp POTS dial peer defined the telephone number of the destination fax device. Because a destination pattern is defined for an outbound POTS peer, number expansion can be used.

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

- Configuring the Transmitting Subscriber Number
- Configuring the Fax Transmission Speed
- Configuring the Receiving Mail Transfer Agent
- Configuring the POTS Dial Peer
- Configuring the MMoIP Dial Peer
- Configuring the Faxed Header Information (fax transmission originates as an e-mail message)
- Configuring the Fax Cover Page Information (fax transmission originates as an e-mail message)
- Verifying the Off-Ramp Gateway Configuration

Configuring the Transmitting Subscriber Number

The first step in configuring the off-ramp gateway, whether the off-ramp gateway is converting a fax TIFF file to a standard fax or sending an e-mail message as a fax, is to configure the transmitting subscriber number.

The transmitting subscriber number is displayed 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.

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

Command	Purpose
Router(config)# fax send transmitting-subscriber { <i>\$d\$</i> <i>string</i> }	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

Next, configure the maximum speed of the fax transmission. This 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.

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 speed at which an off-ramp fax is sent.

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 <i>string</i>	<p>Defines a host name to be used as an alias for the off-ramp Cisco AS5300 device. You can define up to ten different aliases.</p> <p>The Cisco AS5300 SMTP server will only accept incoming mail if the destination host name of the incoming mail matches one of the aliases as configured by the mta receive aliases command.</p> <p>This command does not automatically include reception for a domain IP address—it must be explicitly added. If you add an IP address, you must enclose the address in brackets as follows: [xxx.xxx.xxx.xxx].</p>

	Command	Purpose
Step 2	Router(config)# mta receive generate-mdn	(Optional) Configures the Cisco AS5300 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 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)# application name	Associates a specific IVR application with this dial peer. The out-bound keyword is not used with POTS dial peers, but is used with MMoIP dial peers.
Step 3	Router(config-dial-peer)# destination-pattern [+] string	Identifies the destination fax telephone number.
Step 4	Router(config-dial-peer)# port controller number	(Optional) Specifies the T1 controller port through which to route the outgoing fax calls for this dial peer.
Step 5	Router(config-dial-peer)# prefix number	(Optional) Specifies the prefix of the dialed digits associated with this dial peer. If you configure a prefix, when an outgoing call is initiated, the prefix <i>string</i> value is sent to the VFC first, before the telephone number configured for this dial peer.

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)# application name [out-bound]	Associates a specific IVR application with this dial peer. If the out-bound keyword is used, the named application uses the MMoIP dial peer in the outgoing mode.
Step 3	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 4	Router(config-dial-peer)# incoming called-number string	Identifies the destination fax telephone number.

Command	Purpose
Step 5 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 for Cisco IOS Release 12.1.
Step 6 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 7 Router(config-dial-peer)# exit	Exits the 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

Store-and-forward fax converts standard e-mail messages into fax transmissions. When a fax is sent using a standard Group 3 device, there is usually header information appended to the top of each faxed cover and text page, indicating the telephone number of the sending fax device, the date, and the time of transmission. These faxes require that header information is appended to each faxed page.

Store-and-forward fax configures what header information is appended to the top of each faxed cover and text page, along with its placement. Also, the destination address of an e-mail message can control the cover page generation on a per-recipient basis.



Note 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\$ <i>string</i> }	Specifies the header information to be displayed in the center position. The wildcards used in this command are used to insert the following information: <ul style="list-style-type: none"> • \$a\$—date • \$d\$—destination address • \$s\$—sender address • \$p\$—page count • \$t\$—transmission time Use the <i>string</i> argument in this command to insert personalized text string.

	Command	Purpose
Step 2	Router(config)# fax send right-header {\$a\$ \$d\$ \$p\$ \$s\$ \$t\$ <i>string</i> }	<p>Specifies the header information to be displayed on the right. The wildcards used in this command are used to insert the following information:</p> <ul style="list-style-type: none"> • \$a\$—date • \$d\$—destination address • \$s\$—sender address • \$p\$—page count • \$t\$—transmission time <p>Use the <i>string</i> argument in this command to insert personalized text string.</p>
Step 3	Router(config)# fax send left-header {\$a\$ \$d\$ \$p\$ \$s\$ \$t\$ <i>string</i> }	<p>Specifies the header information to be displayed on the left. The wildcards used in this command are used to insert the following information:</p> <ul style="list-style-type: none"> • \$a\$—date • \$d\$—destination address • \$s\$—sender address • \$p\$—page count • \$t\$—transmission time <p>Use the <i>string</i> variable in this command to insert personalized text string.</p>

Configuring the Fax Cover Page Information

The off-ramp gateway can create fax cover pages for those faxes that originate from e-mail messages.



