



IPv6 Support

Cisco Unified Border Element (SP Edition) supports IPv6 addressing on the unified model for SIP signaling and media. Cisco Unified Border Element (SP Edition) has the ability to handle IPv4 to IPv6 SIP signaling and media interworking, as well as IPv6 to IPv6 SIP signaling and media (RTP) interworking.

Cisco Unified Border Element (SP Edition) was formerly known as Integrated Session Border Controller and may be commonly referred to in this document as the session border controller (SBC).

For a complete description of the commands used in this chapter, refer to the *Cisco Unified Border Element (SP Edition) Command Reference: Unified Model* at:

http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbcu_book.html.

For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or a Cisco IOS master commands list.

Feature History for IPv6 Support

Release	Modification
Cisco IOS XE Release 2.6	IPv6 Support features were introduced on the Cisco ASR 1000 Series Router.
Cisco IOS XE Release 3.1S	IPv6 Support for VRF was added on the Cisco ASR 1000 Series Router.

Contents

This module contains the following sections:

- [Prerequisites, page 54-2](#)
- [Restrictions, page 54-2](#)
- [Information About IPv6 Support, page 54-2](#)
- [Configuring IPv6, page 54-5](#)

Prerequisites

The following prerequisite is required to implement IPv6 Support:

Before implementing IPv6 Support, Cisco Unified Border Element (SP Edition) must already be configured.

Restrictions

The following are restrictions for IPv6 support on the Cisco Unified Border Element (SP Edition):

- H.323 over IPv6 is not supported.
- H.248 over IPv6 is not supported.
- The SBC does not support receiving and sending multiple IP addresses per media stream.

For more information, refer to RFC 4091, The Alternative Network Address Types (ANAT) Semantics for the Session Description Protocol (SDP) Grouping Framework and ICE (Interactive Connectivity Establishment).

- DNS look up over IPv6 is not supported.
- RADIUS (accounting and authentication) over IPv6 is not supported.

Information About IPv6 Support

In Cisco IOS XE Release 2.6, Cisco Unified Border Element (SP Edition) supports IPv6 addressing on the unified model for SIP signaling and media in the following ways:

- IPv4 to IPv6 SIP signaling interworking
- IPv4 to IPv6 media interworking
- IPv6 to IPv6 SIP signaling
- IPv6 to IPv6 media RTP interworking
- AAAA DNS query support

IPv6 to IPv6 RTP interworking on the media plane have been supported on the distributed model. The unified model now can enable IPv6 to IPv6 SIP signaling calls and IPv4 to IPv6 SIP signaling and media interworking calls.

The default behavior is that SBC assumes that the media address type to be used must match the signaling address type configured on the adjacency. Thus the default behavior which can be overridden by configuring a Call Admission Control (CAC) policy is for the media (RTP) to use the same version as used by signaling (SIP). The IP version used by SIP is dictated by the IP addresses configured on the adjacency. For example, if the incoming SIP INVITE comes in on an IPv4 adjacency and is routed out via an IPv6 adjacency, the incoming RTP will come over IPv4 and will be sent out over IPv4

IPv6 support for SIP calls affects the following SBC functions and existing unified SBC features:

- SIP URIs—IPv6 addresses are parsed in SIP URIs.
- Interworking IPv4 and IPv6 Adjacencies:
 - IPv6 addresses are passed through without modification in the Contact Username Passthrough feature.

- SBC supports IP/fully-qualified domain name (FQDN) entries for IPv6 adjacencies



Note An adjacency can be configured for either IPv4 or IPv6 addresses only. Combinations of IPv4 and IPv6 addresses on the same adjacency are not supported.



Note An adjacency configured for IPv4 cannot be changed to IPv6 and vice-versa, without deleting and recreating the adjacency. If the adjacency is referred to in the routing or CAC tables, these references must be removed before unconfiguring the adjacency.

- TLS over IPv6—Handles IPv6 addresses for adjacencies configured for SIP over Transport Layer Security (TLS) encryption.
- Access Authentication for SIP over IPv6

Supports IPv6 adjacencies for SIP inbound authentication to challenge inbound SIP requests.

