



T.37/T.38 Fax Gateway

This document provides the additional information you need to configure T.38 fax relay and T.37 fax store and forward on a voice feature card installed in a Cisco AS5300 access server. The Store and Forward Fax feature, previously documented in other Cisco publications, enables Cisco AS5300 access servers to send and receive faxes across packet-based networks.

This document includes the following sections:

- Feature Overview, page 1
- Supported Platforms, page 6
- Supported Standards, MIBs, and RFCs, page 6
- Prerequisites, page 6
- Configuration Tasks, page 14
- Configuration Examples, page 36
- Command Reference, page 40

Feature Overview

Previously, store and forward fax was supported only on MICA and Microcom modem cards. Voice applications run on the C542 Digital Signal Processing Module (DSPM) and C549 DSPMs that populate a Cisco AS5300 voice feature card (VFC). Equipping a Cisco AS5300 with both store and forward fax and voice is inefficient because of the need to use different technologies for each type of call.

The objective of this software release is to allow a single DSPM technology to support voice, fax relay, and fax store and forward on both the C542 and C549 DSPM. A further objective is to offer voice, fax relay, and fax store and forward on the same voice port, and to provide the ability to dynamically switch from one application to another in the same call (IVR, voice, fax relay, and fax store and forward).

A related objective is to migrate from the current Cisco proprietary implementation of real-time fax relay to the ITU-T T.38 standard. The proposed implementation on the C54x DSPM is for the ingress DSP to perform real-time fax relay to the router processor.

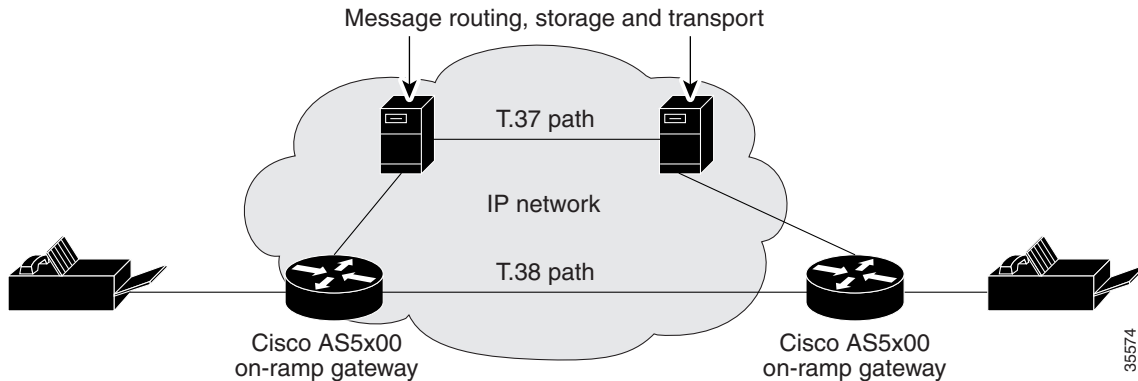


Note

In order to support the maximum of 120 fax store and forward sessions, the Cisco AS5300 must be equipped with 128 MB of RAM.

The diagram below highlights the real-time versus the store and forward processing path for a fax transaction over an IP network.

Figure 1 Real-time versus Store and Forward Fax Processing



The T.38 path represents the real-time fax relay connection between two VOIP gateways. The current fax relay implementation in VOIP uses a proprietary protocol over an H.323 connection. This software release will allow the standard T.38 fax implementation to take preference over the Cisco proprietary protocol where possible. This means that as a fax session is being set up and negotiated over the H.323 connection, the sending gateway will attempt to communicate via the T.38 protocol first and then attempt the Cisco proprietary protocol if the first method is rejected.

The T.37 path represents the processing path for a fax that is delivered via the ESMTP store and forward method. The onramp fax gateway is responsible for accepting fax data from the PSTN fax machine using this software release and the VFC acting as a fax modem. The gateway router processor converts the fax into a TIFF attachment in a MIME e-mail message and transmits it to a store and forward SMTP server. Delivery of the faxmail message to the offramp gateway is the responsibility of the store and forward server(s). Once the offramp gateway receives a faxmail message, it will process the message and initiate a fax session with the destination fax machine using this software release and the VFC acting as a fax modem.

Using Interactive Voice Response for Call Processing

The Interactive Voice Response (IVR) feature is used for call control when VFCs are used for store and forward fax. IVR consists of simple voice prompting and digit collection to gather caller information for authenticating the user and identifying the destination. IVR applications can be assigned to specific ports or invoked based on DNIS. An IP PSTN gateway can have several different IVR applications to accommodate many different gateway services, and you can customize the IVR applications to present different interfaces to the different callers.

IVR uses Tool Control Language (TCL) scripts to gather information and to process accounting and billing. For example, a TCL IVR script plays when a caller receives a voice-prompt instruction to enter a specific type of information, such as a PIN. After playing the voice prompt, the IVR application collects the predetermined number of touch tones (digit collection) and forwards the collected digits to a server for storage and retrieval. Call records can be kept and a variety of accounting functions performed.

**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.

Cisco provides the following IVR scripts:

- `fax_hop_on_1`—Collects digits from the redialer, such as account number and destination number. When a call is placed to an H.323 network, the set of fields configured in the call information structure are *entered*, *destination*, and *account*.
- `clid_authen`—Authenticates the call with ANI and DNIS numbers, collects the destination data, and makes the call.
- `clid_authen_npw`—Same as `clid_authen`, but uses a null password when authenticating, rather than DNIS numbers.
- `clid_authen_collect`—Authenticates the call with ANI and DNIS numbers and collects the destination data, but if authentication fails, it collects the account and password.
- `clid_authen_col_npw`—Same as `clid_authen_collect`, but uses a null password and does not use or collect DNIS numbers.
- `clid_col_npw_3`—Same as `clid_authen_col_npw` except with that script, if authentication with the digits collected (account and PIN) fails, the `clid_authen_col_npw` script just plays a failure message (`auth_failed.au`) and then hangs up. The `clid_col_npw_3` script allows two failures, then plays the retry audio file (`auth_retry.au`) and collects the account and PIN again.

The caller can interrupt the message by entering digits for the account number, which triggers the prompt to tell the caller to enter the PIN. If authentication fails the third time, the script plays the audio file `auth_fail_final.au`, and hangs up.

Table 1 lists the prompt audio files associated with the `clid_col_npw_3` script.

Table 1 *clid_col_npw_3 Script Prompt Audio Files*

Audio File Name	Action
<code>flash:enter_account.au</code>	Asks the caller to enter an account number the first time.
<code>flash:auth_fail_retry.au</code>	Played after two failures, asks the caller to reenter the account number.
<code>flash:enter_pin.au</code>	Asks the caller to enter a PIN.
<code>flash:enter_destination.au</code>	Asks the caller to enter a destination phone number.
<code>flash:auth_fail_final.au</code>	Informs the caller that the authorization failed three times.
<code>auth_fail_retry.au</code>	Informs the caller that authorization failed. Prompts the caller to reenter the account number followed by the pound sign (#).
<code>auth_fail_final.au</code>	Informs the caller, “I’m sorry, your account number cannot be verified. Please hang up and try again.”

- `clid_col_npw_npw`—Tries to authenticate by using ANI, null as the user ID, user, and user password pair. If that fails, it collects an account number and authenticates with account and null. It allows three tries for the caller to enter the account number before ending the call with the authentication failed audio file. If authentication succeeds, it plays a prompt to enter the destination number.

- `clid_col_dnis_3.tcl`—Authenticates the caller ID three times. First it authenticates the caller ID with DNIS. If that is not successful, it attempts to authenticate with the caller PIN up to three times.
- `clid_col_npw_3.tcl`—Authenticates with null. If authentication is not successful, it attempts to authenticate by using the caller PIN up to 3 times.
- `clid_4digits_npw_3.tcl`—Authenticates with null. If the authentication is not successful, it attempts to authenticate with the caller PIN up to 3 times using the 14-digit account number and password entered together.
- `clid_4digits_npw_3_cli.tcl`— Authenticates the account number and PIN respectively by using ANI and null. The length of digits allowed for the account number and password are configurable through the CLI. If the authentication fails, it allows the caller to retry. The retry number is also configured through the CLI.
- `clid_authen_col_npw_cli.tcl`—Authenticates the account number and PIN respectively using ANI and null. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.
- `clid_authen_collect_cli.tcl`—Authenticates the account number and PIN by using ANI and DNIS. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.
- `clid_col_npw_3_cli.tcl`—Authenticates by using ANI and null for account and PIN respectively. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI.
- `clid_col_npw_npw_cli.tcl`—Authenticates by using ANI and null for account and PIN respectively. If authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected together.
- `clid_t37_fax_onramp.tcl`—Authenticates the account and PIN using the following: prompt-user, ANI, DNIS, gateway ID, redialer ID, and redialer DNIS.
- `clid_t37_fax_offramp.tcl`—Authenticates the account and PIN using the following: envelope-from, envelope-to, gateway ID, and x-account ID.
- `clid_t37_fax_rollover.tcl`—Used for on-ramp T.38 fax rollover to T.37 fax when the destination fax line is busy.
- `app_switch*.tcl`—Authenticates and switches dynamically from fax relay to fax store and forward.
- `fax_on_vfc_onramp_app`—Authenticates and completes the on-ramp T.37 call on a VFC.
- `lib_off_app`—Authenticates and completes the off-ramp call on a VFC.

**Note**

To see the contents of the TCL IVR script, use the **show call application voice** command.

The following IVR script is not built into Cisco IOS software but is required for T.37 on-ramp applications using a VFC. You must download this script manually:

- `t37_onramp11.0.0.11`

Benefits

Cost Savings and Port Density

Rather than bearing the cost of maintaining two architectures, one for voice and one for fax, service providers can use a single port for both voice, fax relay, and store and forward fax. For smaller POPs, the ability to use a single port for both technologies is even more significant due to greater efficiencies of handling mixed traffic over a single pool of ports versus splitting traffic across two pools (whose combined total number of ports would exceed the number in the mixed traffic case).

Single Number for Voice and Fax Access

Service providers can advertise new service offerings such as a single number for subscriber voice and fax access. Service provider 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 Fax Store and Forward

Service providers can offer applications that require toggling from voice to fax – for example, providing an IVR front-end to a fax application. Also applications such as never-busy fax service can be addressed once the gateway has the ability to dynamically switch from fax relay to fax store and forward.

Restrictions



Note

In order to support the maximum of 120 fax store and forward sessions, the Cisco AS5300 must be equipped with 128 MB of RAM.

Related Features and Technologies

- Cisco Voice over IP (VoIP)
- 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*
- Cisco IOS Release 12.1 *Cisco IOS Multiservice Applications Configuration Guide*
- Cisco IOS Release 12.1 *Cisco IOS Multiservice Applications Command Reference*
- Cisco IOS Release 12.1 *Cisco IOS Security Configuration Guide*
- Cisco IOS Release 12.1 *Cisco IOS Security Command Reference*
- New feature documentation for Cisco IOS Release 12.0(3)T *Voice over IP for the Cisco AS5300*
- Cisco AS5300 Universal Access Server Software Configuration Guide
- Cisco AS5300 Universal Access Server Module Installation Guide

Supported Platforms

- Cisco AS5300 access server

Supported Standards, MIBs, and RFCs

Standards

- ITU-T T.37
- ITU-T T.38

MIBs

See the *Store and Forward Fax with ESMTP* document.

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

See the *Store and Forward Fax with ESMTP* document.

Prerequisites

Before configuring T.38 fax relay and T.37 store and forward fax on a Cisco AS5300 VFC, you must complete the following tasks:

- Download VFCWare to the VFC
- Copy Flash Files to the VFC
- Unbundle VCWare
- Configure the VFC

These tasks are described in the sections below.

VFCs for the Cisco AS5300 come with a single bundled image of VCWare stored in VFC Flash memory. Table 2 shows the extension types defined for these embedded firmware files.

Table 2 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

Firmware	Filenames	Description
	bas-vfc-*	Base voice
	cdc-*-*	Voice codec files
	fax-vfc-*	Fax relay files

DSPWare is stored as a compressed file within VCWare; you must unbundle VCWare to install DSPWare into Flash memory. During the unbundling process, two default lists (the default file list and the capability list) 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. The capability list defines the set of codecs that can be negotiated for a voice call.

VFC management enables you to add versions of VCWare to Flash memory (download and unbundle files), erase files contained in Flash memory, add files to the default file list and capability list, and delete 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

Downloading VCWare to the VFC

To download software to your VFC, perform the following tasks:

- Determine that the version of VFC ROM Monitor software is compatible with your 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.
- Determine whether the VFC is in VCWare mode or ROM Monitor mode. The mode, whether VCWare or ROM Monitor, determines how you download software to the VFC.
- Download the software using the appropriate procedure.

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

For each VFC identified and located, perform the tasks described in the following sections to upgrade system software on that VFC.

Identifying the VFC Mode



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

Command	Purpose
Router# show vfc slot board	Determines whether your 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 Software (VCWare Mode)

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

Command	Purpose
Step 1 Router# erase vfc slot	Erases the Flash memory.
Step 2 Router# show vfc slot directory	Verifies that the VFC Flash memory is indeed empty.
Step 3 Router# copy tftp: vfc:	Downloads the VCWare from a TFTPBoot server into VFC Flash memory.
or	
Router# copy flash: vfc:	<p> Note The colons in this command are required.</p> <p>Downloads the VCWare from the VFC motherboard into VFC Flash memory.</p> <p> Note The colons in this command are required.</p>
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	Verifies that VCWare is in the VFC Flash.
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	Verifies that the DSPWare has been unbundled.
Step 9 Router# show vfc slot default-list	Verifies that the default file list has been populated.
Step 10 Router# show vfc slot cap-list	Verifies that the capability list has been populated.

After you have completed the preceding tasks, 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-.”

**Note**

In any **copy** command in which “vfc” is the target, it is imperative that you include a colon after the “vfc.” Thus, in Step 3 above and in Step 2 below, **copy tftp vfc:** must be the syntax.

