Voice Port Configuration Overview

Last Updated: December 14, 2011

Voice ports are found at the intersections of packet-based networks and traditional telephony networks, and they facilitate the passing of voice and call signals between the two networks. Physically, voice ports connect a router or access server to a line from a circuit-switched telephony device in a PBX or the PSTN. Basic software configuration for voice ports describes the type of connection being made and the type of signaling to take place over this connection. In addition to the commands for basic configuration, there are also commands that provide fine-tuning for voice quality, enable special features, and specify parameters to match those of proprietary PBXs.

Not all voice-port commands are covered in this document. Some are described in the Cisco IOS ISDN Voice Configuration Guide, Release 12.4 or the “Trunk Management Features” document, Cisco IOS Voice Configuration Library, Release 12.4. The voice-port configuration commands included in this document are fully documented in the Cisco IOS Voice Command Reference.

• Finding Feature Information, page 1
• Voice Port Configuration Overview, page 1

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Voice Port Configuration Overview

Voice ports on routers and access servers emulate physical telephony switch connections so that voice calls and their associated signaling can be transferred intact between a packet network and a circuit-switched network or device. For a voice call to occur, certain information must be passed between the telephony devices at either end of the call, such as the devices’ on-hook status, the line’s availability, and whether an incoming call is trying to reach a device. This information is referred to as signaling, and to process it...
properly, the devices at both ends of the call segment (that is, those directly connected to each other) must use the same type of signaling.

The devices in the packet network must be configured to convey signaling information in a way that the circuit-switched network can understand. They must also be able to understand signaling information received from the circuit-switched network. This is accomplished by installing appropriate voice hardware in the router or access server and by configuring the voice ports that connect to telephony devices or the circuit-switched network.

The following illustrations show examples of how voice ports are used.

- The "Telephone to WAN" figure shows one voice port connecting a telephone to the WAN through the router.
- The "Telephone to PSTN" figure shows one voice port connected to the PSTN and another to a telephone; the router acts like a small PBX.
- The "PBX-to-PBX over a WAN" figure shows how two PBXs can be connected over a WAN to provide toll bypass.

Cisco provides a variety of Cisco IOS commands for flexibility in configuring voice ports to match the physical attributes of the voice connections that are being made. Some of these connections are made using analog means of transmission, while others use digital transmission. The table below shows the analog and digital voice-port connection support of the router platforms discussed in this document.
Table 1  Analog and Digital Voice-Port Support on Cisco Platforms

<table>
<thead>
<tr>
<th>Platform</th>
<th>Analog</th>
<th>Digital</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco 880 series (includes IAD881B, IAD881F, C881SRST, IAD888B, IAD888F, and C888SRST)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco 1750</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Cisco 2600 series</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco 3600 series</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco 3700 series</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco 7200 series</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco 7500 series</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco AS5300</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco AS5350</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco AS5400</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco AS5800</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco AS5850</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco MC3810</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

- Telephony Signaling Interfaces, page 3

Telephony Signaling Interfaces

Voice ports on routers and access servers physically connect the router or access server to telephony devices such as telephones, fax machines, PBXs, and PSTN central office (CO) switches. These devices may use any of several types of signaling interfaces to generate information about on-hook status, ringing, and line seizure.

The router’s voice-port hardware and software need to be configured to transmit and receive the same type of signaling being used by the device with which they are interfacing so that calls can be exchanged smoothly between the packet network and the circuit-switched network.

The signaling interfaces discussed in this document include foreign exchange office (FXO), foreign exchange station (FXS), and receive and transmit (E&M), which are types of analog interfaces. Some digital connections emulate FXO, FXS, and E&M interfaces, and they are discussed in "FXS and FXO Interfaces" and the Telephony Signaling Interfaces, page 3. It is important to know which signaling method the telephony side of the connection is using, and to match the router configuration and voice interface hardware to that signaling method.

The next three illustrations show how the different signaling interfaces are associated with different uses of voice ports. In the "FXS Signaling Interfaces" figure, FXS signaling is used for end-user telephony equipment, such as a telephone or fax machine. The "FXS and FXO Signaling Interfaces" figure shows an
FXS connection to a telephone and an FXO connection to the PSTN at the far side of a WAN; this might be a telephone at a local office going over a WAN to a router at headquarters that connects to the PSTN. In the "E&M Signaling Interfaces" figure, two PBXs are connected across a WAN by E&M interfaces. This illustrates the path over a WAN between two geographically separated offices in the same company.

**Figure 4**  
**FXS Signaling Interfaces**

![FXS Signaling Interfaces](image)

**Figure 5**  
**FXS and FXO Signaling Interfaces**

![FXS and FXO Signaling Interfaces](image)

**Figure 6**  
**E and M Signaling Interfaces**

![E and M Signaling Interfaces](image)

- FXS and FXO Interfaces, page 4
- E and M Interfaces, page 5
- Toll Fraud Prevention, page 6

**FXS and FXO Interfaces**

An FXS interface connects the router or access server to end-user equipment such as telephones, fax machines, or modems. The FXS interface supplies ring, voltage, and dial tone to the station and includes an RJ-11 connector for basic telephone equipment, keysets, and PBXs.