For an incoming call over an IPv6 adjacency if the adjacency is configured for access authentication or inbound authentication, the call is challenged with a nonce (similar to what occurs in IPv4 addressing). The subsequent REGISTER message must have authentication parameters that should result in a RADIUS Access Request or an Access Accept (or reject) message. Note that the communication with the RADIUS server occurs over IPv4.

- Billing for IPv4 and IPv6 Calls

Packetcable billing records do not have IP addresses embedded in them. Therefore, billing for IPv6 calls work in the same manner as for IPv4 calls and no additional configuration is needed in billing and RADIUS configuration.

However only IPv4 addressing is supported for communicating with the RADIUS server. Both authentication and accounting requests go over IPv4, even when the requests are coming over an IPv6 adjacency. The control address used as source address in RADIUS requests is IPv4 only.

The billing manager local address goes in the NAS IP address field of RADIUS requests. This address is also an IPv4 address.

- SRTP Passthrough mode—No additional configuration changes for IPv6 addressing.
- Media bypass in Call Admission Control—The SBC must not attempt to perform media bypass between endpoints with different IP versions, even if media bypass CAC policy permits it.
- Blacklist Support—Supports the configuration of blacklist entries with IPv6 addresses or prefixes in the same way as IPv4 addresses.
- Logging—Displays IPv6 and IPv4 addresses.
- Late-to-Early Media Interworking—Supports calls terminating and originating from an IPv6 adjacency.
- Softswitch Shielding—Supports IPv6 endpoints registering with a softswitch.
- Call Hold—Supports IPv4 to IPv6 call interworking.

Using “c=0.0.0.0” as specified in RFC 2543 to indicate call hold is not valid with IPv6 addresses, and you must use “a=sendonly/inactive” to indicate a call hold.

- ToS/DSCP Marking for Signaling Messages—Supports DSCP marking for outgoing IPv4 and IPv6 signaling packets.

- SIP Header Manipulation—Supports the passthrough header TO and FROM functionality for IPv6 to IPv4 interworked calls by passing the headername unchanged for incoming calls.
SBC rewrites the CONTACT header for outgoing calls.
- DTMF Interworking—Supports IPv6 adjacencies.
- IP Realms—Supports IPv6 adjacencies. IP addresses are assigned based on the realm configured on the IPv6 or IPv4 adjacency.
- SIP Instant Messaging—Supports IPv4 to IPv6 interworked calls.
- SIP IP-FQDN URI Translation—Supports IP-FQDN entries for IPv6 adjacencies.
- Domain Name Lookup (DNS)—Supports name lookup for IPv6 addresses and supports both A and AAAA DNS queries. DNS lookup happens over IPv4.
- Fast Registration—Supports IPv6 addresses.
- High Availability—IPv4 to IPv6 and IPv6 to IPv6 calls behave the same as IPv4 to IPv4 calls during failover.
Calls over UDP are replicated. For calls made over TCP, the signaling state is not replicated and will generate a TCP reset on receiving any SIP message after switchover.
- Media Hair-pinning—Supports IPv6 to IPv6 call hair pinning in the same manner as IPv4 to IPv4 calls. With media hair-pinning, calls come in and go back out on the same adjacency.

**Note**

IPv4 to IPv6 hair-pinning is not supported because an adjacency can only be an IPv4 adjacency or an IPv6 adjacency.

- 3xx Redirect Messages—Supports redirection from IPv4 to IPv6 and from IPv6 to IPv4.
3xx represents a class of SIP response codes used in SIP to indicate that the sender of the request should try the request to an alternate URI or URIs that are presented in the 3xx response. Some of the widely-used response code examples are 301 “Moved Temporarily” or 302 “Moved Permanently.”

Performing ISSU for IPv6 Calls

When performing ISSU to upgrade to a higher version Cisco IOS XE release, IPv4 to IPv4 calls migrate successfully to the higher version.

Before performing ISSU to migrate to a lower version release, you must first unconfigure all IPv6 adjacencies and remove all active IPv6 call states. You can clear calls through IPv6 adjacencies with the **no attach force abort** command. This command executes a forced detach, tearing down calls without signaling their end.

When performing ISSU to downgrade to a lower version Cisco IOS XE release, for example from Cisco IOS XE Release 2.6 to 2.5, if there is any IPv6 configuration or any active calls through an IPv6 adjacency, an error message is reported. If the user continues with the ISSU, the system will reach stateful switchover (SSO) without the SBC configuration being available on the standby processor. Before performing a downgrade, unconfigure all IPv6 configuration and dynamic state (for example, IPv6 to IPv6 and IPv6 to IPv4 calls, as well as IPv6 blacklists).

Configuring IPv6

To configure Cisco Unified Border Element (SP Edition) for IPv6 to IPv6 calls or IPv4 to IPv6 interworked calls, configure the local and remote addresses on the adjacency with IPv6 addresses.

If you have a peer or another SBC in your network that supports both IPv4 and IPv6 addresses, then you should define two adjacencies on the local SBC, one adjacency with IPv4 addresses and a second adjacency with IPv6 addresses.

Configuration Examples

The following example shows the asrl SBC configured with IPv6 and IPv4 signaling and remote addresses on several SIP adjacencies and the 1 call policy set using a round-robin routing rule to implement call routing:



Note

The **caller** and **callee** commands have been used in this procedure. In some scenarios, the **branch** command can be used as an alternative to the **caller** and **callee** command pair. The **branch** command has been introduced in Release 3.5.0. See the [“Configuring Directed Nonlimiting CAC Policies”](#) section on page 7-37 for information about this command.

```
!
!
sbc asrl
sbe
control address aaa ipv4 33.33.36.1
radius authentication
radius accounting server1
server server1
address ipv4 10.0.120.19
key cisco
activate
sip header-profile ccmpf1
header Allow entry 1
action pass
header Call-Info entry 1
action pass
sip method-profile 1
pass-body
method MESSAGE
action pass
sip method-profile method1
pass-body
method INFO
action pass
sip method-profile cmmethod1
pass-body
method SUBSCRIBER
action pass
sip method-profile cmmethod2
pass-body
method INFO
action pass
method NOTIFY
action pass
method SUBSCRIBER
action pass
adjacency sip UEV6
```

```
group IPv6
inherit profile preset-p-cscf-access
visited network identifier open-ims.test
local-id host pcscf.open-ims.test
signaling-address ipv6 2001:A401::33:33:36:1
statistics method summary
signaling-port 4060
remote-address ipv6 2001::/64
signaling-peer 2001::10:0:120:19
dbe-location-id 0
attach
adjacency sip CCM134
force-signaling-peer
group v4
nat force-on
header-profile inbound ccmpf1
header-profile outbound ccmpf1
method-profile inbound ccmmethod2
method-profile outbound ccmmethod2
preferred-transport udp
signaling-address ipv4 33.33.36.1
statistics method summary
signaling-port 5060
remote-address ipv4 10.0.50.134 255.255.255.255
signaling-peer 10.0.50.134
dbe-location-id 0
account CCM134
media-late-to-early-iw incoming
media-late-to-early-iw outgoing
dtmf disable sip notify
dtmf prefer sip info
attach
adjacency sip CCM135
group v4
nat force-on
header-profile inbound ccmpf1
header-profile outbound ccmpf1
preferred-transport udp
signaling-address ipv4 33.33.36.1
statistics method summary
signaling-port 5060
remote-address ipv4 10.0.50.135 255.255.255.255
signaling-peer 10.0.50.135
dbe-location-id 0
attach
adjacency sip CCM136
force-signaling-peer
redirect-mode recurse
signaling-address ipv4 33.33.36.1
statistics method summary
signaling-port 5060
remote-address ipv4 10.0.50.136 255.255.255.255
signaling-peer 10.0.50.136
dbe-location-id 0
ping-enable
ping-interval 60
ping-lifetime 2
attach
adjacency sip CSPA23
nat force-off
preferred-transport udp
signaling-address ipv4 33.33.36.1
statistics method summary
remote-address ipv4 10.0.7.23 255.255.255.255
```

```

signaling-peer 10.0.7.23
dbe-location-id 0
attach
adjacency sip OpensipsV6
group IPv6
nat force-off
inherit profile preset-core
signaling-address ipv6 2001:A401::33:33:36:1
statistics method summary
signaling-port 7060
remote-address ipv6 2001::216:ECFF:FE3B:40DD/128
signaling-peer opensips.cisco.com
dbe-location-id 0
registration target address opensips.cisco.com
header-name From passthrough
dtmf prefer sip info
attach
adjacency sip CCM135-IPv6
force-signaling-peer
group v6
nat force-off
header-profile inbound ccmpf1
header-profile outbound ccmpf1
method-profile inbound ccmmethod2
method-profile outbound ccmmethod2
preferred-transport udp
signaling-address ipv6 2001:A401::33:33:36:1
statistics method summary
signaling-port 5060
remote-address ipv6 2001::10:0:50:135/128
signaling-peer 2001::10:0:50:135
dbe-location-id 0
attach
adjacency sip CCM135-vrfb
vrf h323-vrf-b
nat force-off
preferred-transport udp
signaling-address ipv4 10.190.7.97
statistics method summary
signaling-port 5060
remote-address ipv4 10.0.50.135 255.255.255.255
signaling-peer 10.0.50.135
dbe-location-id 0
attach
adjacency sip CCM136-IPv6
group v6
nat force-off
header-profile inbound ccmpf1
header-profile outbound ccmpf1
method-profile inbound ccmmethod2
method-profile outbound ccmmethod2
signaling-address ipv6 2001:A401::33:33:36:1
statistics method summary
signaling-port 5060
remote-address ipv6 2001::10:0:50:136/128
signaling-peer 2001::10:0:50:136
ping-enable
ping-interval 60
ping-lifetime 2
dtmf prefer sip info
attach
adjacency sip SIPP81-IPv6
group v6
nat force-off

```

```
preferred-transport udp
signaling-address ipv6 2001:A401::33:33:36:1
statistics method summary
signaling-port 5060
remote-address ipv6 2001::/64
signaling-peer 2001::10:0:244:81
dbe-location-id 0
dtmf disable sip notify
dtmf prefer sip info
attach
call-policy-set 1
first-call-routing-table ROUTE-ON-DEST-NUM
first-reg-routing-table REG-ROUTE-ON-SRC-ADJ
rtg-src-adjacency-table REG-ROUTE-ON-SRC-ADJ
  entry 1
    action complete
    dst-adjacency OpensipsV6
    match-adjacency UEV6
rtg-round-robin-table ROUND-ROBIN
  entry 1
    action complete
    dst-adjacency CCM136
  entry 2
    action complete
    dst-adjacency CCM136-IPv6
rtg-dst-address-table ROUTE-ON-DEST-NUM
  entry 1
    action next-table ROUND-ROBIN
    edit del-prefix 3
    match-address 536X digits
    prefix
  entry 2
    action next-table ROUND-ROBIN
    edit del-prefix 4
    match-address 7898X digits
    prefix
  entry 3
    action next-table ROUND-ROBIN
    edit del-prefix 3
    match-address 491X digits
    prefix
  entry 4
    action next-table ROUND-ROBIN
    edit del-prefix 3
    match-address 526X digits
    prefix
  entry 5
    action next-table ROUND-ROBIN
    edit del-prefix 3
    match-address 496X digits
    prefix
  entry 6
    action complete
    edit del-prefix 3
    dst-adjacency CCM135
    match-address 4553X digits
    prefix
  entry 7
    action complete
    edit del-prefix 3
    dst-adjacency CCM135
    match-address 789X digits
    prefix
  entry 8
```



```

    action complete
    edit del-prefix 4
    dst-adjacency CCM135
    match-address 5678X digits
    prefix
  entry 9
    action complete
    edit del-prefix 4
    dst-adjacency CCM135
    match-address 5677X digits
    prefix
  entry 10
    action complete
    edit del-prefix 3
    dst-adjacency CCM135
    match-address 516X digits
    prefix
  complete
  active-call-policy-set 1
  sip dns
    support-type sip-dns-naptr
  sip ip-fqdn-mapping 1 ipv6 2001::10:0:50:137 ccm137.cisco.com ip-to-fqdn
!
!
  billing
    local-address ipv4 33.33.36.1
    ldr-check 0 0
    method packetcable-em
    cache path harddisk:/cdr/
    retry interval 20
    cdr media-info
    packetcable-em 1 transport radius server1
      local-address ipv4 33.33.36.1
    activate

blacklist global ipv6 2002::10:0:0:1
  reason corrupt-message
  trigger-size 65535
  trigger-period 1 minutes
blacklist critical global ipv6 2003::10:0:0:1
  reason authentication-failure
  trigger-size 65535
  trigger-period 1 minutes

  subscriber sip:bob@isp.example.com
    sip-contact 2001::10:1:1:2
      adjacency UEV6
      delegate-registration sip:reg@isp.example.com
      adjacency OpensipsV6
      header-name supported add path
    activate

!
  media-address ipv4 33.33.36.2
  media-address ipv6 2001:A401::33:33:36:2
  media-timeout 360
  activate
!
```

The following example shows different signaling and media addresses configured on the SBC asr1, where the signaling address configured is ipv6 and the media address configured is ipv4:

```

sbc asr1
sbe
  adjacency sip CCM1-IPV6
  group media-v4
  nat force-off
  preferred-transport udp
  signaling-address ipv6 2001:A401::33:33:36:1
  statistics method summary
  signaling-port 5060
  remote-address ipv6 2001::10:0:56:186/128
  signaling-peer 2001::10:0:56:186
  dbe-location-id 0
  attach
  adjacency sip CCM2-IPV6
  group media-v4
  nat force-off
  preferred-transport udp
  signaling-address ipv6 2001:A401::33:33:36:1
  statistics method summary
  signaling-port 5060
  remote-address ipv6 2009::100:0:0:4/128
  signaling-peer 2009::100:0:0:4
  dbe-location-id 0
  attach
  cac-policy-set 1
  first-cac-table table1
  cac-table table1
  table-type limit account
  entry 1
  match-value media-v4
  action cac-complete
  caller media-type ipv4
  callee media-type ipv4
  complete
  active-cac-policy-set 1
  call-policy-set 1
  first-call-routing-table table1
  rtg-dst-address-table table1
  entry 1
  action complete
  edit del-prefix 3
  dst-adjacency CCM2-IPV6
  match-address 123X digits
  prefix
  complete
  active-call-policy-set 1
  !
  !
  !
  media-address ipv4 33.33.36.10
  media-timeout 360
  activate
  !
  !

```

IPv6 Configuration Commands

This section describes the configuration commands used to configure various types of IPv6 addressing or show output listing IPv6 addresses.

For details of the following commands, see the *Cisco Unified Border Element (SP Edition) Command Reference: Unified Model* at

http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbcu_book.html

Table 54-1 lists the new commands introduced in Cisco IOS XE Release 2.6.

Table 54-1 New Commands Introduced in Cisco IOS XE Release 2.6

Command	Description
callee media-type {ipv4 ipv6 inherit both}	To configure the media address type settings for a callee on the Cisco Unified Border Element (SP Edition). Use the no form of this command to disable the media address type settings for a callee.
caller media-type {ipv4 ipv6 inherit both}	To configure the media address type settings for a caller on the Cisco Unified Border Element (SP Edition). Use the no form of this command to disable the media address type settings for a caller.

Table 54-2 lists the commands modified for IPv6 addressing in Cisco IOS XE Release 2.6.