Downloading Software (ROM Monitor Mode)

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

	Command	Purpose
Step 1	Router# clear vfc slot purge	Erases the VFC Flash memory.
Step 2	Router# copy tftp: vfc:	Downloads the VCWare from a TFTP server into VFC Flash memory.
	or	
	Router# copy flash: vfc:	Downloads the VCWare from the VFC motherboard into VFC Flash memory.
		 Note The colons in this command are required.
		or
		 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	Verifies that VCWare is in the VFC Flash.
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.

After you have completed the preceding tasks, reboot the Cisco AS5300 for these changes to take effect.

**Note**

The image name must start with “vcw-.”

Copying Flash Files to the VFC

As mentioned, each VFC comes with a single bundled image of VCWare stored in Flash memory. VoIP for the Cisco AS5300 offers two different ways to copy new versions of VCWare to the VFC Flash memory: either by downloading the image from the AS5300 motherboard or by downloading the VCWare from a TFTP server.

Downloading VCWare to the VFC from the AS5300 Motherboard

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

	Command	Purpose
Step 1	Router# <code>copy flash vfc:</code>	Downloads (copies) the Flash file from the AS5300 motherboard to the Flash memory on the VFC. (NOTE: Be sure to include the colon in this command.)
Step 2	Router# <code>clear vfc slot</code>	Reboots the VFC.

Downloading VCWare to the VFC from a TFTP Server

To download the latest version of VCWare from a TFTP server, make sure that the file is stored on the TFTP server. If you have a copy of the current version of VCWare on disk, you must store that image on a TFTP server before you can download the file to 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: Be sure to include the colon in this command.)
Step 2	Router# <code>clear vfc slot</code>	Reboots the VFC.

Unbundling VCWare

VCWare needs to be unbundled for DSPWare to be loaded in Flash memory and the two necessary default lists (default file list and capability list) created and populated with the appropriate default files for that version of DSPWare. Table 3 shows the files associated with each firmware file.

Table 3 VFC Firmware Filenames

Firmware	Filenames
VCWare	vcw-vfc-mz.c542.t1.6
DSPWare Initialization and Static Files	btl-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# unbundle vfc slot	Unbundles the current image of VCWare.

Adding Files to the Default File List

When you unbundle VCWare, 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 upon bootup. 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 you need to, you can add a file (from those stored in VFC Flash memory) to the default file list or replace an existing file from the default file list. When you add a specific file to the default file list, it replaces the existing default for that extension type.

To select a file to be added 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
```

VFC management lets you add codec files to the capability list to meet the needs of your specific telephony network.



Note

The capability list does not indicate codec preference; it simply reports the codecs that are available. 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, you might need to delete a file from the default file list or the capability list or you might need to revert to a previous version of VCWare stored in Flash memory. To delete a file, you must identify and delete the file from VFC Flash memory. Deleting a file from Flash memory removes the file from the default file list and capability list (if the deleted file is included on those 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 you upgrade to a later version of VCWare, the new files are stored in VFC Flash, along with those already stored in VFC Flash memory—the new files do not overwrite existing files. Consequently, you will eventually need to erase the contents of VFC Flash memory to free VFC Flash memory space.

Erasing VFC Flash memory removes the entire contents stored in Flash memory, including the default file list and the capability list.

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.

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

IVR Prerequisites

Before you configure your Cisco gateway to support IVR, you need to perform the following prerequisite tasks:

- Configure VoIP to support H.323-compliant gateways—meaning that in addition to the basic configuration tasks, such as configuring dial peers and voice ports, you must configure specific devices in your network to act as gateways.
- Configure a TFTP sever to perform storage and retrieval of the audio files, which are required by the Debit Card gateway or other features requiring TCL IVR scripts and audio files.
- Download the appropriate classic or TCL IVR script from the CCO Software Support Center. Use the **copy** command to copy your audio file (.au file) to your Flash memory, and the **audio-prompt load** command to read it into RAM. For more information about loading files into Flash memory, see the “Copying Flash Files to the VFC” section earlier in this chapter.
- Make sure that your audio files are in the proper format. The IVR prompts require audio file (.au) format of 8-bit, u-law, and 8-Khz encoding. To encode your own audio files, we recommend that you use one of these two audio tools (or a similar tool of comparable quality):
 - Cool Edit, manufactured by Syntrillium Software Corporation
 - AudioTool, manufactured by Sun Microsystems
- Make sure that your access platform has a minimum of 16 MB Flash and 64 MB of DRAM memory.
- Install and configure the appropriate RADIUS security server in your network. The version of RADIUS that you are using must be able to support IETF-Supported VSAs, which are implemented by using IETF RADIUS Attribute 26.

Configuration Tasks

Configuring Store and Forward Fax involves the following configuration tasks:

- Configuring the on-ramp gateway
- Configuring the off-ramp gateway
- Configuring on-ramp gateway security
- Configuring off-ramp gateway security
- Configuring MDN
- Configuring DSN

These configuration tasks are described in detail in the *Store and Forward Fax with ESMTX* document. If you are implementing store and forward fax on modem cards, this document contains all the instructions you need.

If you are implementing store and forward fax on a VFC, one additional command is needed in configuring the on-ramp and off-ramp dial peers. These configuration instructions and procedures are repeated below. In addition, you must perform the following additional configuration tasks:

- Configure IVR
- Specify the interface type for fax calls
- Specify the TCL files containing the onramp and offramp applications
- Configure gateway security using the call application voice command
- Associate the TCL applications with the appropriate dial peers

**Note**

You can set up the off-ramp dial peers to steer a specific outgoing fax call to a specific T1 controller port. See the “Configuring Off-Ramp POTS Dial Peers” section on page 26 of this document.

Configuring the On-Ramp Gateway

When acting as the on-ramp gateway, the Cisco AS5300 receives faxes from end users and converts them into TIFF files, creates standard MIME e-mail messages, attaches the TIFF files to them, and then forwards these fax-mail messages to the messaging infrastructure of a designated SMTP server, where fax-mail messages are stored. The on-ramp gateway accomplishes these activities by using the sending MTA and dial peers. 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. These delivery parameters include defining a return e-mail path or designating a destination mail server. The on-ramp POTS dial peers define the call as being a fax transmission and the DNIS of the incoming fax call. The on-ramp MMoIP dial peer defines the destination fax telephone number and the session target, which in this case is the SMTP server.

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

- Configuring the Called Subscriber Number
- Configuring the Sending MTA
- Configuring On-Ramp POTS Dial Peers
- Configuring On-Ramp MMoIP Dial Peers
- Configuring On-Ramp Modem Pooling
- Enabling the Nagle Congestion Control Algorithm

Configuring the Called Subscriber Number

The first step in configuring the on-ramp gateway is to configure called subscriber number—the number displayed in the LCD of the fax device when you are sending a fax 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 { <i>ad\$</i> <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

The next step in configuring inbound faxing is to define the characteristics associated with the sending MTA. You use MTAs to define the elements of the e-mail message to which the fax TIFF file is attached; these elements include the following:

- Subject
- Destination
- Return path
- Postmaster
- Any additional identifying e-mail header information
- Address to which any disposition notices are sent

Of these configuration steps, you must define 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 messages. The remaining configuration steps are optional.



Note

You use the **mta send mail-from username** and **mta send mail-from hostname** commands to configure the From: user name in the e-mail message. The To: address of the fax-mail is derived 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 <i>hostname string</i>	<p>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.</p> <p>When you configure the mta send mail-from hostname command, the host name configured is used with the mta send mail-from username command to form a complete e-mail address, like <code>faxuser@onramp-gateway.com</code>.</p>
Step 2 Router (config)# mta send mail-from { <i>username string</i> <i>username \$\$</i> }	<p>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.</p> <p>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 <code>faxuser@onramp-gateway.com</code>.</p>
Step 3 Router (config)# mta send server { <i>host-name</i> <i>IP-address</i> }	<p>Specifies the destination server.</p> <p>DNS MX records are not used to determine the IP address of the host specified with the mta send server command.</p>
Step 4 Router (config)# mta send subject <i>string</i>	<p>Defines the text that appears in the Subject field of the e-mail fax message.</p>
Step 5 Router (config)# mta send postmaster <i>e-mail-address</i>	<p>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 your 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.</p>
Step 6 Router (config)# mta send origin-prefix <i>string</i>	<p>(Optional) Defines additional identifying information to be prepended to the e-mail header.</p>
Step 7 Router (config)# mta send return-receipt-to { <i>hostname string</i> <i>username string</i> }	<p>(Optional) Specifies the address where MDNs are sent, if you request MDN.</p>

Configuring On-Ramp POTS Dial Peers

On-ramp POTS dial peers define the characteristics of the telephony (PSTN) connection between the sending fax device and the on-ramp gateway. In general, the on-ramp gateway uses the line characteristics defined by POTS dial peers to determine call type and call destination. The on-ramp gateway determines call type and call destination through call discrimination. It matches various POTS peer configuration parameters until it comes up with an appropriate match.

On-Ramp Gateway POTS Dial Peer/Call Discrimination Process

An understanding of how the on-ramp gateway uses POTS dial peers in the course of call discrimination is helpful before you configure on-ramp POTS dial peers. First, though, some functional definitions should be created. As mentioned, store and forward fax uses either DID or a redialer to process a fax call. In both of these cases, a different telephone number is used. For the purposes of the following discussion, the term *destinationDN* refers to the telephone number of the fax machine where the user wants a fax to be sent and *accessDN* refers to the telephone number dialed by a redialer to access an on-ramp gateway.

The process of call discrimination begins when the on-ramp router receives a call. It immediately identifies whether the call is being delivered via a PRI interface or a T1-CAS interface. If the on-ramp gateway determines that the call is coming in over a T1-CAS interface, it checks the service type field of the CAS group configuration. If the service type of the CAS group is fax, it flags the call as a store and forward fax call and forwards it to the MMoIP dial peer to be processed as a fax call. If it determines that the call is coming in over a PRI interface, then the on-ramp gateway begins to look at several POTS dial peer data fields to determine what kind of call it has received.

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 where the data matches. If the on-ramp router does not find a match, it assumes that this is a data call and processes the call 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, it concludes that the telephone number it has received is the *destinationDN* 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 *accessDN*. In this case, the on-ramp router provides a secondary dial tone and collects another telephone number from the redialer at the other end of the connection that it will use as the *destinationDN*. After it has received this number from the redialer, the on-ramp gateway forwards the call to be matched to the appropriate on-ramp MMoIP dial peer.

Redialers Versus DID for POTS Peers

By default, DID is disabled, which means that the on-ramp gateway assumes that the fax call it receives is being placed using a redialer. In this situation, when a call arrives on the on-ramp gateway, it presents a dial tone and collects digits until it can identify the destination, as described. After the destination has been identified, it forwards the call through to the next call leg (in this case, the MMoIP dial peer) to the destination.

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.

To configure on-ramp gateway POTS dial peers, 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-)# application name [out-bound]	Associates a specific IVR application with this dial peer. (The out-bound keyword is not used with POTS dial peers.)
Step 3 Router(config-dial-)# 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-)# 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-)# 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-)# max-conn <i>number</i>	(Optional) Defines the maximum number of on-ramp connections used simultaneously on this Cisco AS5300 to send fax-mail.

Configuring On-Ramp MMoIP Dial Peers

MMoIP dial peers describe the line characteristics generally associated with a packet network connection; in the case of store and forward fax, this is the IP network connection between the on-ramp gateway and the SMTP server.

On-ramp MMoIP dial peers are used to define the destination fax telephone number, to specify a destination e-mail address (which in this case identifies the SMTP server), to define the image encoding and resolution specifics for the associated fax-mail TIFF files, and to request either DSNs, MDNs, or both. If you enabled DID and specified an incoming called number for the on-ramp POTS dial peer, the destination pattern of the on-ramp MMoIP dial peer should be the same as the configured incoming called number. If you did not enable DID, then you need to configure and enable a redialer to use store and forward fax. If you use a redialer, you need to configure the destination pattern to match the forwarded dialed digits from the redialer.

On-Ramp Gateway MMoIP Dial Peer/Call Discrimination Process

An understanding of how the on-ramp gateway uses MMoIP dial peers is helpful before configuring on-ramp MMoIP dial peers. As with on-ramp POTS dial peers, for the purposes of the following discussion, the term *destinationDN* refers to the telephone number of the fax machine where the user wants a fax to be sent, and *accessDN* refers to the telephone number dialed by a redialer to access an on-ramp gateway.

The function of the on-ramp call discrimination process using MMoIP dial peers is to determine the destination of the fax-mail, which in this case means 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 to the number received and selects the first MMoIP dial peer where the data matches. The on-ramp gateway then looks at the session target field for the selected MMoIP dial peer to identify the destination of the fax-mail message—this could be a specific off-ramp gateway for a store and forward fax or, if the fax is being delivered as an e-mail message, an e-mail address for a specific mail server.

Image Encoding and Image Resolution

Depending on your specific needs, you might want to increase or decrease the resolution of the received fax image. As a default, image resolution in store and forward fax is set to passthrough, which means that the image is forwarded exactly as it is received. If you want to specify a different resolution for the fax TIFF image, whether greater or lesser, use the **image resolution** dial-peer configuration command as an attribute of the on-ramp MMoIP dial peer.

Depending on the capacity of the fax machines in your network, you might want to use a different image encoding (compression) scheme for the fax TIFF image store and forward fax creates. As a default, image encoding in store and forward fax is set to passthrough, which means that the image is forwarded exactly as it is received. If you want to specify a specific encoding (compression) scheme for the fax TIFF image, use the **image encoding** dial-peer configuration command.

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

- Delay—Indicates that, for some reason, the message was delayed in being delivered to the recipient.
- Success—Indicates that the message was successfully delivered to the recipient mailbox.
- Failure—Indicates that, for some reason, the SMTP server was unable to deliver the message to the recipient.

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

You enable DSN requests as part of the on-ramp MMoIP dial peer configuration. For complete instructions on how to configure DSNs using store and forward fax, refer to the “Configuring Delivery Status Notification” section later in this chapter.

MDN

One basic e-mail operation that store and forward fax supports is MDN. Described in RFC 2298, MDN is where a message is returned to the originator of an e-mail message indicating that the e-mail message has been opened. To configure MDN for store and forward fax, you need to configure elements on both the on-ramp and off-ramp gateways. You enable MDN requests as part of the on-ramp MMoIP dial peer configuration. For complete instructions on how to configure MDNs using store and forward fax, see the “Configuring Message Delivery Notification” section later in this chapter.

To configure on-ramp gateway MMoIP dial peers, 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-)# application name [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-)# 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-)# session target {mailto:{ <i>name</i> <i>\$d\$</i> }@ <i>domain-name</i> ipv4: <i>destination-address</i> dns:{ <i>\$s\$</i> . <i>\$d\$</i> . <i>\$u\$</i> . <i>\$e\$</i> .} <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-)# 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-)# 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-)# image resolution {fine standard super-fine passthrough}	Selects a specific resolution for the TIFF images attached to the fax-mail message forwarded via this dial peer.
Step 8 Router(config-dial-)# 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-)# 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-)# 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.

Configuring On-Ramp Modem Pooling

You can use modem pooling on the on-ramp gateway to determine which modems are available for the following:

- Fax and data
- Data only

As a default, store and forward fax receives faxes on modems that are in the on-ramp gateway default modem pool—meaning that these modems are available for both fax and data calls. The on-ramp gateway determines the call type by using the DNIS. The on-ramp gateway compares the DNIS to the configured value for the incoming called-number POTS dial-peer configuration command; if the DNIS matches the incoming called number, then it 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.

You can specify which incoming fax calls will not be presented to the default modem pool by defining a named modem pool. This is particularly useful if you have both MICA and Microcom faxes; it allows you to divert fax traffic from MICA modems, which at this time do not support fax transmission.

To configure on-ramp modem pooling, use the following commands beginning in privileged EXEC mode:

Command	Purpose
Step 1 Router# configure terminal	Enters global configuration mode.
Step 2 Router(config)# modem-pool <i>name</i>	Creates a modem pool.
Step 3 Router(config)# pool-range <i>number-number</i>	Assigns a range of modems to the specified modem pool.

Enabling the Nagle Congestion Control Algorithm

In the past, when a standard TCP application sent data between machines, TCP tended to send a series of small packets—for example, TCP would send one packet for each keystroke typed when sending keystrokes between machines. On larger networks, many small packets use up bandwidth and contribute to congestion. John Nagle's algorithm (RFC 896) helped alleviate the small-packet problem in TCP and now is being used, by default, in most modern TCP applications. The effect of this algorithm is to accumulate characters into larger chunks and pace them out to the network at a rate matching the round-trip time of the given connection. For more information about the Nagle algorithm (including a good description of how this algorithm works), refer to RFC 2001.

You need to enable Cisco routers and access servers to support the Nagle congestion control algorithm. To optimize store and forward fax performance and to avoid packet congestion, enable the Nagle congestion control algorithm by using the **service nagle** global configuration command.

To enable the Nagle Congestion Algorithm, use the following command in global configuration mode:

Command	Purpose
Router(config)# service nagle	(Optional) Enables the Nagle congestion control algorithm to optimize store and forward fax performance.

**Note**

There may be unexpected side effects with other services that run over TCP sockets on this same Cisco AS5300 if you enable the Nagle congestion algorithm when using store and forward fax. However, we are unaware of any side effects at this time.

Verifying the On-Ramp Gateway Configuration

- To verify the configured called-subscriber number, use the **debug fax receive called-number** command.
- To check the configured called subscriber number, send a fax and check the number in the sending machine LCD.
- To verify that store and forward fax dial peers have been configured correctly, use the **show dialplan number fax** command.
- To display Class 2 fax tracing information on all on-ramp fax connections, use the **debug fax receive all** command.
- To display output for all of the on-ramp client connections—meaning the messages exchanged (for example, the handshake) between the e-mail server and the on-ramp gateway, use the **debug mta send all** command.
- To display output for a specific on-ramp SMTP client connection during e-mail transmission, use the **debug mta send rept-to** command.
- To test connectivity between the on-ramp gateway and the e-mail server by sending a test e-mail to a specified e-mail address, use the **debug mmoip send email** command.
- If DID is not enabled, the server presents a dial tone to collect the digits. Make a POTS call to the on-ramp gateway and listen for a secondary dial tone to determine if DID is enabled or disabled.

Configuring the Off-Ramp Gateway

Off-ramp faxing requires the Cisco AS5300 acting as the off-ramp gateway to dial the POTS and communicate with a remote fax machine using standard fax protocols. The off-ramp gateway can send a message containing a TIFF image, a plain text message, or a message containing both.

The off-ramp gateway performs the following activities:

- Converts a fax-mail TIFF file (or plain text file) back into a standard format and delivers it to the recipient, which in this case is a Group 3 fax device. Store and forward fax does not alter the TIFF or plain text file in any way from its original format when converting it back into a standard fax format. The off-ramp gateway uses the receiving MTA and dial peers to perform this conversion.
- Delivers an e-mail message as a standard fax transmission, which is received and processed by a Group 3 fax device. The source of this transmission is an e-mail message. The Cisco AS5300 generates information to be appended to the top of each “faxed” page (meaning, 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.

**Note**

Off-ramp faxing activities are not mutually exclusive. You can create an e-mail to be sent as a fax and attach a TIFF file 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 gateway usually uses only POTS dial peers to define the line characteristics between the off-ramp gateway forwarding the converted e-mail message and the fax device; as an option, you can configure MMoIP dial peers, but MMoIP dial peers have limited functionality in off-ramp faxing activities. In general, off-ramp MMoIP dial peers merely define fax compression schemes and resolution and are useful only if you want to alter those parameters for the fax-mails being received.

**Note**

You can set up the off-ramp dial peers to steer specific outgoing fax calls to a specific T1 controller port. This capability enables you to route certain calls to a T1 trunk that may have a different rate structure. See the “Configuring Off-Ramp POTS Dial Peers” section on page 26 of this document.

The off-ramp gateway uses receiving MTAs to define the parameters associated with the AS5300 SMTP server, such as its SMTP host alias(es), which can be different than its normal DNS host name(s) or internal Cisco IOS host name. Off-ramp POTS dial peers basically define the telephone number of the destination fax device. Because a destination pattern is defined for an outbound POTS peer, you can use number expansion.

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 Off-Ramp POTS Dial Peers
- Configuring Off-Ramp MMoIP Dial Peers (Optional)
- Configuring the Faxed Header Information
- Configuring the Fax Cover Page Information

The first four tasks are applicable to all off-ramp faxing activities. The last two tasks apply only to off-ramp faxing activities where the fax transmission originates as an e-mail message.

Configuring the Transmitting Subscriber Number

The first step in configuring the off-ramp gateway, whether the off-ramp gateway will be 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 the number that will be 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 commands beginning in privileged EXEC mode:

Command	Purpose
Step 1 Router# configure terminal	Enters global configuration mode.
Step 2 Router(config)# fax send transmitting-subscriber { <i>sd\$</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

The next step is to 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

The next step in configuring the off-ramp gateway is to configure the receiving MTA. Receiving MTAs define the parameters associated with the SMTP server, such as defining the SMTP host alias(es). 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>
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 <i>number</i>	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 Off-Ramp MMoIP Dial Peers

When implementing store and forward fax on a modem card, the off-ramp gateway does not necessarily need to have MMoIP dial peers configured to establish connectivity with the receiving fax device; therefore, off-ramp MMoIP dial peers are optional when using a modem card. You basically use off-ramp MMoIP dial peers if you need to specify a particular resolution for the fax transmission or if you need to define an encoding type. For example, it might suit your company's needs to send the fax-mail using the least definition as possible to save network resources. In that case, you might want to define a higher image resolution using an off-ramp MMoIP dial peer. Another case where you might want to use an MMoIP dial peer would be if the fax devices in your network could only process a particular type of encoding or compression. If you do decide to configure a MMoIP dial peer, be sure to match the incoming called number command value with the destination pattern telephone number you configured for the corresponding on-ramp POTS dial peer.

Only two resolutions are available for this release: standard and fine. If you select any other **image resolution** command options (such as **passthrough** or **super-fine**), the fax will be sent using the fine resolution. Encoding type defines the type of compression scheme the off-ramp gateway uses for the TIFF image. There are four available compression options: Modified Huffman, Modified Read, Modified Modified Read, and passthrough.

Off-Ramp Gateway MMoIP Dial Peer/Call Discrimination Process

Once again, understanding how the off-ramp gateway uses MMoIP dial peers in the course of call discrimination is helpful before you configure off-ramp MMoIP dial peers. For the purposes of the following discussion, the term *destinationDN* refers to the telephone number of the fax machine where the user wants a fax to be sent, and *accessDN* refers to the telephone number dialed by a redialer to access an on-ramp gateway. For the on-ramp gateway to forward the fax-mail to the appropriate SMTP server, it converts the destinationDN into an e-mail address. The left side of this address is the destinationDN; the right side of this e-mail address defines the domain.

When the off-ramp router receives the fax-mail message, it looks at the destinationDN portion of the e-mail address and tries to match that value with the incoming called number field for each of the defined off-ramp MMoIP dial peers in its lookup table. If the off-ramp gateway finds an appropriate match, it uses the specified resolution and encoding values for the fax-mail message. If it cannot find a match, or if no resolution or encoding information has been defined for a matched off-ramp MMoIP dial peer, it applies fine resolution and non (passthrough) encoding for those parameters.

To configure off-ramp gateway MMoIP dial peers, 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-)# 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-)# 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-)# incoming called-number <i>string</i>	Identifies the destination fax telephone number.

Command	Purpose
Step 5 Router(config-dial-)# image resolution { fine standard super-fine passthrough }	Specifies the fax image resolution for TIFF files associated with this particular MMoIP dial peer. Only standard and fine fax resolutions are supported for Cisco IOS Release 12.1.
Step 6 Router(config-dial-)# image encoding { mh mr mmr passthrough }	Specifies the type of encoding to be used for TIFF files associated with this MMoIP dial peer.

Configuring Off-Ramp POTS Dial Peers

POTS dial peers configured for the off-ramp gateway define the line characteristics between the off-ramp gateway forwarding the converted e-mail message and the receiving fax device.

Off-Ramp Gateway POTS Dial Peer/Call Discrimination Process

Once again, understanding how the off-ramp gateway uses POTS dial peers in the course of call discrimination is helpful before you configure off-ramp POTS dial peers. For the purposes of the following discussion, the term *destinationDN* refers to the telephone number of the fax machine where the user wants a fax to be sent, and *accessDN* refers to the telephone number dialed by a redialer to access an on-ramp gateway. For the on-ramp gateway to forward the fax-mail to the appropriate SMTP server, it converts the destinationDN into an e-mail address. The left side of this address is the destinationDN; the right side of this e-mail address defines the domain.

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 to the destination DN portion of the fax-mail address and selects the first POTS dial peer where the data matches.

After the off-ramp gateway identifies the appropriate POTS dial peer, it then 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 this address will not be accepted by the off-ramp router.

To generate E.164 e-mail addresses compliant with RFC 2304, use the following address format: fax=+\$d\$@your.hostname.com. If the off-ramp gateway receives this type of e-mail address, it strips the + and matches an off-ramp POTS dial peer on 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).

To configure off-ramp gateway POTS dial peers, 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 enter dial-peer configuration mode.
Step 2 Router(config-dial-)# application <i>name</i> [out-bound]	Associates a specific IVR application with this dial peer. (The out-bound keyword is not used with POTS dial peers.)
Step 3 Router(config-dial-)# 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-)# destination-pattern [+] <i>stringT</i>	Identifies the destination fax telephone number.

Command	Purpose
Step 5 Router(config-dial-)# port controller number:D	(Optional) Specifies the T1 controller port through which to route the outgoing fax calls for this dial peer.
Step 6 Router(config-dial-)# 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 modem first, before the telephone number configured for this dial peer.

Configuring the Faxed Header Information

Store and forward fax lets you convert standard e-mail messages into fax transmissions. When you send a fax using a standard Group 3 device, there is usually header information appended to the top of each faxed cover and text page, indicating (among other things) the telephone number of the sending fax device, the date, and the time of transmission. Faxes created using an e-mail application need that header information appended to each faxed page. Store and forward fax lets you configure exactly what header information is appended to the top of each faxed cover and text page, along with its placement. In addition, you can also use the destination address of an e-mail message to control the cover page generation on a per-recipient basis.



Note

Because the off-ramp gateway does not alter fax TIFF attachments, you cannot configure faxed header information 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 You 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> }	Specifies the header information to be displayed on the right. 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 You use the <i>string</i> argument in this command to insert personalized text string.
Step 3 Router(config)# fax send left-header {\$a\$ \$d\$ \$p\$ \$s\$ \$t\$ <i>string</i> }	Specifies the header information to be displayed on the left. 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 You use the <i>string</i> variable in this command to insert personalized text string.

Configuring the Fax Cover Page Information

You can configure the off-ramp gateway to 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, you cannot configure cover pages 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.

You can also use the destination address of an e-mail message to control the cover page generation on a per-recipient basis. You 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.

In essence, the off-ramp router defers to the setting configured in the e-mail address itself. For example, if the address has a parameter set to `cover=no`, this parameter will override the setting for the **fax send coverpage enable** command and the off-ramp gateway will not generate and send a fax cover page. If the address has a parameter set to `cover=yes`, the off-ramp gateway will defer to the setting configured in the e-mail address and generate and send a fax cover page.

Table 4 contains examples of what the user would enter in the To: field of the e-mail message.

Table 4 To: Field Entry Examples

Example for To: Field Entries	Description
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 coverpage 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 coverpage enable command is superseded by the <code>cover=no</code> 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 coverpage enable command is superseded by the <code>cover=yes</code> 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 coverpage 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 coverpage 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 coverpage enable command.

Verifying the Off-Ramp Gateway Configuration

You can verify the off-ramp gateway configuration by performing the following tasks:


- To verify the information configured for the transmitting subscriber number, use the **debug fax send calling-number**.
- To display Class 2 fax protocol tracing information for all off-ramp faxing activities, use the **debug fax send all** command.
- Send a fax-mail message via 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. Request return receipt in the e-mail message. You should receive a returned receipt if the fax-mail is processed correctly.
- To show output relating to the activity on the SMTP server—meaning the messages exchanged (for example, the handshake) between the e-mail server and the off-ramp gateway, use the **debug mta receive all** command.
- To show information relating to the off-ramp text-to-fax conversion, use the **debug text-to-fax** command.
- To display output about the on-ramp TIFF reader, use the **debug tiff reader** command.
- To display output about the on-ramp TIFF writer, use the **debug tiff writer** command.
- If you have enabled fax cover pages, check whether the fax cover page generates correctly by sending an e-mail message to the off-ramp gateway.

Configuring IVR

To configure IVR functionality using either classic or TCL scripts, perform the following tasks after you have completed the prerequisite steps:

- Create an application that will interact with the appropriate classic or TCL script.
- Define and pass the defined parameter values to the application. Depending on the TCL script you select, these values can include the language of the audio file and the location of the audio file. Table 5 lists the TCL scripts and the parameter values they require.
- Associate the application to the incoming POTS dial peer.
- Define the appropriate method lists using AAA so that you identify RADIUS as the security protocol performing accounting.

To configure IVR, 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 for your application and indicates the location (URL) of the appropriate IVR script to be used with this application.
	 <p>Note The <i>application-name</i> is a user-defined name which, once defined, is referenced in all other IVR commands except for the application command used with the on-ramp MMOIP dial peer.</p>
Step 3 Router(config)# call application voice <i>application-name language language</i>	(Optional depending on the TCL script you select) Defines the language of the audio file for the designated application and passes that information to the application.
Step 4 Router(config)# call application voice <i>application-name pin-length number</i>	(Optional depending on the TCL script you select) Defines the number of characters in the PIN for the designated application and passes that information to the application.
Step 5 Router(config)# call application voice <i>application-name retry-count number</i>	(Optional depending on the TCL script you select) Defines the number of times a caller is permitted to reenter the PIN for the designated application and passes that information to the application.
Step 6 Router(config)# call application voice <i>application-name uid-length number</i>	(Optional depending on the TCL script you select) Defines the number of characters in the UID for the designated application and passes that information to the application.
Step 7 Router(config)# call application voice <i>application-name set-location language</i> <i>category location</i>	(Optional depending on the TCL script you select) Defines the location, language, and category of the audio files for the designated application 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.

Command	Purpose
Step 14 Router(config)# dial-peer voice <i>number</i> pots	Enter the dial-peer configuration mode to configure the incoming POTS dial peer. The <i>number</i> value of the dial-peer voice pots command is a tag that uniquely identifies the dial peer.
Step 15 Router(config-dial-peer)# application <i>application-name</i>	Associates the IVR application with the incoming POTS dial peer.
Step 16 Router(config-dial-peer)# destination-pattern [+] <i>string</i> t	Defines the telephone number associated with this dial peer.
Step 17 Router(config-dial-peer)# port <i>port number</i>	Defines the voice port associated with this dial peer.

Table 5 lists TCL script names and the corresponding parameters that are required for each TCL scripts.

Table 5 *TCL Scripts and Parameters*

TCL Script Name	Description — Summary	Commands to Configure
clid_4digits_npw_3_cli.tcl	This script authenticates the account number and PIN respectively using ANI and null. The length of digits allowed for the account number and password are configurable through the CLI. If the authentication fails, it allows the caller to retry. The retry number is also configured through the CLI.	call application voice uid-len min = 1, max = 20, default = 10 call application voice pin-len min = 0, max = 10, default = 4 call application voice retry-count min = 1, max = 5, default = 3
clid_authen_col_npw_cli.tcl	This script authenticates the account number and PIN respectively using ANI and null. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	call application voice retry-count min = 1, max = 5, default = 3
clid_authen_collect_cli.tcl	This script authenticates the account number and PIN using ANI and DNIS. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	call application voice retry-count min = 1, max = 5, default = 3

Table 5 *TCL Scripts and Parameters (continued)*

TCL Script Name	Description —Summary	Commands to Configure
clid_col_npw_3_cli.tcl	This script authenticates using ANI and null for account and PIN respectively. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI.	call application voice retry-count min = 1, max = 5, default = 3
clid_col_npw_npw_cli.tcl	This script authenticates using ANI and null for account and pin respectively. If authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected together.	call application voice retry-count min = 1, max = 5, default = 3
clid_t37_fax_onramp.tcl	This script authenticates the account and PIN using the following: prompt-user, ANI, DNIS, gateway ID, redialer ID, and redialer DNIS.	None
clid_t37_fax_offramp.tcl	This script authenticates the account and PIN using the following: envelope-from, envelope-to, gateway ID, and x-account ID.	None
clid_t37_fax_rollover.tcl	This script is used for on-ramp T.38 fax rollover to T.37 fax when the destination fax line is busy. The script name is an interim name for Beta.	voice hunt user-busy

**Note**

The two TCL scripts, `clid_t37_fax_onramp.tcl` and `clid_t37_fax_offramp.tcl`, have interim names in beta release.

Verifying IVR Configuration

You can verify IVR configuration by performing the following tasks:

- To verify IVR configuration parameters, use the **show running configuration** command.
- To display a list of all voice applications, use the **show call application summary** command.
- To show the contents of that script, use the **show call application voice** command.
- To verify that the operational status of the dial peer is up, use the **show dial-peer voice** command.

Specifying the Interface Type for Fax Calls


Fax calls cannot be made on modem cards and VFC cards simultaneously. When both types of interface cards are present in the Cisco AS5300 chassis, you must select the interface type on which you wish to make fax calls.

To specify the interface type you wish to use for fax calls, use the following command in global configuration mode:

Command	Purpose
Router(config)# fax interface-type { <i>modem</i> <i>vfc</i> }	Specifies the interface type that will be enabled for fax calls.

Specifying the TCL Application Files

To specify the names and locations of the IVR scripts containing the TCL application files for onramp and offramp operation, use the following command in global configuration mode:

Command	Purpose
Router(config)# call application voice <i>application-name location</i>	<p>Specifies the name and TFTP server location of an IVR script used to handle on-ramp or off-ramp fax operations.</p> <p> Note The <i>application-name</i> is a user-defined name which, once defined, is referenced in all other IVR commands except for the application command used with the onramp MMOIP dial peer.</p>

Configuring Gateway Security 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	Router(config)# call application voice <i>application-name</i> accounting enable	Enables AAA accounting services for the named application.
Step 2	Router(config)# call application voice <i>application-name</i> authentication enable	Enables AAA authentication services for the named application.
Step 3	Router(config)# call application voice <i>application-name</i> authen-list <i>method-list</i>	Specifies the name of an authentication method list for the named application.
Step 4	Router(config)# call application voice <i>application-name</i> authen-method <i>id</i>	Specifies the name of the authentication method for the named application. Valid authentication methods are prompt-user, gateway, ANI, DNIS, redialer DMS, and redialer serial number.

Associating TCL Applications with Dial Peers

To associate a TCL application file with a dial peer, use the following command in dial-peer configuration mode:

	Command	Purpose
Step 1	Router(config)# dial-peer voice <i>number</i> { pots vofr voip mmoip }	Specifies a dial-peer type and enters dial-peer configuration mode.
Step 2	Router(config-dial-peer)# application <i>name</i> [out-bound]	Associates the named TCL application with the specified dial peer. Use the out-bound keyword when the application handles the dial peer in outgoing mode.

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:

Reference configuration for Store and Forward Fax and Fax Relay

! using VFCs on a Cisco AS5300