An FXO interface is used for trunk, or tie line, connections to a PSTN CO or to a PBX that does not support E&M signaling (when local telecommunications authority permits). This interface is of value for off-premise station applications. A standard RJ-11 modular telephone cable connects the FXO voice interface card to the PSTN or PBX through a telephone wall outlet.

FXO and FXS interfaces indicate on-hook or off-hook status and the seizure of telephone lines by one of two access signaling methods: loop-start or ground-start. The type of access signaling is determined by the
type of service from the CO; standard home telephone lines use loop-start, but business telephones can order ground-start lines instead.

Loop-start is the more common of the access signaling techniques. When a handset is picked up (the telephone goes off-hook), this action closes the circuit that draws current from the telephone company CO and indicates a change in status, which signals the CO to provide dial tone. An incoming call is signaled from the CO to the handset by sending a signal in a standard on/off pattern, which causes the telephone to ring.

Loop-start has two disadvantages, however, that usually are not a problem on residential telephones but that become significant with the higher call volume experienced on business telephones. Loop-start signaling has no means of preventing two sides from seizing the same line simultaneously, a condition known as glare. Also, loop-start signaling does not provide switch-side disconnect supervision for FXO calls. The telephony switch (the connection in the PSTN, another PBX, or key system) expects the router’s FXO interface, which looks like a telephone to the switch, to hang up the calls it receives through its FXO port. However, this function is not built into the router for received calls; it operates only for calls originating from the FXO port.

Another access signaling method used by FXO and FXS interfaces to indicate on-hook or off-hook status to the CO is ground-start signaling. It works by using ground and current detectors that allow the network to indicate off-hook or seizure of an incoming call independent of the ringing signal and allow for positive recognition of connects and disconnects. For this reason, ground-start signaling is typically used on trunk lines between PBXs and in businesses where call volume on loop-start lines can result in glare. See the "Configuring Disconnect Supervision" and "Configuring FXO Supervisory Disconnect Tones" sections in the "Fine-Tuning Analog and Digital Voice Ports" chapter for voice port commands that configure additional recognition of disconnect signaling.

In most cases, the default voice port command values are sufficient to configure FXO and FXS voice ports.

**E and M Interfaces**

Trunk circuits connect telephone switches to one another; they do not connect end-user equipment to the network. The most common form of analog trunk circuit is the E&M interface, which uses special signaling paths that are separate from the trunk’s audio path to convey information about the calls. The signaling paths are known as the E-lead and the M-lead. The name E&M is thought to derive from the phrase Ear and Mouth or rEceive and transMit although it could also come from Earth and Magnet. The history of these names dates back to the days of telegraphy, when the CO side had a key that grounded the E circuit, and the other side had a sounder with an electromagnet attached to a battery. Descriptions such as Ear and Mouth were adopted to help field personnel determine the direction of a signal in a wire. E&M connections from routers to telephone switches or to PBXs are preferable to FXS/FXO connections because E&M provides better answer and disconnect supervision.

Like a serial port, an E&M interface has a data terminal equipment/data communications equipment (DTE/ DCE) type of reference. In telecommunications, the trunking side is similar to the DCE, and is usually associated with CO functionality. The router acts as this side of the interface. The other side is referred to as the signaling side, like a DTE, and is usually a device such as a PBX. Five distinct physical configurations for the signaling part of the interface (Types I-V) use different methods to signal on-hook/off-hook status, as shown in the table below. Cisco voice implementation supports E&M Types I, II, III, and V.
### Table 2  EandM Wiring and Signaling Methods

<table>
<thead>
<tr>
<th>E&amp;M Type</th>
<th>E-Lead Configuration</th>
<th>M-Lead Configuration</th>
<th>Signal Battery Lead Configuration</th>
<th>Signal Ground Lead Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>Output, relay to ground</td>
<td>Input, referenced to ground</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>II</td>
<td>Output, relay to SG</td>
<td>Input, referenced to ground</td>
<td>Feed for M, connected to -48V</td>
<td>Return for E, galvanically isolated from ground</td>
</tr>
<tr>
<td>III</td>
<td>Output, relay to ground</td>
<td>Input, referenced to ground</td>
<td>Connected to -48V</td>
<td>Connected to ground</td>
</tr>
<tr>
<td>V</td>
<td>Output, relay to ground</td>
<td>Input, referenced to -48V</td>
<td>--</td>
<td>--</td>
</tr>
</tbody>
</table>

The physical E&M interface is an RJ-48 connector that connects to PBX trunk lines, which are classified as either two-wire or four-wire. This refers to whether the audio path is full duplex on one pair of wires (two-wire) or on two pair of wires (four-wire). A connection may be called a four-wire E&M circuit although it actually has six to eight physical wires. It is an analog connection although an analog E&M circuit may be emulated on a digital line. For more information on digital voice port configuration of E&M signaling, see the "DS0 Groups on Digital T1/E1 Voice Ports" section in the "Configuring Digital Voice Ports" chapter.

