IPv6 and IPv4 Interworking

The SBC Core supports IPv4 and IPv6 interworking for media and signaling IP versions.

- Dual IPv4 and IPv6 stacks
- IPv6 for UDP
- TCP and TLS for SIP signaling
- Both A and AAAA queries to the DNS server
- Assigning both an IPv4 and IPv6 interface to the same physical Ethernet port or VLAN on that port
- Assigning SIP signaling port to both IPv4 and IPv6 address

**IPv6 Addressing**

The SBC provides the ability to assign IP Interface IPv6 addresses from address spaces that are not reserved by IETF or multicast. This can be global unicast, local unicast, or link-local unicast addresses. Avoid using multicast addresses as source addresses in IPv6 packets or in any routing header. When received, such packets must be dropped.

⚠️ Once configured, an IPv6 address cannot be deleted without removing the underlying interface configuration. However, an existing IPv6 address may be changed without removal of the interface itself.

**IPv6 Ingress Behavior**

If the SBC receives an INVITE from a peer using IPv6 address and the contact header contains a FQDN, then a DNS query for the FQDN is made to resolve the FQDN. If the FQDN query returns a IPv4 address, then the SBC contacts the peer using the IPv4 address even though the INVITE from the peer was received using a IPv6 address.

In another instance, a remote peer may send INVITE using IPv6 and FQDN in the contact header. When trying to send a request back to the peer, AAAA query is made for the FQDN in contact header. If an IPv4 address is returned, a request is sent to the peer using IPv4 even though INVITE was received from peer on IPv6.

**IPv6 Egress Behavior**

- If the next hop address is FQDN, the first A query is made to resolve FQDN to IP address. If the DNS query is successful and it returns an IPv4 address then IPv4 SIP signaling port from the zone (to which SIP Service group belongs) is selected to send message on outgoing leg.
- If a media offer is sent and if value of “IP Version Control for Media” is “Choose IPv4 only”, then SDP offer is generated for all media lines having IP version IPv4.
- If a media offer is to sent and if value of “IP Version Control for Media” is “Choose IPv6 only”, then SDP offer is generated for all media lines having IP version IPv6.
- If a media offer is sent and if value of “IP Version Control for Media” is “Media to match Signaling IP version”, then SDP offer is generated for all media lines having IP version IPv4.
- If the next hop address is FQDN, and if AAAA query returns IPv4 address only then call fails.
- If the next hop address is FQDN, and if a query fails, then crank back is run and egress leg creation process is started from beginning. This time AAAA query is made assuming that peer is IPv6. When crank back processing begins, IPv6 port is selected to send the signaling message.
- If the next hop address is FQDN, and after crank back AAAA query is successful and returns an IPv6 address, IPv6 type egress signaling leg is created.
• If media offer is made and value of flag “IP Version Control for Media” is “Choose IPv4 only” then SDP offer is generated of IP version IPv4.
• If a media offer is to be made and value of flag “IP Version Control for Media” is “Choose IPv6 only” then SDP offer is generated of IP version IPv6.
• If a media offer is made and value of flag “IP Version Control for Media” is “Media to match Signaling IP version” then SDP offer is generated of IPv6.
• If the next hop address is FQDN, and after crank back AAAA query is successful and returns an IPv4 address, further crank back does not happen again and hence call is rejected.
• If the next hop address is FQDN and DNS query to resolve this FQDN fails, call is rejected.

Configuring Objects for IPv4 and IPv6 Interworking

Signaling ports can have both an IPv4 and an IPv6 address configured on the same port. Local and Remote IP version types must be same for the IP Packets.

Trunk groups can be heterogeneous:

• Peer prefixes can be of either IP version.
• A SIP trunk group is not tied to a given SIP signaling port.
• The same trunk group can be used for sending signaling traffic toward IPv4 and IPv6 SIP Peers.
• The same trunk group can be used for sending media traffic toward IPv4 as well as IPv6 media SIP Peers.

An IP interface group can be heterogeneous. This allows configuring media interface group with mixed IP versions, and is useful for supporting different versions for signaling and media leg in the same call:

• SIP signaling port will point to IP Interface group for signaling.
• SIP trunk group will point to IP Interface group for media.
• The SBC supports heterogeneous IP version for signaling and media on same call leg (that is IPv6 Signaling and IPv4 media) to support scenarios where signaling path and media path for a call are different.
• A SIP Peer object is capable of creating and configuring a static SIP Peer endpoint comprised of zone and IPv4 or IPv6 address information. This information is used in the routing of SIP messages and Call Admission Control (CAC).

The IP Version Control flag "mediaAddrType" can be configured for a SIP trunk group to make an SDP offer on egress leg. The flag chooses the appropriate IP version if the media interface group is heterogeneous. Refer to SIP Trunk Group - Media - CLI for configuration details.

Note
The SBC Core does not support NAT traversal for IPv6 calls. Ensure NAT is disabled in pure IPv6 call scenarios.