Table 54-2 Commands Modified for IPv6 Addressing in Cisco IOS XE Release 2.6

Command	Description
blacklist [critical] global [address-default {ipv4 {addr} ipv6 {addr}} [tcp {tcp-port} udp {udp-port} default-port-limit]]	The ipv6 keyword was added. Use this command to enter the mode for configuring the default event limits for the IPv6 address. For IPv6, only <i>global</i> option can be used.
clear sbc sbc-name sbe blacklist [critical] {ipv4 addr ipv6 addr} [{udp tcp} port]	The ipv6 keyword was added. To clear the blacklist for the specified Session Border Controller (SBC) service.
remote-address {ipv4 ip-address ip-mask ipv6 ip-address / prefix-length}	The ipv6 keyword was added. To configure either an H.323 or SIP adjacency to restrict the set of remote signaling peers that can be contacted over the adjacency to those with a given IP address prefix. To remove this configuration, use the no form of this command.
show sbc sbc-name sbe addresses	The output of this command was modified.
show sbc sbc-name sbe adjacencies {adjacency-name} [detail]	The output of this command was modified.

Table 54-2 Commands Modified for IPv6 Addressing in Cisco IOS XE Release 2.6

Command	Description
show sbc <i>sbc-name</i> sbe blacklist critical { <i>ipv4</i> <i>addr</i> <i>ipv6</i> <i>addr</i> } [tcp <i>tcp-port</i> udp <i>udp-port</i>]	The ipv6 keyword was added. The command was updated to show all configured critical blacklists for IPv6 addresses.
show sbc <i>sbc-name</i> sbe blacklist [<i>source</i>] { <i>ipv4</i> <i>IP address</i> <i>ipv6</i> <i>IP address</i> }	The ipv6 keyword was added.
show sbc <i>name</i> sbe cac-policy-set [<i>id</i> [<i>table name</i> [<i>entry id</i>]] <i>active</i> [<i>table name</i> [<i>entry id</i>]]] [detail]	The output of this command was modified.
show sbc <i>sbc-name</i> sbe calls	To provide details of IPv6 calls.
show sbc <i>sbc-name</i> sbe call-stats { all global src-seccount <i>name</i> dst-account <i>name</i> src-adjacency <i>name</i> dst-adjacency <i>name</i> } <i>period</i>	To list the number of active IPv6 calls.
show sbc <i>sbc-name</i> sbe addresses	The output of this command was modified.
show sbc <i>sbc-name</i> sbe sip ip-fqdn-mapping	Displays the IP-FQDN mapping table. The output of this command was modified to include IPv6 details.
signaling-address { <i>ipv4</i> <i>ipv4_IP_address</i> <i>ipv6</i> <i>ipv6_IP_address</i> }	To define the local signaling address of an H.323 (IPv4 only) or SIP adjacency. The ipv6 keyword was added. To return to the default behavior, use the no form of this command.
sip ip-fqdn-mapping <i>index</i> { <i>ipv4</i> <i>ipv6</i> } <i>ip-address fqdn</i> { both-ways ip-to-fqdn }	To configure SIP IP-to-FQDN mapping on signaling border elements (SBEs). The ipv6 keyword was added.

Table 54-3 lists the command modified for IPv6 addressing in Cisco IOS XE Release 3.1.0S.

Table 54-3 Command Modified for IPv6 Addressing in Cisco IOS XE Release 3.1.0S

Command	Description
blacklist [critical] vpn { <i>vpn-name</i> } [address-default [address-family { <i>ipv4</i> <i>ipv6</i> }] address-family { <i>ipv4</i> <i>ipv6</i> } <i>ipv4</i> <i>addr</i> [tcp { <i>tcp-port</i> } udp { <i>udp-port</i> } default-port-limit] <i>ipv6</i> <i>addr</i> [tcp { <i>tcp-port</i> } udp { <i>udp-port</i> } default-port-limit]]	The ipv6 keyword was added. Use this command to enter the mode for configuring the default event limits for the IPv6 address in a VPN.

Table 54-4 lists the command modified for IPv6 addressing in Cisco IOS XE Release 3.5.0S.

Table 54-4 Command Modified for IPv6 Addressing in Cisco IOS XE Release 3.5.0S

Command	Description
branch media-type {ipv4 ipv6 inherit both}	Configures the media address type settings for a caller or callee on the Cisco Unified Border Element (SP Edition). Use the no form of this command to disable the media address type settings for the caller or callee.