Note

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 <i>string</i>	(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 the e-mail header information as part of the fax cover sheet text.

Also the destination address of an e-mail message can control the cover page generation on a per-recipient basis. Use the **fax send coverpage e-mail-controllable** command to configure the router to defer to the cover page setting in the e-mail header.

For example, if the address has the cover parameter set to no, the parameter overrides the setting for the **fax send coverage enable** command and the off-ramp gateway does not generate a fax cover page. If the address has the cover parameter set to yes, the off-ramp gateway defers the setting configured in the e-mail address and generates cover page. Table 4 contains examples of what the user would enter in the e-mail To: field.

Table 4 To: Field Entry Examples

To: Field Entries	Descriptions
FAX=+1-312-555-3260@fax.com	Fax sent to an E.164-compliant long distance telephone number in the United States. If the fax coverage enable command has been configured, store-and-forward fax will generate a fax cover page.
FAX=+1-312-555-3260/cover=no@fax.com	Fax sent to an E.164-compliant long distance telephone number in the United States. In this example, the fax coverage enable command is superseded by the cover=no statement. No cover page will be generated.
FAX=+1-312-555-3260/cover=yes@fax.com	Fax sent to an E.164-compliant long distance telephone number in the United States. In this example, the fax coverage enable command is superseded by the cover=yes statement. Store-and-forward fax will generate a fax cover page.
FAX=+1-312-555-3260/T33S=123456@fax.com	Fax sent to an E.164-compliant long distance telephone number in the United States; this example has an attached T.33 substring.
FAX=+49-515-555-5637@faxgateway.com	Fax sent to an E.164-compliant long distance telephone number in Germany.
FAX=+61-2-555-8765@fax.host.com	Fax sent to an E.164-compliant long distance telephone number in Australia.
FAX=+33-65-555-5555@fax.com	Fax sent to an E.164-compliant long distance telephone number in France.

To configure the router to defer to the cover page setting in the e-mail header, use the following commands in global configuration mode:

	Command	Purpose
Step 1	Router(config)# fax send coverage enable	Enables the off-ramp gateway to send a cover page with faxes that originate from e-mail messages.
Step 2	Router(config)# fax send coverage e-mail controllable	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 coverage enable command.

Verifying the Off-Ramp Gateway Configuration

Perform the following to verify the off-ramp gateway configuration:

- 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.

To check whether the fax cover page generates correctly, send an e-mail message to the off-ramp gateway. To check if the fax-mail is processed correctly, request a return receipt in the e-mail message and send a fax-mail using a mail client, such as Eudora to the off-ramp gateway. The destination e-mail address must have the appropriate `fax=user@receive` alias to be allowed.

Configuring the Gateway Security

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

- Configuring On-Ramp Gateway Security
- Configuring Off-Ramp Gateway Security
- Configuring the ACLs
- Using Attribute-Value Pairs
- Configuring the Gateway for TCL Application Files
- Verifying the Gateway Security Configuration

Configuring On-Ramp Gateway Security

On-ramp security controls who can send fax messages to the network and is facilitated by AAA security services using either RADIUS or TACACS+ as the local security protocol. On-ramp faxing is a client of the authentication server, whether RADIUS or TACACS+. User information is forwarded to the AAA interface, which is then forwarded as an authentication request to the security server.

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

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

	Command	Purpose
Step 1	<code>Router(config)# aaa new model</code>	Enables AAA security services.
Step 2	<code>Router(config)# mmoip aaa method fax authentication method-list-name</code>	Defines the name of the method list to be used for store-and-forward fax AAA authentication.
Step 3	<code>Router(config)# mmoip aaa method fax accounting method-list-name</code>	Defines the name of the method list to be used for store-and-forward fax AAA accounting.