```

!
! 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
!
! used for fallback from T.38 fax relay to T.37 fax
voice hunt user-busy
!
! global service for fax relay
voice service voip
  fax protocol t38 ls_redundancy 0 hs_redundancy 0
!
!
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 $$
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 for T.37 onramp operation
dial-peer voice 2 pots
  application app_onramp9
  incoming called-number 5.....
  direct-inward-dial
!
!
! Outbound peer for T.37 onramp operation
dial-peer voice 3 mmoip
  ! The application name below must be exactly as shown!
  application fax_on_vfc_onramp_app out-bound
  destination-pattern 57108..
  session target mailto:$d$@mail-server.cisco.com
! MDN and DSN configuration can be set in this peer
!
! Inbound peer for T.37 offramp operation
dial-peer voice 21 mmoip
  application lib_off_app5
  incoming called-number 5.....
  information-type fax
!
!
! Outbound peer for T.37 offramp operation
dial-peer voice 20 pots
  destination-pattern 5.....
  port 0:D
  prefix 5
!
!
! Notice that the pots 20 peer has "port 0:D" which
! means that when this peer is matched, controller
! : T1-0 will be used for the outgoing call.
!
! The following peers are for two different gateways
! processing the same call for T.38
!
! Inbound peer for T.38 ingress gateway
dial-peer voice 50 pots
  incoming called-number 1800555...
!
! Outbound peer for T.38 ingress gateway
dial-peer voice 51 voip
  destination-pattern 57108..
  session target ipv4:12.22.95.20
!
! Inbound peer for T.38 egress gateway
dial-peer voice 61 voip
  incoming called-number 57108..
!
!
! Outbound peer for T.38 egress gateway
dial-peer voice 60 pots
  destination-pattern 57108..
  port 0:D
  prefix 57108
!
!
! The following set of 3 peers are for onramp T.38 fax rollover to T.37 fax
! Rollover occurs when the destination fax line is busy
!
! The following configuration command must be set for T.38 rollover to T.37
voice hunt user-busy
!
!

```

```
! Inbound peer for T.38/T.37 onramp rollover operation
! This peer includes the TCL application for rollover operation
dial-peer voice 70 pots
  application app_lib_rollover15
  incoming called-number 5.....
!
!
! Outbound peer for T.38 ingress gateway
! This peer requires lower preference number than 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
!
!
! Outbound peer for T.37 onramp operation
dial-peer voice 72 mmoip
  preference 2
  ! The application name below must be exactly as shown!
  application fax_on_vfc_onramp_app out-bound
  destination-pattern 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
```

Command Reference

This section documents new or modified commands for the T.37/T.38 Fax Gateway feature. All other commands used with this feature are documented in the Cisco IOS Release 12.0(4)XJ *Store and Forward Fax* feature and in the Cisco IOS Release 12.1 *Cisco IOS Multiservice Applications Command Reference*.

- **application**
- **call application voice**
- **call application voice access-method**
- **call application voice accounting enable**
- **call application voice accounting-list**
- **call application voice authentication enable**
- **call application voice authen-list**
- **call application voice authen-method**
- **call application voice global-password**
- **call application voice language**
- **call application voice load**
- **call application voice pin-len**
- **call application voice redirect-number**
- **call application voice retry-count**
- **call application voice set-location**
- **call application voice uid-len**
- **call application voice warning-time**
- **fax interface-type**
- **fax protocol (voice-service)**
- **fax protocol (dial-peer)**
- **fax rate**
- **voice hunt user-busy**
- **voice service**

application

To enable a specific interactive voice response (IVR) application on a dial peer, use the **application** command in dial-peer configuration mode. To remove the application from the dial peer, use the **no** form of this command.

application *application-name* [**out-bound**]

no application *application-name* [**out-bound**]

Syntax	Description
<i>name</i>	Indicates the name of the predefined IVR application. Incoming calls using this POTS dial peer, and outgoing calls using the MMOIP dial peer, will be handed off to this application.
out-bound	The named application will handle the MMOIP dial peer in the outgoing mode.

Defaults No default behavior or values.

Command Modes Dial-peer configuration mode

Command History	Release	Modification
	11.3(6)NA2	This command was introduced.
	12.0(5)T	The SGCPAPP application was first supported on the Cisco AS5300 in a private release not generally available.
	12.0(7)XK	Support for the SGCPAPP application was extended to the Cisco MC3810 and the Cisco 3600 series routers (except for the Cisco 3620) in a private release that was not publically available.
	12.1(3)XI	The out-bound keyword was added for the store and forward fax feature on the Cisco AS5300 access server.

Usage Guidelines Use this command when configuring interactive voice response (IVR) or any of the IVR-related features to associate a predefined session application with an incoming POTS dial peer or an outgoing MMOIP dial peer. Calls using this incoming POTS dial peer or this outgoing MMOIP dial peer will be handed to the predefined specified session application.

Examples

This following example shows how to define an application and how to apply it to an incoming POTS dial peer:

```
Router(config)# call application voice c4 tftp://santa/username/clid_4digits_npw_3.tcl
Router(config)#
!
Router(config-if)# dial-peer voice 100 pots
Router(config-dial-peer)# application c4
Router(config-dial-peer)#
```

Related Commands

Command	Description
call application voice	Defines the name to be used for an application and indicates the location of the appropriate IVR script to be used with this application.

call application voice

To create an application and to indicate the location where the corresponding TCL files that implement this application are located, use the **call application voice** command in global configuration mode. To remove the defined application and all configured parameters associated with it, use the **no** form of the command.

call application voice *application-name location*

no call application voice *application-name location*

Syntax Description

<i>application-name</i>	User-defined character string that names the application located at the URL specified in <i>location</i> .
<i>location</i>	The location of the TCL file in URL format. Valid storage locations are TFTP, FTP, and Flash.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.

Usage Guidelines

Use this command when configuring interactive voice response (IVR) or one of the IVR-related features (such as Debit Card) to define the name of an application and to identify the location of the TCL script associated with this application.

Examples

This example shows how to define the application “prepaid” and the TFTP server location of the associated TCL script:

```
Router(config)# call application voice prepaid tftp://keyer/debitcard.tcl
```

Related Commands

Command	Description
call application voice access-method	Specifies the access method for the designated application.
call application voice language	Defines the language of the audio file for the designated application and passes that information to the application.
call application voice load	Reload the designated TCL script.
call application voice pin-len	Defines the number of characters in the personal identification number (PIN) for the application and passes that information to the application.

Command	Description
call application voice redirect-number	Defines the telephone number to which a call will be redirected—for example, the operator telephone number of the service provider—for the designated application.
call application voice retry-count	Defines the number of times a caller is permitted to reenter the PIN for a designated application and passes that information to the application.
call application voice set-location	Defines the location, language, and category of the audio files for the designated application and passes that information to the application.
call application voice uid-len	Defines the number of characters in the UID for the designated application and passes that information to the application.
call application voice warning-time	Defines the number of seconds a user is warned before their allowed calling time runs out for the designated application.

call application voice access-method

To specify the access method for two-stage dialing for the designated application, use the **call application voice access-method** command in global configuration mode. To restore default values for this command, use the **no** form of this command.

call application voice *application-name* **access-method** { **prompt-user** | **redialer** }

no call application voice *application-name* **access-method**

Syntax Description	
<i>application-name</i>	The name of the application.
prompt-user	Specifies that no DID is set in the incoming POTS dial peer and that a TCL script in the incoming POTS dial peer will be used for two-stage dialing.
redialer	Specifies that no DID is set in the incoming POTS dial peer and that the redialer device will be used for two-stage dialing.

Defaults prompt-user (when DID is not set in the dial peer)

Command Modes Global configuration mode

Command History	Release	Modification
	12.1(3)XI	This command was introduced on the Cisco AS5300 access server.

Usage Guidelines Use the call application voice access-method command to specify the access method for two-stage dialing when DID is disabled in the POTS dial peer.

Examples The following example specifies **prompt-user** as the access method for two-stage dialing for the **app_onramp6** IVR application:

```
Router(config)# call application voice app_onramp6 access-method prompt-user
```

Related Commands	Command	Description
	call application voice	Defines the name to be used for an application and indicates the location of the appropriate IVR script to be used with this application.
	call application voice language	Defines the language of the audio file for the designated application and passes that information to the application.
	call application voice load	Reload the designated TCL script.

Command	Description
call application voice pin-len	Defines the number of characters in the personal identification number (PIN) for the application and passes that information to the application.
call application voice redirect-number	Defines the telephone number to which a call will be redirected—for example, the operator telephone number of the service provider—for the designated application.
call application voice retry-count	Defines the number of times a caller is permitted to reenter the PIN for a designated application and passes that information to the application.
call application voice set-location	Defines the location, language, and category of the audio files for the designated application and passes that information to the application.
call application voice uid-len	Defines the number of characters in the UID for the designated application and passes that information to the application.
call application voice warning-time	Defines the number of seconds a user is warned before their allowed calling time runs out for the designated application.

call application voice accounting enable

To enable AAA accounting for a TCL application, use the **call application voice accounting** command in global configuration mode. To disable accounting for a TCL application, use the **no** form of this command.

call application voice *application-name* **accounting enable**

no call application voice *application-name* **accounting enable**

Syntax Description	<i>application-name</i> The name of the application.				
Defaults	Disabled				
Command Modes	Global configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.1(3)XI</td> <td>This command was introduced on the Cisco AS5300 access server.</td> </tr> </tbody> </table>	Release	Modification	12.1(3)XI	This command was introduced on the Cisco AS5300 access server.
Release	Modification				
12.1(3)XI	This command was introduced on the Cisco AS5300 access server.				
Usage Guidelines	<p>This command enables AAA accounting services if a AAA accounting method list has been defined using both the aaa accounting command and the mmoip aaa method fax accounting command.</p> <p>This command applies to off-ramp store and forward fax functions on AS5300 voice feature cards. It is not used on modem cards.</p>				
Examples	<p>The following example enables a AAA accounting to be used with outbound store and forward fax:</p> <pre>Router(config)# call application voice app_onramp6 accounting enable</pre>				
Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>mmoip aaa method fax accounting</td> <td>Defines the name of the method list to be used for AAA accounting with store and forward fax.</td> </tr> </tbody> </table>	Command	Description	mmoip aaa method fax accounting	Defines the name of the method list to be used for AAA accounting with store and forward fax.
Command	Description				
mmoip aaa method fax accounting	Defines the name of the method list to be used for AAA accounting with store and forward fax.				

call application voice accounting-list

To define the name of the method list to be used for AAA accounting with store and forward fax on a voice feature card, use the **call application voice accounting-list** global configuration command. Use the **no** form of this command to restore the default value.

call application voice *application-name* **accounting-list** *method-list-name*

no call application voice *application-name* **accounting-list** *method-list-name*

Syntax Description

<i>application-name</i>	The name of the application.
<i>method-list-name</i>	Character string used to name a list of accounting methods to be used with store and forward fax.

Defaults

No AAA accounting method list defined.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(3)XI	This command was introduced on the Cisco AS5300 access server.

Usage Guidelines

This command defines the name of the AAA accounting method list to be used with store and forward fax. The method list itself, which defines the type of accounting services provided for store and forward fax, is defined using the **aaa accounting** global configuration command. Unlike standard AAA (where each defined method list can be applied to specific interfaces and lines), the AAA accounting method lists used in store and forward fax are applied globally on the Cisco AS5300.

After the accounting method lists have been defined, they are enabled by using the **mmoip aaa receive-accounting enable** command.

This command applies to both on-ramp and off-ramp store and forward fax functions on AS5300 voice feature cards. It is not used on modem cards.

Examples

The following example defines a AAA accounting method list (called sherman) to be used with store and forward fax:

```
Router(config)# aaa new-model
Router(config)# call application voice app_onramp6 accounting-list sherman
```

Related Commands

Command	Description
call application voice accounting enable	Enables on-ramp AAA accounting services.

call application voice authentication enable

To enable AAA authentication services for a TCL application, use the **call application voice authentication** command in global configuration mode. To disable authentication for a TCL application, use the **no** form of this command.

call application voice *application-name* **authentication enable**

no call application voice *application-name* **authentication enable**

Syntax Description	<i>application-name</i> The name of the application.
---------------------------	--

Defaults	No default behavior or values.
-----------------	--------------------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.1(3)XI	This command was introduced on the Cisco AS5300 access server.

Usage Guidelines	This command enables AAA authentication services for a TCL application if a AAA authentication method list has been defined using both the aaa authentication command and the call application voice authen-list command.
-------------------------	---

Examples	The following example enables a AAA authentication method list (called peabody) to be used with outbound store and forward fax.
-----------------	---

```
Router(config)# aaa new-model
Router(config)# call application voice app_onramp6 authen-list peabody
Router(config)# call application voice app_onramp6 authentication enable
```

Related Commands	Command	Description
	call application voice authen-list	Specifies the name of an authentication method list for a TCL application.
call application voice authen-method	Specifies the authentication method for a TCL application.	

call application voice authen-list

To specify the name of an authentication method list for a TCL application, use the **call application voice authen-list** command in global configuration mode. To disable the authentication method list for a TCL application, use the **no** form of this command.

call application voice *application-name* **authen-list** *method-list-name*

no call application voice *application-name* **authen-list** *method-list-name*

Syntax Description

<i>application-name</i>	The name of the application.
<i>method-list-name</i>	Character string used to name a list of authentication methods to be used with T.38 fax relay and T.37 store and forward fax.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)XI	This command was introduced on the Cisco AS5300 access server.

Usage Guidelines

This command defines the name of the AAA authentication method list to be used with fax applications on voice feature cards. The method list itself, which defines the type of authentication services provided for store and forward fax, is defined using the **aaa authentication** global configuration command. Unlike standard AAA (where each defined method list can be applied to specific interfaces and lines), AAA authentication method lists used with fax applications are applied globally on the Cisco AS5300. After the authentication method lists have been defined, they are enabled by using the **call application voice authentication enable** command.

Examples

The following example defines a AAA authentication method list (called fax) to be used with T.38 fax relay and T.37 store and forward fax:

```
Router(config)# call application voice app_onramp6 authen-list fax
```

Related Commands

Command	Description
call application voice authentication enable	Enables AAA authentication services for a TCL application.
call application voice authen-method	Specifies the authentication method for a TCL application.

call application voice authen-method

To specify a AAA authentication method for a TCL application, use the **call application voice authen-method** command in global configuration mode. To disable the authentication method for a TCL application, use the **no** form of this command.

```
call application voice application-name authen-method {prompt-user | ani | dnis | gateway | redialer-id | redialer-dnis}
```

```
no call application voice application-name authen-method {prompt-user | ani | dnis | gateway | redialer-id | redialer-dnis}
```

Syntax Description

<i>application-name</i>	The name of the application.
prompt-user	Indicates that the user is prompted for the TCL application account identifier.
ani	Indicates that the calling party telephone number (automatic number identification or ANI) is used as the TCL application account identifier.
dnis	Indicates that the called party telephone number (dialed number identification service or DNIS) is used as the TCL application account identifier.
gateway	Indicates that the router-specific name derived from the host name and domain name is used as the TCL application account identifier, displayed in the following format: <i>router-name.domain-name</i> .
redialer-id	Indicates that the account string returned by the external redialer device is used as the TCL application account identifier. In this case, the redialer ID is either the redialer serial number or the redialer account number.
redialer-dnis	Indicates that the called party telephone number (dialed number identification service or DNIS) is used as the TCL application account identifier captured by the redialer if a redialer device is present.

Defaults

No default behavior or values.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(3)XI	This command was introduced on the Cisco AS5300 access server.

Usage Guidelines

Normally, when AAA is being used for simple user authentication, AAA uses the username information defined in the user profile for authentication. With T.37 store and forward fax and T.38 real-time fax, you can specify that the ANI, DNIS, gateway ID, redialer ID, or redialer DNIS be used to identify the user for authentication, or that the user be prompted for the TCL application .

Examples

The following example shows how to configure the router-specific name derived from the host name and domain name as the TCL application account identifier for the **app_onramp6** TCL application:

```
Router(config)# call application voice app_onramp6 authen-method gateway
```

Related Commands

Command	Description
call application voice authentication enable	Enables AAA authentication services for a TCL application.
call application voice authen-list	Specifies the name of an authentication method list for a TCL application.

call application voice global-password

To define a password to be used with CiscoSecure for Windows NT when using store and forward fax on a voice feature card, use the **call application voice global-password** global configuration command. Use the **no** form of this command to restore the default value.

call application voice *application-name* **global-password** *password*

no call application voice *application-name* **global-password** *password*

Syntax Description

<i>application-name</i>	The name of the application.
<i>password</i>	Character string used to define the CiscoSecure for Windows NT password to be used with store and forward fax. Maximum length is 64 alphanumeric characters.

Defaults

No password defined.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)XI	This command was introduced on the Cisco AS5300 access server.

Usage Guidelines

CiscoSecure for Windows NT might require a separate password in order to complete authentication, no matter what security protocol you use. This command defines the password to be used with CiscoSecure for Windows NT. All records on the Windows NT server use this defined password.

This command applies to on-ramp store and forward fax functions on AS5300 voice feature cards. It is not used on modem cards.

Examples

The following example defines a password (abercrombie) for use by AAA for the **app_onramp6** TCL application:

```
Router(config)# call application voice app_onramp6 global-password abercrombie
```

call application voice language

To define the language of the audio file for the specified application and to pass that information to the specified application, use the **call application voice language** command in global configuration mode. To remove the associated language of the audio file from the application, use the **no** form of this command.

call application voice *application-name* **language** *number language*

no call application voice *application-name* **language** *number language*

Syntax Description		
<i>application-name</i>	The name of the application to which the language parameters are being passed.	
<i>number</i>	Tag that uniquely identifies an audio file. Valid entries are 0 to 9.	
<i>language</i>	Defines the language of the associated audio file. Valid entries are:	<ul style="list-style-type: none"> • en—English • sp—Spanish • ch—Mandarin • aa—all

Defaults No default behavior or values.

Command Modes Global configuration

Command History	Release	Modification
	12.0(7)T	This command was introduced.

Usage Guidelines Use this command when configuring IVR (depending on the TCL script being used) or one of the IVR-related features (such as Debit Card) to define the language of the audio file for the specified application and to pass that information to the specified application.

Table 6 lists TCL script names and the corresponding parameters that are required for each TCL scripts.

Table 6 *TCL Scripts and Parameters*

TCL Script Name	Description —Summary	Commands to Configure
clid_4digits_npw_3_cli.tcl	This script authenticates the account number and PIN respectively using ANI and null. The length of digits allowed for the account number and password are configurable through the CLI. If the authentication fails, it allows the caller to retry. The retry number is also configured through the CLI.	call application voice uid-len min = 1, max = 20, default = 10 call application voice pin-len min = 0, max = 10, default = 4 call application voice retry-count min = 1, max = 5, default = 3
clid_authen_col_npw_cli.tcl	This script authenticates the account number and PIN respectively using ANI and null. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	call application voice retry-count min = 1, max = 5, default = 3
clid_authen_collect_cli.tcl	This script authenticates the account number and PIN using ANI and DNIS. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	call application voice retry-count min = 1, max = 5, default = 3
clid_col_npw_3_cli.tcl	This script authenticates using ANI and null for account and PIN respectively. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI.	call application voice retry-count min = 1, max = 5, default = 3
clid_col_npw_npw_cli.tcl	This script authenticates using ANI and null for account and pin respectively. If authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected together.	call application voice retry-count min = 1, max = 5, default = 3

Table 6 TCL Scripts and Parameters (continued)

TCL Script Name	Description — Summary	Commands to Configure
clid_t37_fax_onramp.tcl	This script authenticates the account and PIN using the following: prompt-user, ANI, DNIS, gateway ID, redialer ID, and redialer DNIS.	None
clid_t37_fax_offramp.tcl	This script authenticates the account and PIN using the following: envelope-from, envelope-to, gateway ID, and x-account ID.	None
clid_t37_fax_rollover.tcl	This script is used for on-ramp T.38 fax rollover to T.37 fax when the destination fax line is busy. The script name is an interim name for Beta.	voice hunt user-busy

**Note**

The two TCL scripts, clid_t37_fax_onramp.tcl and clid_t37_fax_offramp.tcl, have interim names in beta release.

Examples

The following example shows how to define English and Spanish as the languages of the audio files associated with the application named prepaid:

```
Router(config)# call application voice prepaid language 1 en
Router(config)# call application voice prepaid language 2 sp
```

Related Commands

Command	Description
call application voice	Defines the name to be used for an application and indicates the location of the appropriate IVR script to be used with this application.
call application voice load	Reload the designated TCL script.
call application voice pin-len	Defines the number of characters in the PIN for the application and passes that information to the application.
call application voice redirect-number	Defines the telephone number to which a call will be redirected—for example, the operator telephone number of the service provider—for the designated application.
call application voice retry-count	Defines the number of times a caller is permitted to reenter the PIN for a designated application and passes that information to the application.
call application voice set-location	Defines the location, language, and category of the audio files for the designated application and passes that information to the application.

Command	Description
call application voice uid-len	Defines the number of characters in the UID for the designated application and passes that information to the application.
call application voice warning-time	Defines the number of seconds a user is warned before their allowed calling time runs out for the designated application.

call application voice load

To reload the selected TCL script from the URL, use the **call application voice load** command in privileged EXEC mode.

call application voice load *name*

Syntax Description

<i>name</i>	Defines the TCL application to use for the call.
-------------	--

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced.

Usage Guidelines

The software checks the signature lock to ensure it is a Cisco-supported TCL script.



Note

If the TCL script does not have a valid Cisco-supported signature, the software fails to load the script and generates the following error message:

```
00:02:54: %IVR-3-BAD_IVR_SIG: Script signature is invalid
```

Examples

The following example shows how to reload the TCL script called `clid_4digits_npw_3.tcl`:

```
Router(config)# call application voice load clid_4digits_npw_3.tclj
```

call application voice pin-len

To define the number of characters in the personal identification number (PIN) for the designated application, use the **call application voice pin-len** command in global configuration mode. To restore default values for this command, use the **no** form of this command.

call application voice *application-name* **pin-len** *number*

no call application voice *application-name* **pin-len** *number*

Syntax Description	
<i>application-name</i>	The name of the application to which the PIN length parameter is being passed.
<i>number</i>	Defines the number of allowable characters in PINs associated with the specified application. Valid entries are 0 to 10.

Defaults No default behavior or values.

Command Modes Global configuration

Command History	Release	Modification
	12.0(7)T	This command was introduced.

Usage Guidelines Use this command when configuring IVR (depending on the TCL script being used) or one of the IVR-related features (such as Debit Card) to define the number of allowable characters in a PIN for the specified application and to pass that information to the specified application.

Table 7 lists TCL script names and the corresponding parameters that are required for each TCL scripts.

Table 7 *TCL Scripts and Parameters*

TCL Script Name	Description —Summary	Commands to Configure
clid_4digits_npw_3_cli.tcl	This script authenticates the account number and PIN respectively using ANI and null. The length of digits allowed for the account number and password are configurable through the CLI. If the authentication fails, it allows the caller to retry. The retry number is also configured through the CLI.	call application voice uid-len min = 1, max = 20, default = 10 call application voice pin-len min = 0, max = 10, default = 4 call application voice retry-count min = 1, max = 5, default = 3
clid_authen_col_npw_cli.tcl	This script authenticates the account number and PIN respectively using ANI and null. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	call application voice retry-count min = 1, max = 5, default = 3
clid_authen_collect_cli.tcl	This script authenticates the account number and PIN using ANI and DNIS. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	call application voice retry-count min = 1, max = 5, default = 3
clid_col_npw_3_cli.tcl	This script authenticates using ANI and null for account and PIN respectively. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI.	call application voice retry-count min = 1, max = 5, default = 3
clid_col_npw_npw_cli.tcl	This script authenticates using ANI and null for account and pin respectively. If authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected together.	call application voice retry-count min = 1, max = 5, default = 3

Table 7 TCL Scripts and Parameters (continued)

TCL Script Name	Description — Summary	Commands to Configure
clid_t37_fax_onramp.tcl	This script authenticates the account and PIN using the following: prompt-user, ANI, DNIS, gateway ID, redialer ID, and redialer DNIS.	None
clid_t37_fax_offramp.tcl	This script authenticates the account and PIN using the following: envelope-from, envelope-to, gateway ID, and x-account ID.	None
clid_t37_fax_rollover.tcl	This script is used for on-ramp T.38 fax rollover to T.37 fax when the destination fax line is busy. The script name is an interim name for Beta.	voice hunt user-busy

**Note**

The two TCL scripts, clid_t37_fax_onramp.tcl and clid_t37_fax_offramp.tcl, have interim names in beta release.

Examples

The following example shows how to define a PIN length of 4 characters for the application named **prepaid**:

```
Router(config)# call application voice prepaid pin-len 4
```

Related Commands

Command	Description
call application voice	Defines the name to be used for an application and indicates the location of the appropriate IVR script to be used with this application.
call application voice language	Defines the language of the audio file for the designated application and passes that information to the application.
call application voice load	Reload this designated TCL script.
call application voice redirect-number	Defines the telephone number to which a call will be redirected—for example, the operator telephone number of the service provider—for the designated application.
call application voice retry-count	Defines the number of times a caller is permitted to reenter the PIN for a designated application and passes that information to the application.
call application voice set-location	Defines the location, language, and category of the audio files for the designated application and passes that information to the application.

Command	Description
call application voice uid-len	Defines the number of characters in the UID for the designated application and passes that information to the application.
call application voice warning-time	Defines the number of seconds a user is warned before their allowed calling time runs out for the designated application.

call application voice redirect-number

To define the telephone number to which a call will be redirected—for example, the operator telephone number of the service provider—for the designated application, use the **call application voice redirect-number** command in global configuration mode. To cancel this particular parameter, use the **no** form of this command.

call application voice *application-name* **redirect-number** *number*

no call application voice *application-name* **redirect-number** *number*

Syntax Description	<i>application-name</i>	The name of the application to which the redirect telephone number parameter is being passed.
	<i>number</i>	Defines the designated operator telephone number of the service provider (or any other number designated by the customer). This is the number that calls are terminated to when, for example, debit time allowed has run out or the debit amount is exceeded.

Defaults No default behavior or values.

Command Modes Global configuration

Command History	Release	Modification
	12.0(7)T	This command was introduced.

Usage Guidelines Use this command when configuring IVR (depending on the TCL script being used) or one of the IVR-related features (such as Debit Card) to define the telephone number to which a call will be redirected.

Table 8 lists TCL script names and the corresponding parameters that are required for each TCL scripts.

Table 8 TCL Scripts and Parameters

TCL Script Name	Description —Summary	Commands to Configure
clid_4digits_npw_3_cli.tcl	This script authenticates the account number and PIN respectively using ANI and null. The length of digits allowed for the account number and password are configurable through the CLI. If the authentication fails, it allows the caller to retry. The retry number is also configured through the CLI.	call application voice uid-len min = 1, max = 20, default = 10 call application voice pin-len min = 0, max = 10, default = 4 call application voice retry-count min = 1, max = 5, default = 3
clid_authen_col_npw_cli.tcl	This script authenticates the account number and PIN respectively using ANI and null. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	call application voice retry-count min = 1, max = 5, default = 3
clid_authen_collect_cli.tcl	This script authenticates the account number and PIN using ANI and DNIS. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	call application voice retry-count min = 1, max = 5, default = 3
clid_col_npw_3_cli.tcl	This script authenticates using ANI and null for account and PIN respectively. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI.	call application voice retry-count min = 1, max = 5, default = 3
clid_col_npw_npw_cli.tcl	This script authenticates using ANI and null for account and pin respectively. If authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected together.	call application voice retry-count min = 1, max = 5, default = 3

Table 8 *TCL Scripts and Parameters (continued)*

TCL Script Name	Description — Summary	Commands to Configure
clid_t37_fax_onramp.tcl	This script authenticates the account and PIN using the following: prompt-user, ANI, DNIS, gateway ID, redialer ID, and redialer DNIS.	None
clid_t37_fax_offramp.tcl	This script authenticates the account and PIN using the following: envelope-from, envelope-to, gateway ID, and x-account ID.	None
clid_t37_fax_rollover.tcl	This script is used for on-ramp T.38 fax rollover to T.37 fax when the destination fax line is busy. The script name is an interim name for Beta.	voice hunt user-busy

**Note**

The two TCL scripts, clid_t37_fax_onramp.tcl and clid_t37_fax_offramp.tcl, have interim names in beta release.

Examples

The following example shows how to define a redirect number for the application named prepaid:

```
Router(config)# call application voice prepaid redirect-number 5551111
```

Related Commands

Command	Description
call application voice	Defines the name to be used for an application and indicates the location of the appropriate IVR script to be used with this application.
call application voice language	Defines the language of the audio file for the designated application and passes that information to the application.
call application voice load	Reload the designated TCL script.
call application voice pin-len	Defines the number of characters in the PIN for the application and passes that information to the application.
call application voice retry-count	Defines the number of times a caller is permitted to reenter the PIN for a designated application and passes that information to the application.
call application voice set-location	Defines the location, language, and category of the audio files for the designated application and passes that information to the application.

Command	Description
call application voice uid-len	Defines the number of characters in the UID for the designated application and passes that information to the application.
call application voice warning-time	Defines the number of seconds a user is warned before their allowed calling time runs out for the designated application.

call application voice retry-count

To define the number of times a caller is permitted to reenter the personal identification number (PIN) for the designated application, use the **call application voice retry-count** command in global configuration mode. To cancel this particular parameter, use the **no** form of this command.

call application voice *application-name* **retry-count** *number*

no call application voice *application-name* **retry-count** *number*

Syntax Description	<i>application-name</i>	The name of the application to which the number of possible retries is being passed.
	<i>number</i>	Defines the number of times the caller is permitted to re-enter PIN digits. Valid entries for this parameter are 1 to 5.

Defaults No default behavior or values.

Command Modes Global configuration

Command History	Release	Modification
	12.0(7)T	This command was introduced.

Usage Guidelines Use this command when configuring IVR (depending on the TCL script being used) or one of the IVR-related features (such as Debit Card) to define how many times a user can reenter a PIN.

Table 9 lists TCL script names and the corresponding parameters that are required for each TCL scripts

Table 9 TCL Scripts and Parameters

TCL Script Name	Description —Summary	Commands to Configure
clid_4digits_npw_3_cli.tcl	This script authenticates the account number and PIN respectively using ANI and null. The length of digits allowed for the account number and password are configurable through the CLI. If the authentication fails, it allows the caller to retry. The retry number is also configured through the CLI.	call application voice uid-len min = 1, max = 20, default = 10 call application voice pin-len min = 0, max = 10, default = 4 call application voice retry-count min = 1, max = 5, default = 3
clid_authen_col_npw_cli.tcl	This script authenticates the account number and PIN respectively using ANI and null. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	call application voice retry-count min = 1, max = 5, default = 3
clid_authen_collect_cli.tcl	This script authenticates the account number and PIN using ANI and DNIS. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	call application voice retry-count min = 1, max = 5, default = 3
clid_col_npw_3_cli.tcl	This script authenticates using ANI and null for account and PIN respectively. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI.	call application voice retry-count min = 1, max = 5, default = 3
clid_col_npw_npw_cli.tcl	This script authenticates using ANI and null for account and pin respectively. If authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected together.	call application voice retry-count min = 1, max = 5, default = 3

Table 9 *TCL Scripts and Parameters (continued)*

TCL Script Name	Description —Summary	Commands to Configure
clid_t37_fax_onramp.tcl	This script authenticates the account and PIN using the following: prompt-user, ANI, DNIS, gateway ID, redialer ID, and redialer DNIS.	None
clid_t37_fax_offramp.tcl	This script authenticates the account and PIN using the following: envelope-from, envelope-to, gateway ID, and x-account ID.	None
clid_t37_fax_rollover.tcl	This script is used for on-ramp T.38 fax rollover to T.37 fax when the destination fax line is busy. The script name is an interim name for Beta.	voice hunt user-busy

**Note**

The two TCL scripts, clid_t37_fax_onramp.tcl and clid_t37_fax_offramp.tcl, have interim names in beta release.

Examples

The following example shows how to define that a user can re-enter a PIN 3 times before being disconnected for the application named prepaid:

```
Router(config)# call application voice prepaid retry-count 3
```

Related Commands

Command	Description
call application voice	Defines the name to be used for an application and indicates the location of the appropriate IVR script to be used with this application.
call application voice language	Defines the language of the audio file for the designated application and passes that information to the application.
call application voice load	Reload the designated TCL script.
call application voice pin-len	Defines the number of characters in the PIN for the application and passes that information to the application.
call application voice redirect-number	Defines the telephone number to which a call will be redirected—for example, the operator telephone number of the service provider—for the designated application.
call application voice set-location	Defines the location, language, and category of the audio files for the designated application and passes that information to the application.

Command	Description
call application voice uid-len	Defines the number of characters in the UID for the designated application and passes that information to the application.
call application voice warning-time	Defines the number of seconds a user is warned before their allowed calling time runs out for the designated application.

call application voice set-location

To define the location, language, and category of the audio files for the specified application, use the **call application voice set-location** command in global configuration mode. To cancel this particular parameter, use the **no** form of this command.

call application voice *application-name* **set-location** *language category location*

no call application voice *application-name* **set-location** *language category location*

Syntax Description	
<i>application-name</i>	The name of the application to which the set-location parameters are being passed.
<i>language</i>	Defines the language associated with the audio files. Possible values for this parameter are: <ul style="list-style-type: none"> • en = English, • ch = Mandarin • sp = Spanish
<i>category</i>	Defines a particular category group. Audio files can be divided into category groups (from 0 to 4). For example, audio files representing the days and months can be category 1, audio files representing units of currency can be category 2, audio files representing units of time: seconds, minutes, and hours can be category 3. Min = 0, Max = 4 (0 means all).
<i>location</i>	Defines the location (audio file URL or directory in the TFTP server) where the audio files are stored.

Defaults No default behavior or values.

Command Modes Global configuration

Command History	Release	Modification
	12.0(7)T	This command was introduced.

Usage Guidelines Use this command when configuring IVR (depending on the TCL script being used) or one of the IVR-related features (such as Debit Card) to define the location, language, and category of the audio files for the designated application and pass that information to the application.

Table 10 lists TCL script names and the corresponding parameters that are required for each TCL scripts.

Table 10 *TCL Scripts and Parameters*

TCL Script Name	Description —Summary	Commands to Configure
clid_4digits_npw_3_cli.tcl	This script authenticates the account number and PIN respectively using ANI and null. The length of digits allowed for the account number and password are configurable through the CLI. If the authentication fails, it allows the caller to retry. The retry number is also configured through the CLI.	call application voice uid-len min = 1, max = 20, default = 10 call application voice pin-len min = 0, max = 10, default = 4 call application voice retry-count min = 1, max = 5, default = 3
clid_authen_col_npw_cli.tcl	This script authenticates the account number and PIN respectively using ANI and null. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	call application voice retry-count min = 1, max = 5, default = 3
clid_authen_collect_cli.tcl	This script authenticates the account number and PIN using ANI and DNIS. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	call application voice retry-count min = 1, max = 5, default = 3
clid_col_npw_3_cli.tcl	This script authenticates using ANI and null for account and PIN respectively. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI.	call application voice retry-count min = 1, max = 5, default = 3
clid_col_npw_npw_cli.tcl	This script authenticates using ANI and null for account and pin respectively. If authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected together.	call application voice retry-count min = 1, max = 5, default = 3

Table 10 TCL Scripts and Parameters (continued)

TCL Script Name	Description —Summary	Commands to Configure
clid_t37_fax_onramp.tcl	This script authenticates the account and PIN using the following: prompt-user, ANI, DNIS, gateway ID, redialer ID, and redialer DNIS.	None
clid_t37_fax_offramp.tcl	This script authenticates the account and PIN using the following: envelope-from, envelope-to, gateway ID, and x-account ID.	None
clid_t37_fax_rollover.tcl	This script is used for on-ramp T.38 fax rollover to T.37 fax when the destination fax line is busy. The script name is an interim name for Beta.	voice hunt user-busy

**Note**

The two TCL scripts, clid_t37_fax_onramp.tcl and clid_t37_fax_offramp.tcl, have interim names in beta release.

Examples

The following example shows how to configure the **call application voice set-location** command for the application named prepaid. In this example, the language defined is English, the category into which the audio files are group is Category 0 (meaning all) and the location is the keyer directory on the TFTP server.

