Cisco Unified Border Element Enterprise Protocol-Independent Features and Setup

This Cisco Unified Border Element (Enterprise) is a special Cisco IOS XE software image that runs on Cisco ASR1000. It provides a network-to-network interface point for billing, security, call admission control, quality of service, and signaling interworking. This chapter describes basic gateway functionality, software images, topology, and summarizes supported features.

Note Cisco Product Authorization Key (PAK)--A Product Authorization Key (PAK) is required to configure some of the features described in this guide. Before you start the configuration process, please register your products and activate your PAK at the following URL http://www.cisco.com/go/license .

Finding Feature Information

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

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.

Cisco Unified Border Element Enterprise Protocol-Independent Features and Setup

This chapter contains the following configuration topics:

Cisco Unified Border Element Enterprise Protocol-Independent Features and Setup

Cisco UBE (Enterprise) Prerequisites and Restrictions

Dial Plan Management

- Dial Peer Configuration on Voice Gateway Routers — http://www.cisco.com/en/US/docs/ios-xml/ios/voice/dialpeer/configuration/15-1mt/vd-15-1mt-book.html
- Translation Rules — http://www.cisco.com/en/US/docs/ios-xml/ios/voice/vcr5/vcr-t3.html#GUID-62D8FEDA-D685-40FB-A70D-1794E8150036
- ENUM support
- Configuring Tool Command Language (Tcl) — http://www.cisco.com/en/US/products/sw/voicesw/ps2192/products_programming_reference_guides_list.html
- Cisco Service Advertisement Framework (SAF) — http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps10587/ps10591/ps10621/product_bulletin_c25-561938.html#wp9000293

Configuring Call Admissions Control

- VoIP Call Admissions Control — http://www.cisco.com/en/US/docs/ios/solutions_docs/voip_solutions/CAC.html

Resource Reservation Protocol (RSVP)

- Interworking Between RSVP Capable and RSVP Incapable Networks
- Cisco Resource Reservation Protocol Agent

Dual-Tone Multifrequency (DTMF) Support and Interworking

- SIP--INFO Method for DTMF Tone Generation
- DTMF Events through SIP Signaling
- Configuring SIP DTMF Features — http://www.cisco.com/en/US/docs/ios-xml/ios/voice/sip/configuration/15-1mt/Configuring_SIP_DTMF_Features.html
- H.323 RFC2833 - SIP NOTIFY

Codec Negotiation

- Negotiation of an Audio Codec from a List of Codecs on Each Leg of a SIP-to-SIP Call on the Cisco Unified Border Element

Transcoding

- iLBC Support for SIP and H.323
- Negotiation of an Audio Codec From a List of Codecs on Each Leg of a SIP-to-SIP Call on the Cisco UBE

Cisco Unified Border Element Enterprise Protocol-Independent Features and Setup

Payload Type Interoperability

- Interworking Between RSVP Capable and RSVP Incapable Networks
- Modem Pass Through Capability for Individual Dial Peers — http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/dial_peer/dp_confg.html#wp1068501
- Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls

Transrating

- DSP Based Functionality on the Cisco UBE (Enterprise) Including Transcoding and Transrating

Voice Quality Controls

- QoS Marking Settings on dial-peers — http://www.cisco.com/en/US/docs/ios-xml/ios/voice/vcr2/vcr-i1.html#GUID-2FC584E4-49EB-455F-BA0B-B1EB68515CCF

Fax/modem Support

- Modem passthrough
- T.38 Fax Relay — http://www.cisco.com/en/US/docs/ios-xml/ios/voice/fax/configuration/15-1mt/vf-cfg-t38-fxrly.html
- Cisco Fax Relay — http://www.cisco.com/en/US/docs/ios-xml/ios/voice/fax/configuration/15-1mt/vf-cfg-fx-relay.html

H.323 Video

- Cisco Unified Border Element Videoconferencing

SIP Video

- SIP Video Calls with Flow Around Media
- RTP Media Loopback for SIP Calls
- Configuring RTP Media Loopback for SIP Calls

Telepresence

- SIP Video Support for Telepresence Calls

Security Features

- Toll Fraud Prevention
- Access lists (ACLs)
- CAC (call spike) — http://www.cisco.com/en/US/docs/ios-xml/ios/voice/vcr1/vcr-c3.html#GUID-ED81C161-885D-4BEC-A6A0-D4C9886AEA2F
- SIP--Ability to Send a SIP Registration Message on a Border Element

- SIP Parameter Modification
- SIP--SIP Stack Portability
- Session Refresh with Reinvites
- CDR
- Transport Layer Security (TLS)
- Interworking of Secure RTP calls for SIP and H.323
- SIP SRTP Fallback to Nonsecure RTP
- VRF aware H.323 and SIP

IPv4 and IPv6 Interworking

- VoIP for IPv6

RSVP Interworking

- Interworking Between RSVP Capable and RSVP Incapable Networks

Collocated Services

- Software Media Termination Point
- Cisco Unified Communication Trusted Firewall Control
- Cisco Unified Communication Trusted Firewall Control-Version II
- Cisco Unified Border Element with Gatekeeper — http://www.cisco.com/en/US/docs/ios/voice/cubegk/configuration/guide/ve_book/ve_book.html

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.