Configure IPv6

IPv6 Configuration

Packaged CCE can support IPv6 connections for agent and supervisor Finesse desktops and phones. An IPv6-enabled deployment can use either all IPv6 endpoints or a mix of IPv4 and IPv6 endpoints. Servers that communicate with these endpoints can accept both IPv4 and IPv6 connections. Communication between servers continues to use IPv4 connections.

This chapter contains the configuration procedures that you perform for IPv6-enabled deployments.

Set Up IPv6 for VOS-Based Contact Center Applications

By default, only IPv4 is enabled for Unified Communications Manager, Cisco Finesse, and Unified Intelligence Center.

If you choose to enable IPv6 on these applications, you must enable it on both the publisher/primary nodes and subscriber/secondary nodes for those applications.

You can use Cisco Unified Operating System Administration or the CLI to enable IPv6.

See the *Solution Design Guide for Cisco Packaged Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-technical-reference-list.html for more information about IPv6 support in Packaged CCE deployments.

Set Up IPv6 Using Cisco Unified Operating System Administration

To set up IPv6 using Cisco Unified Operating System Administration, perform the following procedure on the primary and secondary VOS servers.

Procedure

Step 1   Sign into Cisco Unified Operating System Administration on the Publisher/Primary node:.

- Unified Communications Manager and Unified Intelligence Center: `https://<host or IP address of the Publisher or Primary node>/cmplatform`

- Finesse: `https://FQDN of the Primary node:8443/cmplatform`

Step 2   Navigate to **Settings** > **IP** > **Ethernet IPv6**.

Step 3   Check the **Enable IPv6** check box.

Step 4   Enter values for **IPv6Address**, **Prefix Length**, and **Default Gateway**.

Step 5   Check the **Update with Reboot** check box.

Step 6   Click **Save**.
The server restarts.

Step 7   Repeat this procedure on the subscriber/secondary node.

Set Up IPv6 for VOS-Based Applications Using the CLI

To set up IPv6 using the CLI, perform the following procedure on both the primary and secondary VOS servers.

Procedure

Step 1   Access the CLI on the VOS server.

Step 2   To enable or disable IPv6, enter:
set network ipv6 service {enable | disable}

Step 3   Set the IPv6 address and prefix length:
set network ipv6 static_address *addr mask*

Example:
```
set network ipv6 static_address 2001:db8:2::a 64
```

Step 4   Set the default gateway:
set network ipv6 gateway *addr*

Step 5   Restart the system for the changes to take effect.
utils system restart

Step 6   To display the IPv6 settings, enter:
show network ipv6 settings

Configure NAT64 for IPv6-Enabled Deployment

NAT64 allows communication between IPv6 and IPv4 networks. For IPv6-enabled deployments, you must set up NAT64 so that supervisors on an IPv6 network can access Unified CCE Administration web tools on an IPv4 network.

You can use either Stateful and Stateless NAT64. To read more about which translation type is the most appropriate for your deployment see Table 2. Comparison Between Stateless and Stateful NAT64 here: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/white_paper_c11-676278.html

Note NAT64 is NOT supported on M train IOS. T train is required.

For more information, see the Compatibility Matrix for Packaged Contact Center Enterprise at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-device-support-tables-list.html.

The following example network diagram and interface configuration demonstrates Stateful NAT64 translation between an IPv6 network and an IPv4 network.
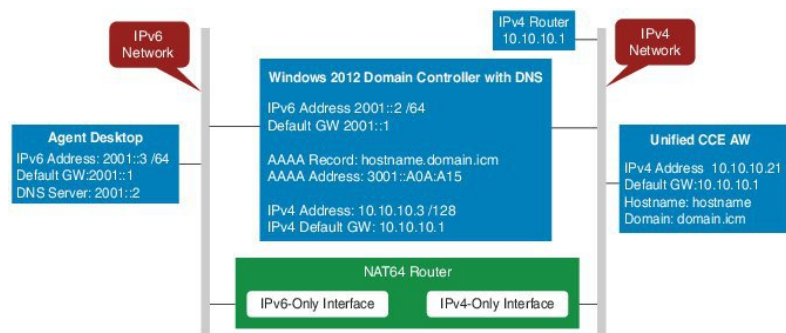

```
interface GigabitEthernet0/0
description ipv4-only interface
 ip address 10.10.10.81 255.255.255.128
 duplex auto
 speed auto
 nat64 enable
 no mop enabled

interface GigabitEthernet0/1
description ipv6-only interface
 no ip address
 duplex auto
 speed auto
 nat64 enable
 ipv6 address 2001::1/64
 ipv6 enable

ipv6 unicast-routing
ipv6 cef
!
nat64 prefix stateful 3001::/96
nat64 v4 pool POOL1 10.10.10.129 10.10.10.250
```

```
nat64 v6v4 list V6ACL1 pool POOL1 overload
ipv6 router rip RIPv6
!
ipv6 router rip RIP

!
ipv6 access-list V6ACL1
 permit ipv6 2001::/64 any
```

Configure DNS for IPv6

To meet the requirement that Unified CCE Administration be accessed by FQDN, a Forward lookup AAAA record for the Unified CCE AW-HDS-DDS servers and any External HDS servers must be created in DNS.