	Command	Purpose
Step 4	<code>Router(config)# aaa authentication login {default list-name} method1 [method2...]</code>	Creates a local authentication method list and enables authentication.
Step 5	<code>Router(config)# aaa accounting {system network exec connection commands level} {default list-name} {stop-only} [method1 [method2...]]</code>	Creates an accounting method list and enables accounting. We recommend the following configuration: aaa accounting connection list-name stop-only .
Step 6	<code>Router(config)# mmoip aaa receive-id primary {ani dnis gateway redialer-id redialer-dnis}</code>	Specifies the primary location where AAA retrieves its identifying information for on-ramp faxing.
Step 7	<code>Router(config)# mmoip aaa receive-id secondary {ani dnis gateway redialer-id redialer-dnis}</code>	(Optional) Specifies the secondary location where AAA retrieves its identifying information for on-ramp faxing.
Step 8	<code>Router(config)# mmoip aaa receive-authentication enable</code>	Enables on-ramp AAA authentication services.
Step 9	<code>Router(config)# mmoip aaa receive-accounting enable</code>	Enables on-ramp AAA accounting services.
Step 10	<code>Router(config)# radius-server host {hostname ip-address} [auth-port port-number] [acct-port port-number]</code>	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	<code>Router(config)# radius-server key string</code>	Specifies the shared secret text string used between the router and the RADIUS server.
Step 12	<code>Router(config)# radius-server vsa send accounting</code>	Enables the network access server to recognize and use accounting Vendor-Specific Attributes (VSAs) as defined by RADIUS IETF attribute 26.
Step 13	<code>Router(config)# radius-server vsa send authentication</code>	Enables the network access server to recognize and use authentication VSAs as defined by RADIUS IETF attribute 26.

Configuring Off-Ramp Gateway Security

Off-ramp security controls who can send outgoing fax messages and is facilitated by AAA security services using either RADIUS or TACACS+. Authentication begins as soon as a fax e-mail message header is received from the e-mail server on the off-ramp gateway. The Cisco AS5300 does not dial the destination fax device until authentication for each fax-mail is successfully completed.

The on-ramp gateway inserts whatever value was configured for the **mmoip aaa receive-id primary** command in the X-account-ID field of the e-mail header. This X-account ID field contains the value that is used for authentication and accounting by the on-ramp gateway.

For example, if the **mmoip aaa receive-id primary** command is set to **gateway**, the on-ramp gateway name (for example, hostname.domain-name) is inserted in the X-account-ID field of the e-mail header of the fax-mail message.

If configured gateway value in the X-account-ID field is used, the **mmoip aaa send-id primary** command must be configured with the **account-id** keyword. This particular keyword enables store-and-forward fax to generate end-to-end authentication and accounting tracking records. If authentication is not configured on the on-ramp gateway, the X-account-ID field is left blank.

**Note**

It is recommended that Access Control Lists (ACLs) be configured to restrict which IP addresses can connect to the SMTP port (port 25). For information about configuring ACLs, refer to the *Cisco IOS Security Configuration Guide*.

**Note**

It is also recommended that the Cisco AS5300 be configured to act as an off-ramp gateway and only accept incoming SMTP connections from trusted mailers. Configure packet filters to permit only certain trusted IP addresses to send faxes to the store-and-forward fax off-ramp gateway.

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 ACLs

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

Creating ACLs is a relatively complicated task and beyond the scope of this document. The following example, though, provides a starting point.

The following example shows how to restrict access to the SMTP port 25 to a trusted e-mail server (IP address 10.0.0.1):

```
! Enter global configuration mode.
configure terminal
!
! Configure ACLs to restrict access to the SMTP port (port 25) to only "trusted"
! e-mail servers. Depending on the topology of your particular network, replace the
! any keyword with the destination IP addresses of the Ethernet and FastEthernet
! interfaces. Define all trusted e-mail servers using the tcp host ip-address
! portion of this command.
access-list 100 permit tcp host 10.0.0.1 any eq smtp
access-list 100 deny tcp any any eq smtp
access-list 100 permit ip any any
!
! Enter interface configuration mode for Ethernet interface 0.
interface ethernet 0
! Apply the access list to this interface.
access-group 100 in
!
! Enter interface configuration mode for FastEthernet interface 0.
interface fastethernet 0
! Apply the access list to this interface.
access-group 100 in
```

For complete information about configuring ACLs, refer to the relative chapters in the *Cisco IOS Security Configuration Guide*.