```
Router(config)# call application voice prepaid set-location en 0 tftp://keyer/
```

Related Commands

Command	Description
call application voice	Defines the name to be used for an application and indicates the location of the appropriate IVR script to be used with this application.
call application voice language	Defines the language of the audio file for the designated application and passes that information to the application.
call application voice load	Reload this designated TCL script.
call application voice pin-len	Defines the number of characters in the PIN for the application and passes that information to the application.
call application voice redirect-number	Defines the telephone number to which a call will be redirected—for example, the operator telephone number of the service provider—for the designated application.

Command	Description
call application voice retry-count	Defines the number of times a caller is permitted to reenter the PIN for a designated application and passes that information to the application.
call application voice uid-len	Defines the number of characters in the UID for the designated application and passes that information to the application.
call application voice warning-time	Defines the number of seconds a user is warned before their allowed calling time runs out for the designated application.

call application voice uid-len

To define the number of characters in the user identification number (UID) for the designated application, use the **call application voice uid-length** command in global configuration mode. To restore default values for this command, use the **no** form of this command.

call application voice *application-name* **uid-len** *number*

no call application voice *application-name* **uid-len** *number*

Syntax Description

<i>application-name</i>	The name of the application to which the UID length parameter is being passed.
<i>number</i>	Defines the number of allowable characters in UIDs associated with the specified application. Valid entries are from 1 to 64.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.

Usage Guidelines

Use this command when configuring IVR (depending on the TCL script being used) or one of the IVR-related features (such as Debit Card) to define the number of allowable characters in a UID for the specified application and to pass that information to the specified application.

Table 11 lists TCL script names and the corresponding parameters that are required for each TCL scripts.

Table 11 *TCL Scripts and Parameters*

TCL Script Name	Description —Summary	Commands to Configure
clid_4digits_npw_3_cli.tcl	This script authenticates the account number and PIN respectively using ANI and null. The length of digits allowed for the account number and password are configurable through the CLI. If the authentication fails, it allows the caller to retry. The retry number is also configured through the CLI.	call application voice uid-len min = 1, max = 20, default = 10 call application voice pin-len min = 0, max = 10, default = 4 call application voice retry-count min = 1, max = 5, default = 3
clid_authen_col_npw_cli.tcl	This script authenticates the account number and PIN respectively using ANI and null. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	call application voice retry-count min = 1, max = 5, default = 3
clid_authen_collect_cli.tcl	This script authenticates the account number and PIN using ANI and DNIS. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	call application voice retry-count min = 1, max = 5, default = 3
clid_col_npw_3_cli.tcl	This script authenticates using ANI and null for account and PIN respectively. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI.	call application voice retry-count min = 1, max = 5, default = 3
clid_col_npw_npw_cli.tcl	This script authenticates using ANI and null for account and pin respectively. If authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected together.	call application voice retry-count min = 1, max = 5, default = 3

Table 11 TCL Scripts and Parameters (continued)

TCL Script Name	Description — Summary	Commands to Configure
clid_t37_fax_onramp.tcl	This script authenticates the account and PIN using the following: prompt-user, ANI, DNIS, gateway ID, redialer ID, and redialer DNIS.	None
clid_t37_fax_offramp.tcl	This script authenticates the account and PIN using the following: envelope-from, envelope-to, gateway ID, and x-account ID.	None
clid_t37_fax_rollover.tcl	This script is used for on-ramp T.38 fax rollover to T.37 fax when the destination fax line is busy. The script name is an interim name for Beta.	voice hunt user-busy

**Note**

The two TCL scripts, clid_t37_fax_onramp.tcl and clid_t37_fax_offramp.tcl, have interim names in beta release.

Examples

The following example shows how to configure 4 allowable characters in the UID for the application named prepaid:

```
Router(config)# call application voice prepaid uid-len 4
```

Related Commands

Command	Description
call application voice	Defines the name to be used for an application and indicates the location of the appropriate IVR script to be used with this application.
call application voice language	Defines the language of the audio file for the designated application and passes that information to the application.
call application voice load	Reload this designated TCL script.
call application voice pin-len	Defines the number of characters in the PIN for the application and passes that information to the application.
call application voice redirect-number	Defines the telephone number to which a call will be redirected—for example, the operator telephone number of the service provider—for the designated application.
call application voice retry-count	Defines the number of times a caller is permitted to reenter the PIN for a designated application and passes that information to the application.

Command	Description
call application voice set-location	Defines the location, language, and category of the audio files for the designated application and passes that information to the application.
call application voice warning-time	Defines the number of seconds a user is warned before their allowed calling time runs out for the designated application.

call application voice warning-time

To define the number of seconds a user is warned before the allowed calling time runs out, use the **call application voice warning-time** command in global configuration mode. To restore default values for this command, use the **no** form of this command.

call application voice *application-name* **warning-time** *number*

no call application voice *application-name* **warning-time** *number*

Syntax Description	
<i>application-name</i>	The name of the application to which the warning time parameter is being passed.
<i>number</i>	Defines the number of seconds the user is warned before the allowed calling time runs out. Valid entries are 10 to 600.

Defaults No default behavior or values.

Command Modes Global configuration

Command History	Release	Modification
	12.0(7)T	This command was introduced.

Usage Guidelines Use this command when configuring IVR (depending on the TCL script being used) or one of the IVR-related features (such as Debit Card) to define the number of seconds a user is warned before the allowed calling time runs out for the specified application and to pass that information to the specified application.

Table 12 lists TCL script names and the corresponding parameters that are required for each TCL scripts.

Table 12 *TCL Scripts and Parameters*

TCL Script Name	Description —Summary	Commands to Configure
clid_4digits_npw_3_cli.tcl	This script authenticates the account number and PIN respectively using ANI and null. The length of digits allowed for the account number and password are configurable through the CLI. If the authentication fails, it allows the caller to retry. The retry number is also configured through the CLI.	call application voice uid-len min = 1, max = 20, default = 10 call application voice pin-len min = 0, max = 10, default = 4 call application voice retry-count min = 1, max = 5, default = 3
clid_authen_col_npw_cli.tcl	This script authenticates the account number and PIN respectively using ANI and null. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	call application voice retry-count min = 1, max = 5, default = 3
clid_authen_collect_cli.tcl	This script authenticates the account number and PIN using ANI and DNIS. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected separately.	call application voice retry-count min = 1, max = 5, default = 3
clid_col_npw_3_cli.tcl	This script authenticates using ANI and null for account and PIN respectively. If the authentication fails, it allows the caller to retry. The retry number is configured through the CLI.	call application voice retry-count min = 1, max = 5, default = 3
clid_col_npw_npw_cli.tcl	This script authenticates using ANI and null for account and pin respectively. If authentication fails, it allows the caller to retry. The retry number is configured through the CLI. The account number and PIN are collected together.	call application voice retry-count min = 1, max = 5, default = 3

Table 12 TCL Scripts and Parameters (continued)

TCL Script Name	Description — Summary	Commands to Configure
clid_t37_fax_onramp.tcl	This script authenticates the account and PIN using the following: prompt-user, ANI, DNIS, gateway ID, redialer ID, and redialer DNIS.	None
clid_t37_fax_offramp.tcl	This script authenticates the account and PIN using the following: envelope-from, envelope-to, gateway ID, and x-account ID.	None
clid_t37_fax_rollover.tcl	This script is used for on-ramp T.38 fax rollover to T.37 fax when the destination fax line is busy. The script name is an interim name for Beta.	voice hunt user-busy

**Note**

The two TCL scripts, clid_t37_fax_onramp.tcl and clid_t37_fax_offramp.tcl, have interim names in beta release.

Examples

The following example shows how to configure a 30-second warning time for the application named prepaid:

```
Router(config)# call application voice prepaid warning-time 30
```

Related Commands

Command	Description
call application voice language	Defines the language of the audio file for the designated application and passes that information to the application.
call application voice load	Reload this designated TCL script.
call application voice location	Defines the name to be used for an application and indicates the location of the appropriate IVR script to be used with this application.
call application voice pin-len	Defines the number of characters in the PIN for the application and passes that information to the application.
call application voice redirect-number	Defines the telephone number to which a call will be redirected—for example, the operator telephone number of the service provider—for the designated application.
call application voice retry-count	Defines the number of times a caller is permitted to reenter the PIN for a designated application and passes that information to the application.

Command	Description
call application voice set-location	Defines the location, language, and category of the audio files for the designated application and passes that information to the application.
call application voice uid-len	Defines the number of characters in the UID for the designated application and passes that information to the application.

fax interface-type

To specify the interface type to be used for a fax call, use the **fax interface-type** command in global configuration mode. To return to the default fax protocol, use the **no** form of this command.

```
fax interface-type {modem | vfc}
```

```
no fax interface-type {modem | vfc}
```

Syntax Description	modem Use a modem card interface for fax calls.				
	vfc Use a Cisco voice feature card (VFC) for fax calls.				
Defaults	vfc—if no modem cards are present in the router				
	modem—if at least one modem card is present in the router				
Command Modes	Global configuration				
Command History	<table border="1"> <thead> <tr> <th data-bbox="380 966 714 1003">Release</th> <th data-bbox="714 966 1529 1003">Modification</th> </tr> </thead> <tbody> <tr> <td data-bbox="380 1003 714 1041">12.1(3)XI</td> <td data-bbox="714 1003 1529 1041">This command was introduced on the Cisco AS5300 access server.</td> </tr> </tbody> </table>	Release	Modification	12.1(3)XI	This command was introduced on the Cisco AS5300 access server.
Release	Modification				
12.1(3)XI	This command was introduced on the Cisco AS5300 access server.				
Usage Guidelines	If the Cisco AS5300 has only voice feature cards installed, the default interface type for fax calls is vfc . If the router has at least one modem card installed, the default interface type for fax calls is modem .				
	When using this command to change the interface type for fax calls, you must reload (reboot or reset) the router.				
Examples	The following example specifies the use of a VFC interface for fax calls:				
	<pre>Router(config)# fax interface-type vfc</pre>				
	<pre>Router(config)#</pre>				
Related Commands	None				

fax protocol (voice-service)

To specify the global default fax protocol to be used for all VoIP dial peers, use the **fax protocol** command in voice-service configuration mode. To return to the default fax protocol, use the **no** form of this command.

```
fax protocol { cisco | t38 [ls-redundancy value] [hs-redundancy value] }
```

```
no fax protocol
```

Syntax Description

cisco	Cisco proprietary fax protocol.
t38	ITU-T T.38 standard fax protocol.
ls-redundancy value	(Optional) Low-speed redundancy for the T.38 fax protocol. The <i>value</i> can be from 0 to 5. The default is 0 (no redundancy). The ls-redundancy parameter refers to data redundancy in the low-speed V.21-based T.30 fax machine protocol.
hs-redundancy value	(Optional) High-speed redundancy for the T.38 fax protocol. The <i>value</i> can be from 0 to 2. The default is 0 (no redundancy). The hs-redundancy parameter refers to data redundancy in the high-speed V.17, V.27, and V.29 T.4 or T.6 fax machine image data.

Defaults

cisco

Command Modes

Voice-service configuration

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco 2600 series routers, Cisco 3600 series routers, and Cisco MC3810 concentrators.
12.1(3)XI	This command was introduced on the Cisco AS5300 access server.

Usage Guidelines

Use the **fax protocol t38** command in voice-service configuration mode to configure T.38 fax relay for all VoIP dial peers. The **t38** keyword enables the T.38 standard fax relay protocol. The **cisco** keyword selects the original Cisco proprietary fax protocol. When the **system** keyword is selected in the dial-peer version of the **fax protocol** command, it specifies that the global default fax protocol will be used by that dial peer. The optional parameters **ls-redundancy** and **hs-redundancy** are used to send redundant T.38 fax packets when using the T.38 fax protocol.



Note The **ls-redundancy** and **hs-redundancy** parameters are applicable only to T.38 Fax Relay protocol.

The **ls-redundancy** parameter refers to data redundancy in the low-speed V.21-based T.30 fax machine protocol. For the **ls-redundancy** parameter, the *value* can be from 0 to 5. The default is 0 (no redundancy). The parameter *value* sets the redundancy factor for T.38 fax relay.

The **hs-redundancy** parameter refers to data redundancy in the high-speed V.17, V.27, and V.29 T.4 or T.6 fax machine image data. For the **hs-redundancy** parameter, the *value* can be from 0 to 2. The default is 0 (no redundancy). The parameter *value* sets the redundancy factor for T.38 fax relay.



Note Setting the **hs-redundancy** parameter greater than 0 will cause a significant increase in the network bandwidth consumed by the fax call.

Examples

The following example specifies T.38 fax protocol for all VoIP dial peers and sets low-speed redundancy to a factor of 2 and high-speed redundancy to a factor of 1:

```
Router(config)# voice service voip
Router(config-voice-service)# fax protocol t38 ls 2 hs 1
```

Related Commands

Command	Description
fax protocol (dial-peer)	Specifies the fax protocol for a specific VoIP dial peer.

fax protocol (dial-peer)

To specify the fax protocol to be used for a specific VoIP dial peer, use the **fax protocol** command in dial-peer configuration mode. To return to the global default fax protocol, use the **fax protocol system** command. To disable T.38 fax protocol for a specific dial peer, use the **no** form of this command.