The steps in this procedure are for a Windows DNS server.

Procedure

Step 1	In Windows, navigate to **Administrative Tools > DNS**. This opens the DNS Manager.
Step 2	In the Forward lookup zone, navigate to your deployment's domain name.
Step 3	Right-click the domain name and select **New Host (A or AAAA)**.
Step 4	In the New Host dialog box, enter the computer name and IP address of the Unified CCE AW-HDS-DDS servers and any External HDS servers. Click **Add Host**.

Determine IPv6 Translation of IPv4 Address for DNS Entry

You can determine the IPv6 address needed for the AAAA DNS record by running a ping command on any Windows machine using mixed notation. Type "ping -6" followed by your IPv6 Nat64 Prefix, two colons, and then the IPv4 address.
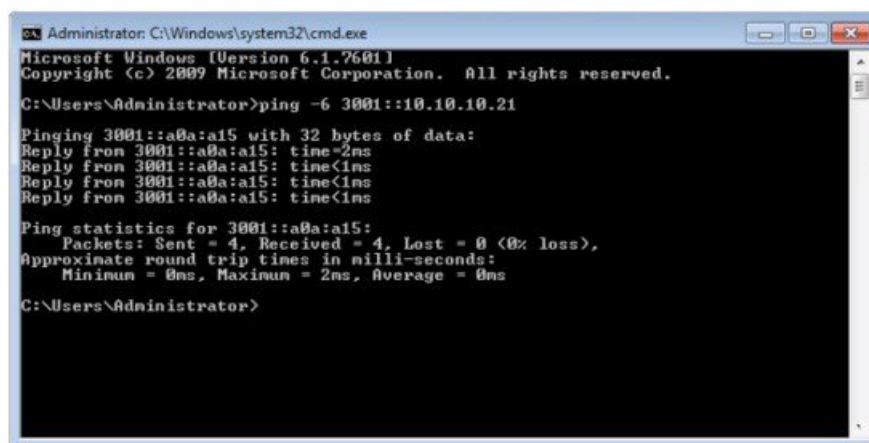
In the ping response, the IPv4 address is converted to the hexadecimal equivalent. Use this address in your static AAAA record.

Note   Optionally, DNS64 can be used in place of static DNS entries. Use of DNS64 helps facilitate translation between IPv6 and IPv4 networks by synthesizing AAAA resource records from A resource records.

The *NAT64 Technology: Connecting IPv6 and IPv4 Networks* whitepaper gives an overview of DNS64 and how it is used with IPv6: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/white_paper_c11-676278.html.

Configure IPv6 on Unified CVP Call Server

For IPv6-enabled deployments, you must add an IPv6 address to your Unified CVP Call Server's existing network interface.

Perform this procedure only if you have an IPv6-enabled environment.

Procedure

Step 1	On the Unified CVP Call Server, navigate to **Control Panel** > **Network and Sharing**.
Step 2	Click **Ethernet**.
Step 3	From the **Ethernet Status** window, select **Properties**.
Step 4	Check the **Internet Protocol Version 6 (TCP/IPv6)** check box, and choose **Properties**.
Step 5	Choose **Use the following IPv6 address** radio button.
Step 6	Enter values in the **IPv6 address**, **Subnet prefix length**, and **Default gateway** fields.
Step 7	Click **OK** and restart Windows when prompted.

Configure Gateways to Support IPv6

For IPv6-enabled deployments, you must configure your Ingress and VXML gateways to enable IPv6 addressing.

Configure an Interface to Support IPv6 Protocol Stack

This procedure applies to both the Ingress and the VXML gateway.

Procedure

Configure the following on the Gateway:

```
>Enable
>configure terminal
>interface type number
```

```
>ipv6 address{ ipv6-address / prefix-length | prefix-name sub-bits / prefix-length}
>ipv6 enable
```

Enable ANAT in Ingress Gateway

Procedure

Configure the following on the Gateway:

```
>conf t
>voice service voip
>SIP
>ANAT
>bind control source-interface GigabitEthernet0/2
>bind media source-interface GigabitEthernet0/2
```

Enable Dual Stack in the Ingress Gateway

Procedure

Configure the following on the Gateway:

```
>conf t
>sip-ua
>protocol mode dual-stack preference ipv6
```

Configure IPv6 on Unified Communications Manager

In an IPv6-enabled environment, you must perform the procedures in this section to configure IPv6 on Unified Communications Manager.