Using Attribute-Value Pairs

RADIUS attributes are used to define specific AAA elements in a user profile, which is stored on the RADIUS daemon. The Cisco implementation of RADIUS supports both IETF and vendor-proprietary attributes. IETF RADIUS attribute 26 allows vendors to support their own extended attributes not suitable for general use. Store-and-forward fax uses the Cisco RADIUS implementation of vendor-specific options using the format recommended in the specification. The Cisco vendor-ID company code is 9; the vendor-specific options are represented by subtype numbers from 3 through 21.

Table 5 lists the store-and-forward fax vendor-specific options supported using vendor-specific IETF RADIUS attribute 26.

Table 5 Vendor-Specific RADIUS Attributes for Store-and-Forward Fax

IETF RADIUS Attribute	Vendor-Specific Company Code	Subtype Number	Attribute	Description
26	9	3	Cisco-Fax-Account-Id-Origin	Indicates the account ID origin as defined by the system administrator for the mmoip aaa receive-id or the mmoip aaa send-id command.
26	9	4	Cisco-Fax-Msg-Id=	Indicates a unique fax message identification number assigned by store-and-forward fax.
26	9	5	Cisco-Fax-Pages	Indicates the number of pages sent or received during this fax session. This page count includes cover pages.
26	9	6	Cisco-Fax-Coverpage-Flag	Indicates whether a cover page was generated by the off-ramp gateway for this fax session. True indicates that a cover page was generated; false means that a cover page was not generated.
26	9	8	Cisco-Fax-Connect-Speed	Indicates the speed at which this fax-mail was initially sent or received. Possible values are 1200, 4800, 9600, and 14400.
26	9	9	Cisco-Fax-Recipient-Count	Indicates the number of recipients for this fax transmission. Until e-mail servers support session mode, the number should be 1.
26	9	10	Cisco-Fax-Process-Abort-Flag	Indicates whether the fax session was aborted or successful. True means that the session was aborted; false means that the session was successful.
26	9	11	Cisco-Fax-Dsn-Address	Indicates the address to which DSNs will be sent.
26	9	12	Cisco-Fax-Dsn-Flag	Indicates whether DSN has been enabled. True indicates that DSN has been enabled; false means that DSN has not been enabled.
26	9	13	Cisco-Fax-Mdn-Address	Indicates the address to which MDNs will be sent.
26	9	14	Cisco-Fax-Mdn-Flag	Indicates whether or not MDN has been enabled. True indicates that MDN has been enabled; false means that MDN has not been enabled.

Table 5 Vendor-Specific RADIUS Attributes for Store-and-Forward Fax (continued)

IETF RADIUS Attribute	Vendor-Specific Company Code	Subtype Number	Attribute	Description
26	9	15	Cisco-Fax-Auth-Status	Indicates whether authentication for this fax session was successful. Possible values for this field are success, failed, bypassed, or unknown.
26	9	16	Cisco-Email-Server-Address	Indicates the IP address of the e-mail server handling the on-ramp fax-mail message.
26	9	17	Cisco-Email-Server-Ack-Flag	Indicates that the on-ramp gateway has received a positive acknowledgment from the e-mail server accepting the fax-mail message.
26	9	18	Cisco-Gateway-Id	Indicates the name of the gateway that processed the fax session. The name appears in the following format: hostname.domain-name.
26	9	19	Cisco-Call-Type	Describes the type of fax activity: fax receive or fax send.
26	9	20	Cisco-Port-Used	Indicates the slot/port number of the Cisco AS5300 used to either send or receive this fax-mail.
26	9	21	Cisco-Abort-Cause	If the fax session aborts, indicates the system component that signaled the abort. Examples of system components that could trigger an abort are Fax Application Process (FAP), TIFF (the TIFF reader or the TIFF writer), fax-mail client, fax-mail server, ESMTP client, or ESMTP server.