```
fax protocol { cisco | t38 [ls-redundancy value] [hs-redundancy value] | system }
```

```
no fax protocol
```

Syntax Description		
cisco		Cisco proprietary fax protocol.
t38		ITU-T T.38 standard fax protocol.
ls-redundancy value		(Optional) Low-speed redundancy for the T.38 fax protocol. The <i>value</i> can be from 0 to 5. The default is 0 (no redundancy). The ls-redundancy parameter refers to data redundancy in the low-speed V.21-based T.30 fax machine protocol.
hs-redundancy value		(Optional) High-speed redundancy for the T.38 fax protocol. The <i>value</i> can be from 0 to 2. The default is 0 (no redundancy). The hs-redundancy parameter refers to data redundancy in the high-speed V.17, V.27, and V.29 T.4 or T.6 fax machine image data.
system		Specifies that the fax protocol for this dial peer will default to the global default fax protocol that has been set using the fax protocol (voice-service) command.

Defaults	
	system

Command Modes	
	Dial-peer configuration

Command History	Release	Modification
	12.1(3)T	This command was introduced on the Cisco 2600 series routers, Cisco 3600 series routers, and Cisco MC3810 concentrators.
	12.1(3)XI	This command was introduced on the Cisco AS5300 access server.

Usage Guidelines

Use the **fax protocol t38** command in dial-peer configuration mode to configure T.38 fax relay for a specific dial peer. The **t38** keyword enables the T.38 Fax Relay protocol. The **cisco** keyword selects the original Cisco proprietary fax protocol. When the **system** keyword is selected, it specifies that the global default fax protocol will be used by that dial peer. The optional parameters **ls-redundancy** and **hs-redundancy** are used to send redundant T.38 fax packets when using the T.38 fax protocol.



Note The **ls-redundancy** and **hs-redundancy** parameters are applicable only to T.38 fax relay protocol.

The **ls-redundancy** refers to data redundancy in the low-speed V.21-based T.30 fax machine protocol. For the **ls-redundancy**, the *value* can be from 0 to 5. The default is 0 (no redundancy). The parameter *value* sets the redundancy factor for T.38 fax relay.

The **hs-redundancy** refers to data redundancy in the high-speed V.17, V.27, and V.29 T.4 or T.6 fax machine image data. For the **hs-redundancy**, the *value* can be from 0 to 2. The default is 0 (no redundancy). The parameter *value* sets the redundancy factor for T.38 fax relay.

**Note**

Setting the **hs-redundancy** greater than 0 will cause a significant increase in the network bandwidth consumed by the fax call.

Examples

The following example specifies T.38 fax protocol for VoIP dial peer 99:

```
Router(config-if)# dial-peer voice 99 voip
Router(config-dial-peer)# fax protocol t38
```

Related Commands

Command	Description
fax protocol (voice-service)	Specifies the default fax protocol for all VoIP dial peers.

fax rate

To establish the rate at which a fax is sent to the specified dial peer, use the **fax rate** command in dial-peer configuration mode. To reset the dial peer for voice calls, use the **no** form of the command.

fax rate { **12000** | **14400** | **2400** | **4800** | **7200** | **9600** } [**disable** | **voice**] [**bytes** *bytes*]

no fax rate

Syntax Description		
	12000	Specifies a fax transmission speed of 12,000 bits per second (bps).
	14400	Specifies a fax transmission speed of 14,400 bps.
	2400	Specifies a fax transmission speed of 2400 bps.
	4800	Specifies a fax transmission speed of 4800 bps.
	7200	Specifies a fax transmission speed of 7200 bps.
	9600	Specifies a fax transmission speed of 9600 bps.
	disable	(Optional) Disables fax relay transmission capability.
	voice	(Optional) Specifies the highest possible transmission speed allowed by the voice rate. For example, if the voice codec is G.711, fax transmission may occur up to 14400 bps since 14400 bps is less than the 64k voice rate. If the voice codec is G.729 (8k), the fax transmission speed will be 7200 bps.
	bytes	(Optional) Selects the fax payload size.
	<i>bytes</i>	Number of bytes.

Defaults voice

Command Modes Dial-peer configuration

Command History	Release	Modification
	11.3(1)T	This command was introduced as fax-rate command.
	12.0(2)XH	The fax transmission rate of 12000 was added.
	12.0(4)T	This command was supported on the Cisco MC3810.
	12.1(3)T	The command name changed from fax-rate command to fax rate command (non-hyphenated).
	12.1(3)XI	This command was introduced on the Cisco AS5300 access server.

Usage Guidelines Use this command to specify the fax transmission rate to the specified dial peer.

The values for this command apply only to the fax transmission speed and do not affect the quality of the fax itself. The higher values provide a faster transmission speed but monopolize a significantly larger portion of the available bandwidth. Slower transmission speeds use less bandwidth.

If the fax rate transmission speed is set higher than the codec rate in the same dial peer, the data sent over the network for fax transmission will be above the bandwidth reserved for Resource Reservation Protocol (RSVP).

**Note**

Because a large portion of the available network bandwidth will be monopolized by the fax transmission, Cisco does not recommend setting the fax rate value higher than the value of the selected codec. If the fax rate value is set lower than the codec value, faxes will take longer to send but will use less bandwidth.

The **voice** keyword specifies the highest possible transmission speed allowed by the voice rate. For example, if the voice codec is G.711, the fax transmission may occur up to 14400 bps since 14400 bps is less than the 64k voice rate. If the voice codec is G.729 (8k), the fax transmission speed will be 7200 bps.

**Note**

If you need to turn off the fax on a dial peer, you can configure the fax rate to 0. This will disable the fax tone detection.

Examples

The following example shows a fax rate transmission speed of 9600 bps for faxes sent using dial peer 100:

```
Router(config)# dial-peer voice 100 voip
Router(config-dial-peer)# fax rate 9600
```

The following example sets a fax rate transmission speed of 12000 bps and the size of the fax-data frame at 20 bytes for dial peer 100:

```
Router(config)# dial-peer voice 100 voip
Router(config-dial-peer)# fax rate 12000 bytes 20
```

Related Commands

Command	Description
codec (dial-peer)	Specifies the voice coder rate of speech for a dial peer.
fax protocol (dial-peer)	Specifies the fax protocol for a specific VoIP dial peer.

voice hunt user-busy

To configure fax roll-over from T.38 (fax relay) to T.37 (store and forward fax), use the **voice hunt user-busy** command in global configuration mode. To return to the default settings, use the **no** form of this command.

voice hunt user-busy

no voice hunt user-busy

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

This command enables you to specify that, if your T.38 fax relay connection is busy, your fax call will roll over to T.37 store and forward fax connection. This command acts as a switch, either enabling or disabling the roll-over functionality.

To use this command, you need to make sure that there are specific values configured for the ingress VoIP dial peer for T.38 and the on-ramp MMoIP dial peer for T.37. The ingress VoIP dial peer must be configured to have higher preference than the on-ramp MMoIP dial peer. For example, if the preference for the ingress VoIP dial peer is configured as 2, the preference value of the on-ramp MMoIP dial peer must be 3 or greater.

Examples

The following example shows how to configure T.38 to T.37 roll over capabilities:

```
Router(config)# voice hunt user-busy
Router(config)#
```

voice service

To enter the voice-service configuration mode and specify the fax protocol to be used for fax applications, use the **voice service** global configuration command. To exit the voice-service configuration mode and return to global configuration mode, use the **exit** command.

voice service voip

Syntax Description	voip	Specifies Voice over IP parameters.
---------------------------	-------------	-------------------------------------

Defaults	No default behavior or values.
-----------------	--------------------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.1(1)XA	This command was introduced for VoATM on the Cisco MC3810 concentrators.
	12.1(2)T	This command was introduced on the T train for VoATM on the Cisco MC3810 concentrators.
	121(3)T	This command was implemented for VoIP on the Cisco 2600 series routers, Cisco 3600 series routers, and Cisco MC3810 concentrators.
	12.1(3)XI	This command was introduced on the Cisco AS5300 access server.

Usage Guidelines	Use the voice service command to switch to the voice-service configuration mode from the global configuration mode and to specify a voice encapsulation type. Use the exit command to exit the voice-service configuration mode and return to the global configuration mode.
-------------------------	--

Examples	The following example shows how to access the voice-service configuration mode and specify VoIP parameters, beginning in global configuration mode:
-----------------	---

```
Router(config)# voice service voip
Router(config-voice-service)#
```

Related Commands	Command	Description
	modem passthrough	Configures modem passthrough over VoIP.
	fax protocol	Specifies the global default fax protocol for all the VoIP dial peers.

Debug Commands

This section documents new or modified debug commands for the store and forward fax application using Cisco AS5300 VFCs. All other commands used with this feature are documented in the *Store and Forward Fax with ESMTF* document and in the Cisco IOS Release 12.0 command references.

- **debug dmosp doc-to-fax**
- **debug dmosp fax-to-doc**
- **debug fmosp receive**
- **debug fmosp send**
- **debug foip off-ramp**
- **debug foip on-ramp**
- **debug mspi receive**
- **debug mspi send**

debug dmsp doc-to-fax

To display debug messages for the doc Media Service Provider TIFF or text2Fax engine, use the **debug dmsp doc-to-fax** EXEC command. To disable the debug messages, use the **no** form of this command.

debug dmsp doc-to-fax [**text-to-fax** | **tiff-reader**]

no debug dmsp doc-to-fax [**text-to-fax** | **tiff-reader**]

Syntax Description

text-to-fax	Displays debug messages that occur while the DocMSP component is receiving text packets and producing T4 fax data.
tiff-reader	Displays debug messages that occur while the DocMSP component is receiving TIFF packets and producing T4 fax data.

Defaults

No default behavior or values.

Command History

Release	Modification
12.1(3)XI	This command was introduced on the Cisco AS5300 access server.

Examples

command example

Related Commands

Command	Description
debug dmsp fax-to-do c	Displays debug messages for the doc Media Service Provider fax-to-doc TIFF engine.

debug dmsp fax-to-doc

To display debug messages for doc MSP fax-to-doc, use the **debug dmsp fax-to-doc EXEC** command. To disable the debug messages, use the **no** form of this command.

debug dmsp fax-to-doc [tiff-writer]

no debug dmsp fax-to-doc [tiff-writer]

Syntax Description

tiff-writer	Displays debug messages that occur while the DocMSP component is receiving T4 fax data and producing TIFF packets.
--------------------	--

Defaults

No default behavior or values.

Command History

Release	Modification
12.1(3)XI	This command was introduced on the Cisco AS5300 access server.

Examples

command example

Related Commands

Command	Description
debug dmsp doc-to-fax	Displays debug messages for the doc Media Service Provider TIFF or text2Fax engine.

debug fmsp receive

To display debug messages for FMSP receive, use the **debug fmsp receive EXEC** command. To disable the debug messages, use the **no** form of this command.

debug fmsp receive [t30 | t38]

no debug fmsp receive [t30 | t38]

Syntax Description	Field	Description
	t30	Specifies T.30 fax protocol.
	t38	Specifies T.38 fax protocol.

Defaults No default behavior or values.

Command History	Release	Modification
	12.1(3)XI	This command was introduced on the Cisco AS5300 access server.

Examples

command example

Related Commands	Command	Description
	debug fmsp send	Displays debug messages for FMSP send.

debug fmosp send

To display debug messages for FMSP send, use the **debug fmosp send EXEC** command. To disable the debug messages, use the **no** form of this command.

```
debug fmosp send [t30 | t38]
```

```
no debug fmosp send [t30 | t38]
```

Syntax Description

t30	Specifies T.30 fax protocol.
t38	Specifies T.38 fax protocol.

Defaults

No default behavior or values.

Command History

Release	Modification
12.1(3)XI	This command was introduced on the Cisco AS5300 access server.

Examples

```
command example
```

Related Commands

Command	Description
debug fmosp receive	Displays debug messages for FMSP receive.

debug foip off-ramp

To display debug messages for off-ramp faxmail, use the **debug foip off-ramp** EXEC command. To disable the debug messages, use the **no** form of this command.

debug foip off-ramp

no debug foip off-ramp

Syntax Description

There are no arguments or keywords for this command.

Defaults

No default behavior or values.

Command History

Release	Modification
12.1(3)XI	This command was introduced on the Cisco AS5300 access server.

Examples

command example

Related Commands

Command	Description
debug foip on-ramp	Displays debug messages for on-ramp faxmail.

debug foip on-ramp

To display debug messages for on-ramp faxmail, use the **debug foip on-ramp** EXEC command. To disable the debug messages, use the **no** form of this command.

debug foip on-ramp

no debug foip on-ramp

Syntax Description

There are no arguments or keywords for this command.

Defaults

No default behavior or values.

Command History

Release	Modification
12.1(3)XI	This command was introduced on the Cisco AS5300 access server.

Examples

command example

Related Commands

Command	Description
debug foip off-ramp	Displays debug messages for off-ramp faxmail.

debug mspi receive

To display debug messages for mail Service Provider Interface receive, use the **debug mspi receive EXEC** command. To disable the debug messages, use the **no** form of this command.

debug mspi receive

no debug mspi receive

Syntax Description

There are no arguments or keywords for this command.

Defaults

No default behavior or values.

Command History

Release	Modification
12.1(3)XI	This command was introduced on the Cisco AS5300 access server.

Examples

command example

Related Commands

Command	Description
debug mspi send	Displays debug messages for mail SPI send.

debug mspi send

To display debug messages for mail Service Provider Interface send, use the **debug mspi send EXEC** command. To disable the debug messages, use the **no** form of this command.

debug mspi send

no debug mspi send

Syntax Description

There are no arguments or keywords for this command.

Defaults

No default behavior or values.

Command History

Release	Modification
12.1(3)XI	This command was introduced on the Cisco AS5300 access server.

Examples

```
command example
```

Related Commands

Command	Description
debug mspi receive	Displays debug messages for mail SPI receive.