Cluster-Wide Configuration in Unified CM Administration

Perform the following procedure to set IPv6 as the addressing mode preference for media and signaling cluster-wide.

Procedure

Step 1	From **Cisco Unified CM Administration**, choose **System** > **Enterprise Parameters** > **IPv6 Configuration Modes** to configure the cluster-wide IPv6 settings for each Unified Communications Manager server.
Step 2	From the **Enable IPv6** drop-down list, choose **True**.
Step 3	From the **IP Addressing Mode Preference for Media** drop-down list, choose **IPv6**.
Step 4	From the **IP Addressing Mode Preference for Signaling** drop-down list, choose **IPv6**.
Step 5	From the **Allow Auto-configuration for Phones** drop-down list, choose **Off**.
Step 6	Save your changes.

Transcoding

In an IPv6-enabled environment, a transcoder is required for the following scenarios:

- An agent logged in to an IPv6 endpoint needs to send or receive transfers from an agent logged in to an IPv4 endpoint.

- An agent logged in to an IPv6 endpoint needs to connect to a VXML Gateway for self service.

Related Topics

Transcoder Configuration in Unified CM and IOS Gateway

Add a Common Device Configuration Profile in Unified Communications Manager

In an IPv6-enabled environment, you may have both IPv4 and IPv6 devices.

Perform the following procedure to add an IPv4, IPv6, or dual stack common device configuration profile in Unified Communications Manager.

Procedure

Step 1	From **Cisco Unified CM Administration**, choose **Device** > **Device Settings** > **Common Device Configuration**.
Step 2	Click **Add New** and enter the name of the new common device configuration profile.
Step 3	From the **IP Addressing Mode** drop-down list:

- To add an IPv6 common device configuration profile in Unified Communications Manager, choose **IPv6 only**.
- To add an IPv4 common device configuration profile in Unified Communications Manager, choose **IPv4 only**.
- To add a dual stack common device configuration profile in Unified Communications Manager, choose **IPv4 and IPv6**. Then choose **IPv4** from the **IP Addressing Mode Preference for Signaling** drop-down list.

Step 4 Save your changes.

Associate the Common Device Configuration Profile with Gateway Trunk

Perform the following procedure to associate the common device configuration profile with the Gateway trunk. This procedure applies to the Ingress Gateway.

Procedure

Step 1 From **Cisco Unified CM Administration**, choose **Device** > **Trunk**.

Step 2 Click **Find**.
Choose the trunk profile that you want to view.

Step 3 From the **Common Device Configuration** drop-down list:

- To associate the IPv6 common device configuration profile with the Gateway trunk, choose the IPv6 common device configuration profile.
- To associate the IPv4 common device configuration profile with the Gateway trunk, choose the IPv4 common device configuration profile.

Note Unified CM gateway trunk supports only an IPv4 or IPv6 trunk. You cannot associate a dual stack common device configuration profile to a Unified CM gateway trunk.

Step 4 Enter the IPv6 address in the **Destination Address IPv6** field.

Note Unified CM to Gateway trunk supports only standard SIP Profile and does not support ANAT enabled dual-stack SIP trunk.

Step 5 Save your changes.

Associate the Common Device Configuration Profile with an IPv4 or IPv6 Phone

Procedure

Step 1 From **Cisco Unified CM Administration**, choose **Device** > **Phone**.

Step 2 Click **Find**.
Choose the trunk profile that you want to view.

Step 3 From the **Common Device Configuration** drop-down list: choose the IPv6 common device configuration profile.

- To associate the IPv6 common device configuration profile to an IPv6 phone, choose the IPv6 common device configuration profile.
- To associate the IPv4 common device configuration profile to an IPv4 phone, choose the IPv4 common device configuration profle.

Step 4   Save your changes.

Associate a SIP Profile in Unified CM

In an IPv6-enabled deployment, you must associate a SIP profile with the trunk you configured for Unified CVP.

Procedure

Step 1   From **Cisco Unified CM Administration**, choose **Device** > **Trunk**.

Step 2   Click **Find**. Choose the trunk profile that you want to view.

Step 3   From the **SIP Profile** drop-down list, choose the SIP Profile you created.

    Note   For more information on how to create a SIP Profile, see

        Add a SIP Profile in Unified CM.

Step 4   Save your change.

Related Topics

    Configure Trunk

Associate the Dual Stack Common Device Configuration Profile with SIP Trunk

Procedure

Step 1   From **Cisco Unified CM Administration**, choose **Device** > **Trunk**.

Step 2   Click **Find**. Choose the trunk profile that you want to view.

Step 3   From the **Common Device Configuration** drop-down list, choose the Dual Stack Common Device Configuration Profile.

    Note   For more information on how to add a Dual Stack Common Device Configuration Profile, see Add a Common Device Configuration Profile in Unified Communications Manager, on page 7.

Step 4   Save your change.