For more information about using vendor-specific RADIUS attributes, refer to “RADIUS Attributes” appendix in the *Cisco IOS Security Configuration Guide*. This appendix file contains a complete list of supported vendor-specific, vendor-proprietary, and IETF-compliant RADIUS attributes, the Cisco IOS releases in which they were implemented, and their definitions.

Configuring the Gateway for TCL Application Files

To configure gateway security for the TCL application files being used for fax calls on a VFC, use the following commands in global configuration mode:

	Command	Purpose
Step 1	<code>Router(config)# call application voice application-name accounting enable</code>	Enables AAA accounting services for the named application.
Step 2	<code>Router(config)# call application voice application-name accounting-list method-list-name</code>	Defines the name of the method list to be used for AAA accounting with fax applications on a VFC.
Step 3	<code>Router(config)# call application voice application-name authentication enable</code>	Enables AAA authentication services for the named application.
Step 4	<code>Router(config)# call application voice application-name authen-list method-list-name</code>	Specifies the name of an authentication method list for the named application.
Step 5	<code>Router(config)# call application voice application-name authen-method id</code>	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

Verify the gateway security configuration by:

- Using **debug mmoip aaa** to verify that the on-ramp security for store-and-forward fax is configured correctly.
- Checking the console log file, depending upon the Radius version used, to verify connection to the RADIUS server.
- Using **debug aaa** to verify AAA performance.

Configuring MDN

One basic e-mail operation that store-and-forward fax supports is MDN (return receipt). Described in RFC 2298, MDN indicates that the e-mail message has been opened. A sender requests that an MDN be returned when the receiver opens an e-mail message.

The MDN is initiated by the sending e-mail client, and the return receipt is generated by the receiving e-mail client. Most PC-based e-mail software applications, such as Eudora, Netscape Messenger, and Microsoft Outlook,) generate MDNs.

The MDN is sent to an address chosen by the sender and the following header is included in the e-mail header of the message:

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

This header is followed by the address of the sender.

RFC 2298 requires that the receiver can prevent the automatic generation of an MDN. Because of the requirement, it is difficult to determine whether or not the user has actually received the e-mail message. For example, the recipient can always choose not to respond to MDN requests, or the recipient software cannot understand or accept MDN requests.

To configure MDN for store-and-forward fax, configure the MDN elements on both the on-ramp and off-ramp gateways.

The required tasks are:

- Configuring the On-Ramp Gateway Elements for MDN
- Configuring the Off-Ramp Gateway Element for MDN
- Verifying MDN Configuration

Configuring the On-Ramp Gateway Elements for MDN

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 <i>string</i>	Specifies the user name address where MDNs are sent. 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 <i>string</i>	Specifies the host name address where MDNs are sent. If this field is left blank, the on-ramp gateway inserts the postmaster address in this field as a default.
Step 3	Router(config)# dial-peer voice <i>number</i> mmoip	Defines the MMoIP dial peer tag number and enters dial-peer configuration mode.
Step 4	Router(config-dial-peer)# mdn	Requests that an MDN be sent to the destination(s) defined by the mta send return-receipt-to command.

Configuring the Off-Ramp Gateway Element for MDN

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 acting as the off-ramp gateway will respond to a request for an MDN.

Verifying MDN Configuration

Perform the following to verify the MDN configuration:

- Use **show dial-peer voice** and look at the disposition notification field to verify if DSN is enabled or disabled.
- Use **show running-config** to verify that **mta send return-receipt-to username**, **mta send return-receipt-to hostname**, and **mta receive generate-mdn** have been configured.
- 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 DSN

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. The on-ramp DSN request is included as part of the fax-mail message sent by the on-ramp gateway when the matching MMoIP dial peer has been configured. The on-ramp DSN response is generated by the SMTP server when the fax-mail message is accepted. The DSN is sent back to the user defined in the **mta send mail-from** command.

The off-ramp DSN is requested by the e-mail client. The DSN response is generated by the off-ramp gateway when it receives a request as part of the fax-mail message. DSNs can only be generated if the mail client on the SMTP server is capable of responding to a DSN request. Because the SMTP server generates the DSNs, you need to configure both the mail from: and rcpt to: commands for the DSN feature to be operational, for example:

```
mail from: <user@mail-server.company.com>
rcpt to: <fax=555-1212@company.com> NOTIFY=SUCCESS,FAILURE,DELAY
```

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

- Delay—message delivery was delayed.
- Success—message was successfully delivered to the recipient mailbox.
- Failure—SMTP server was unable to deliver the message to the recipient.