PBXs built by different manufacturers can indicate on-hook/off-hook status and telephone line seizure on the E&M interface by using any of the following three types of access signaling:

- **Immediate-start** is the simplest method of E&M access signaling. The calling side seizes the line by going off-hook on its E-lead and sends address information as dual-tone multifrequency (DTMF) digits (or as dialed pulses on Cisco 2600 and Cisco 3600 series routers) following a short, fixed-length pause.

- **Wink-start** is the most commonly used method for E&M access signaling, and is the default for E&M voice ports. Wink-start was developed to minimize glare, a condition found in immediate-start E&M, in which both ends attempt to seize a trunk at the same time. In wink-start, the calling side seizes the line by going off-hook on its E-lead, then waits for a short temporary off-hook pulse, or "wink," from the other end on its M-lead before sending address information. The switch interprets the pulse as an indication to proceed and then sends the dialed digits as DTMF or dialed pulses.

- **In delay-dial signaling**, the calling station seizes the line by going off-hook on its E-lead. After a timed interval, the calling side looks at the status of the called side. If the called side is on-hook, the calling side starts sending information as DTMF digits; otherwise, the calling side waits until the called side goes on-hook and then starts sending address information.

---

**Toll Fraud Prevention**

When a Cisco router platform is installed with a voice-capable Cisco IOS software image, appropriate features must be enabled on the platform to prevent potential toll fraud exploitation by unauthorized users. Deploy these features on all Cisco router Unified Communications applications that process voice calls, such as Cisco Unified Communications Manager Express (CME), Cisco Survivable Remote Site Telephony (SRST), Cisco Unified Border Element (UBE), Cisco IOS-based router and standalone analog and digital PBX and public-switched telephone network (PSTN) gateways, and Cisco contact-center VoiceXML gateways. These features include, but are not limited to, the following:
• Disable secondary dial tone on voice ports--By default, secondary dial tone is presented on voice ports on Cisco router gateways. Use private line automatic ringdown (PLAR) for foreign exchange office (FXO) ports and direct-inward-dial (DID) for T1/E1 ports to prevent secondary dial tone from being presented to inbound callers.

• Cisco router access control lists (ACLs)--Define ACLs to allow only explicitly valid sources of calls to the router or gateway, and therefore to prevent unauthorized Session Initiation Protocol (SIP) or H.323 calls from unknown parties to be processed and connected by the router or gateway.

• Close unused SIP and H.323 ports--If either the SIP or H.323 protocol is not used in your deployment, close the associated protocol ports. If a Cisco voice gateway has dial peers configured to route calls outbound to the PSTN using either time division multiplex (TDM) trunks or IP, close the unused H.323 or SIP ports so that calls from unauthorized endpoints cannot connect calls. If the protocols are used and the ports must remain open, use ACLs to limit access to legitimate sources.

• Change SIP port 5060--If SIP is actively used, consider changing the port to something other than well-known port 5060.

• SIP registration--If SIP registration is available on SIP trunks, turn on this feature because it provides an extra level of authentication and validation that only legitimate sources can connect calls. If it is not available, ensure that the appropriate ACLs are in place.

• SIP Digest Authentication--If the SIP Digest Authentication feature is available for either registrations or invites, turn this feature on because it provides an extra level of authentication and validation that only legitimate sources can connect calls.

• Explicit incoming and outgoing dial peers--Use explicit dial peers to control the types and parameters of calls allowed by the router, especially in IP-to-IP connections used on CME, SRST, and Cisco UBE. Incoming dial peers offer additional control on the sources of calls, and outgoing dial peers on the destinations. Incoming dial peers are always used for calls. If a dial peer is not explicitly defined, the implicit dial peer 0 is used to allow all calls.

• Explicit destination patterns--Use dial peers with more granularity than .T for destination patterns to block disallowed off-net call destinations. Use class of restriction (COR) on dial peers with specific destination patterns to allow even more granular control of calls to different destinations on the PSTN.

• Translation rules--Use translation rules to manipulate dialed digits before calls connect to the PSTN to provide better control over who may dial PSTN destinations. Legitimate users dial an access code and an augmented number for PSTN for certain PSTN (for example, international) locations.

• Tcl and VoiceXML scripts--Attach a Tcl/VoiceXML script to dial peers to do database lookups or additional off-router authorization checks to allow or deny call flows based on origination or destination numbers. Tcl/VoiceXML scripts can also be used to add a prefix to inbound DID calls. If the prefix plus DID matches internal extensions, then the call is completed. Otherwise, a prompt can be played to the caller that an invalid number has been dialed.

• Host name validation--Use the "permit hostname" feature to validate initial SIP Invites that contain a fully qualified domain name (FQDN) host name in the Request Uniform Resource Identifier (Request URI) against a configured list of legitimate source hostnames.

• Dynamic Domain Name Service (DNS)--If you are using DNS as the "session target" on dial peers, the actual IP address destination of call connections can vary from one call to the next. Use voice source groups and ACLs to restrict the valid address ranges expected in DNS responses (which are used subsequently for call setup destinations).

For more configuration guidance, see the "Cisco IOS Unified Communications Toll Fraud Prevention" paper.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks.