Support for IPv6

This chapter describes the IPv6 support provided in Campus Manager 4.0.3. It contains the following topics:

Understanding IPv6

IPv6 support in Campus Manager 4.0.3 includes the following network scenarios:

- Devices that may have IPv6 configured on their interfaces, but which have at least one IPv4 interface. Devices are managed using IPv4.
- Hosts running IPv6 are supported in the User Tracking application.

Campus Manager has been updated as follows for IPv6 support:

Discovery Related Changes

Device Discovery collects IPv6 address and related information from devices, which is used in User Tracking and Path Analysis.

For Discovery to support IPv6 in Campus Manager:

- Ensure that the Discovery.IPv6 property is set to ON in the ANIServer.properties file. By default, it is set to ON.
- Give preference to local device database. Use **`/etc/inet/ipnodes`** for IPv6 addresses and use **`/etc/hosts`** for IPv4 addresses.
- Do not configure multiple IPv6 addresses on your Solaris server.
- Do not configure your Solaris machine as IPv6 only. Discovery supports only IPv6 on dual stack devices. Dual stack devices are those that have both IPv4 and IPv6 address.
- Check your Layer 3 connectivity from Solaris to other IPv6 enabled devices using traceroute and ping.
- Ensure that all the devices in the network covered during Discovery are dual stack.
- Use **`name lookup`** and configure your device for IPv6.

Note You can only specify a device with IPv4 address as seed device.

User Tracking Changes

IPv6 support in User Tracking is available on both Solaris and Windows servers. In User Tracking, hosts configured with IPv6 address are discovered and shown in the main table. IPv6 name lookup is done if IPv4 name lookup fails. That is, for a given IPv6 address, it returns the host name. IPv6 does not support reverse name lookup.

All global unicast addresses are fetched and used for User Tracking computation but link local addresses are dropped.

User Tracking end host reports have an IPv6 format. Select this format to view the IPv6 address, Prefix Length and Prefix of IPv6 enabled devices.

User Tracking Ping Sweep Applicability to IPv6 Subnets

Ping Sweep functionality is currently available for Class C or smaller subnets. With IPv6, each of the networks can be larger than Class C networks. Hence we cannot determine individual IPv6 addresses that can be present in a given network or sub-network. Therefore, Ping Sweep is not applicable on any of the IPv6 subnets.

Path Analysis Changes

Path Analysis is modified to support only the IPv6 source to IPv6 destination through IPv6 network scenario. To accommodate the above requirement the following changes are made:

- Current IP trace algorithms are reused and modified appropriately to accommodate IPv6 trace.
- Change address resolution is provided to accommodate AAAA type records. The AAAA resource record type is a new record specific to the Internet class that stores a single IPv6 address. The value of the type is 28 (decimal).

Path Analysis Related Restrictions

For IPv6 support in Path Analysis:

- IPv6 trace is not supported for CiscoWorks server on Windows platforms due to non-availability of Label Switch Router (LSR) traceroute on Windows platforms
- Configure one global IPv6 address on your Solaris server running Campus Manager.
- Perform name lookup using **`/etc/inet/ipnodes`**.
- Map the device name to IPv6 addresses in DNS server or in the local device database [**`/etc/inet/ipnodes`**] for the Path traces to run.
- As part of the IPv6 network you can have a tunnel between a Solaris machine running Campus Manager with IPv6, and an IPv6 network.
- You can have tunnels between two IPv6 networks.
- IPv6 name lookup feature is available only on Solaris, Windows 2003 and Windows XP machines. Windows 2000 Server (WinSock) does not support this feature.
- Routing protocols such as BGP, RIPv6, and OSPFv3 are supported.

Subnet to VLAN Mapping

Sometimes Layer 2 traces are not seen in Path Analysis when you run IPv6 Trace. Subnet to VLAN mapping does not contain enough entries to determine the Layer 2 trace.

However, you can overcome this constraint by:

1. Creating anisubnet6.conf file with permissions (r w _ r_ _ _ _ _)640 under *NMSROOT*/campus/etc/cwsi/
2. Adding subnet to VLAN mapping entries

   Format: subnet address|subnetmask|VTP Domain|VLAN

   For example: `2001:5:a:1::|64|CMTestLab|vlan2`

You can enter subnet to VLAN mapping entries for IPv4 traces through the workflow provided.

Topology Changes

Topology Services provides the following for IPv6 support:

- IPv6 filter that lets you highlight the IPv6 devices
- Find option for IPv6 devices
- Table for devices running IPv6

Viewing IPv6 Addresses Report

You can view IPv6 addresses report for IPv6 enabled devices.

To view this report:

Step 1 Right-click the LAN Edge View or Layer 2 View from Network Views in the Topology Services window.

Step 2 Click **Display View**.

The Network Topology window appears.

Step 3 Select an IPv6 enabled device.

Step 4 Right-click the device then select IPv6 Addresses, or click **Reports > IPv6 Addresses**.

The IPv6 Addresses report appears.

Interpreting IPv6 Addresses Report

See Table 11-1 for interpreting the fields in the IPv6 Addresses Report.

Table 11-1 IPv6 Addresses Report

Field	Description
Interface Name	Name of the IPv6 address interface.
IPv6 Address	IPv6 address of the device. An IPv6 address typically has four groups of 8 bits each. Example: `2001:5:A:3:0:0:0:2`
Prefix Length	Length of the prefix. It is a decimal value representing how many of the left most contiguous bits of the address comprise the prefix.
Prefix Address	Prefix portion of the IPv6 address. This is similar to CIDR in IPv4 and is written in CIDR notation. An IPv6 address prefix is represented by the notation: `IPv6-address/prefix-length`
Address Type	Type of IPv6 address. Campus Manager supports unicast addresses. The Address Type can be global, link-local, or site-local. Global addresses are identified by the Format Prefix of 001. Addresses of this type are designed to be aggregated or summarized to produce an efficient routing infrastructure. Link-local addresses are used to communicate between hosts on the link with no router. Site-local addresses are used between nodes that communicate with other nodes in the same site. Site-local addresses are identified by the Format Prefix of 1111 1110 11.