Note

Because the delivery states are not mutually exclusive, configure store-and-forward fax to generate the messages for all or any combination of these events.

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. This information appears in the RFC 822 From: field and the RFC 821 MAIL FROM field of the e-mail fax message. This information is also used for generating DSNs. When the mta send mail-from hostname command is configured, the configured host name is used with the mta send mail-from username command to form a complete e-mail address, like faxuser@onramp-gateway.com.
Step 2	Router(config)# mta send mail-from {username string username \$\$}	Specifies the originator (username portion) of the e-mail fax message. This information appears in the RFC 822 From: field and the RFC 821 MAIL FROM field of the e-mail fax message. If the wild card \$\$ is used, a transmission report is sent to the originating fax machine. This information is also used for generating DSNs. When you configure the mta send mail-from username command, the username configured is used with the mta send mail-from hostname command to form a complete e-mail address, like faxuser@onramp-gateway.com.

	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)# dsn {delay success failure}	Requests that a DSN be sent to the destination(s) defined by the mta send mail-from command.

Verifying DSN Configuration

Perform the following tasks to verify the DSN configuration:

- Use **show dial-peer voice** and look at the delivery status notification field.
- Use **show running-config** to verify that **mta send mail-from username** and **mta send mail-from hostname** have been configured. If these commands are not configured, the DSN is delivered to the postmaster defined by the **mta send postmaster** command.
- Use **show running-config** to verify that **mta send return-receipt-to username**, **mta send return-receipt-to hostname**, and **mta receive generate-mdn** have been configured.
- 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.

Configuration Examples

The following is an annotated sample configuration for store-and-forward fax and fax relay using VFCs on a Cisco AS5300 access server:

```
!version 12.1
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 example is for fallback from the T.38 gateway to the T.37 gateway:

```
voice hunt user-busy
```

The following example is for global service:

```
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
  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

```

The following example is for the inbound peer of the T.37 on-ramp operation:

```

dial-peer voice 2 pots
  application app_onramp9
  incoming called-number 5.....
  direct-inward-dial

```

The following example is for the outbound peer of the T.37 on-ramp operation:

```

dial-peer voice 3 mmoip

```

The following example is to configure the application name and must be input exactly as shown. Note that the MDN and DSN configuration can be set in this peer:

```

  application fax_on_vfc_onramp_app out-bound
  destination-pattern 57108..
  session target mailto:$d$@mail-server.cisco.com

```

The following example is for the inbound peer of the T.37 off-ramp operation:

```

dial-peer voice 21 mmoip
  application lib_off_app5
  incoming called-number 5.....
  information-type fax

```

The following example is for the outbound peer of the T.37 off-ramp operation. Note that 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

```

The following examples are for two different gateways processing the same call for T.38 gateway.

Example 1—Inbound peer for on-ramp gateway:

```

dial-peer voice 50 pots
  incoming called-number 1800555...

```

Example 2—Outbound peer for on-ramp gateway:

```

dial-peer voice 51 voip
  destination-pattern 57108..
  session target ipv4:12.22.95.20

```

Example 3—Inbound peer for off-ramp gateway:

```

dial-peer voice 61 voip
  incoming called-number 57108..

```

Example 4—Outbound peer for off-ramp gateway:

```

dial-peer voice 60 pots
  destination-pattern 57108..
  port 0:D

```

```
prefix 57108
```

The following three examples are for on-ramp T.38 fax rollover to T.37 fax rollover which occurs when the destination fax line is busy. Note that the following configuration command must be set first for the T.38 rollover to T.37:

```
voice hunt user-busy
```

Example 1—Inbound peer of the T.38/T.37 on-ramp rollover operation, which includes the TCL application for rollover operation:

```
dial-peer voice 70 pots
  application app_lib_rollover15
  incoming called-number 5.....
```

Example 2—Outbound peer of the T.38 on-ramp gateway, which requires a lower preference number than the next matching peer:

```
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
```

Example 3—Outbound peer of the T.37 onramp operation. Note that the application name below must be input exactly as shown:

```
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
```