Configuring IPv6 Client Mobility

- Prerequisites for IPv6 Client Mobility, on page 1
- Restrictions For IPv6 Client Mobility, on page 1
- Information About IPv6 Client Mobility, on page 2
- Verifying IPv6 Client Mobility, on page 5
- Monitoring IPv6 Client Mobility, on page 5
- Additional References, on page 6
- Feature Information For IPv6 Client Mobility, on page 7

Prerequisites for IPv6 Client Mobility

To enable wireless IPv6 client connectivity, the underlying wired network must support IPv6 routing and an address assignment mechanism such as SLAAC or DHCPv6. The device must have L2 adjacency to the IPv6 router, and the VLAN needs to be tagged when the packets enter the device. APs do not require connectivity on an IPv6 network, as all traffic is encapsulated inside the IPv4 CAPWAP tunnel between the AP and device.

Restrictions For IPv6 Client Mobility

- When using the IPv6 Client Mobility, clients must support IPv6 with either static stateless auto configuration (such as Windows XP clients) or stateful DHCPv6 IP addressing (such as Windows 7 clients).
- To allow smooth operation of stateful DHCPv6 IP addressing, you must have a switch or router that supports the DHCP for IPv6 feature (such as the device) that is configured to act like a DHCPv6 server, or you need a dedicated server such as a Windows 2008 server with a built-in DHCPv6 server. Cisco Catalyst 3850 switch and Cisco Catalyst 5700 switch can act as (internal) a DHCPv6 server.

Note To load the SDM IPv6 template in the Cisco Catalyst 3850 switch, enter the **sdm prefer dual-ipv4** and **v6** default command and then reset the switch.

Information About IPv6 Client Mobility

The Device supports IPv6 mobility for IPv6-only or dual-stack nodes. The IPv6 Client Mobility is divided into:

- Link Layer and
- Network Layer

The link layer is handled by the 802.11 protocol which enables the client to roam to any AP in the same BSS (basic service set) identified by the same SSID without losing the link layer connectivity.

However, link layer mobility is not enough to make wireless client Layer 3 applications continue to work seamlessly while roaming. Cisco IOSd's wireless mobility module uses mobility tunneling to retain seamless connectivity for the client's Layer 3 PoP (point of presence) when the client roams across different subnets on different switches.

IPv6 is the next-generation network layer Internet protocol intended to replace IPv4 in the TCP/IP suite of protocols. This new version increases the internet global address space to accommodate users and applications that require unique global IP addresses. IPv6 incorporates 128-bit source and destination addresses, which provide significantly more addresses than the 32-bit IPv4 addresses.

To support IPv6 clients across controllers, ICMPv6 messages must be dealt with specially to ensure the IPv6 client remains on the same Layer 3 network. The device keep track of IPv6 clients by intercepting the ICMPv6 messages to provide seamless mobility and protect the network from network attacks. The NDP (neighbor discovery packets) packets are converted from multicast to unicast and delivered individually per client. This unique solution ensures that Neighbor Discovery and Router Advertisement packets are not leaked across Vlans. Clients can receive specific Neighbor Discovery and Router Advertisement packets ensuring correct IPv6 addressing and avoids unnecessary multicast traffic.

The configuration for IPv6 mobility is the same as IPv4 mobility and requires no separate software on the client side to achieve seamless roaming. The device must be part of the same mobility group. Both IPv4 and IPv6 client mobility are enabled by default.

IPv6 client mobility is used for the following:

- Retaining the client IPv6 multiple addresses in Layer-2 and Layer-3 roaming.
- IPv6 Neighbor Discovery Prootcol (NDP) packet management.
- Client IPv6 addresses learning.

Using Router Advertisment

The Neighbor Discovery Protocol(NDP) operates in the link-layer and is responsible for the discovery of other nodes on the link. It determines the link-layer addresses of other nodes, finds the available routers, and maintains reachability information about the paths to other active neighbor nodes.

Router Advertisement (RA) is one of the IPv6 Neighbor Discovery Protocol (NDP) packets that is used by the hosts to discover available routers, acquire the network prefix to generate the IPv6 addresses, link MTU, and so on. The routers send RA on a regular basis, or in response to hosts Router Solicitation messages.

IPv6 wireless client mobility manages the IPv6 RA packet . The converged access device forwards the link-local all-nodes multicast RA packets to the local and roaming wireless nodes mapped on same VLAN the RA was received on.

Figure 1 illustrates the link-local all-nodes mcast RA forwarding issue in the wireless node mobility.

Figure 1: Roaming Client Receiving Invalid RA from Router 2

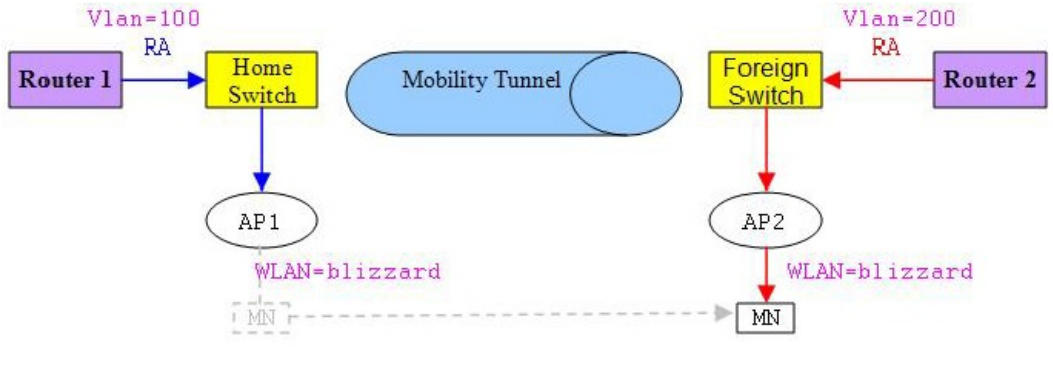
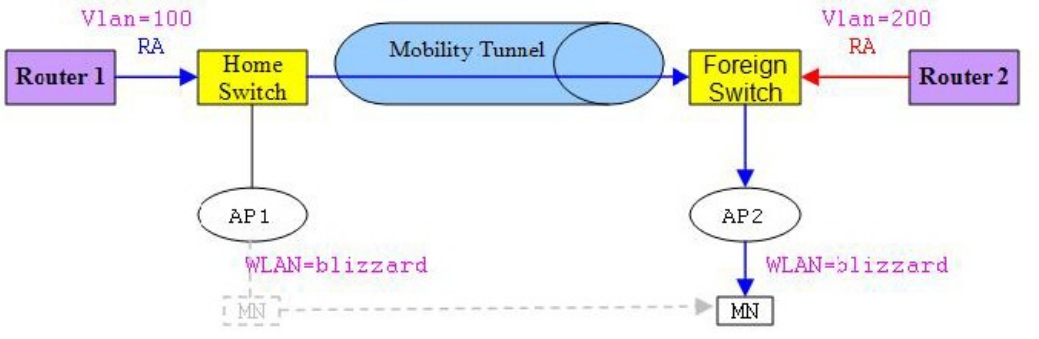


Figure 2 illustrates how a roaming client “MN” receives RA from VLAN 200 in a foreign switch and how it acquires an new IP address and breaks into L3 mobility's point of presence.

Figure 2: Roaming Client Receives Valid RA from Router 1



Related Topics

Verifying IPv6 Client Mobility, on page 5
Monitoring IPv6 Client Mobility, on page 5

RA Throttling and NS suppression

To safeguard the power-saving wireless clients form being disturbed by frequent unsolicited periodic RAs, the controller can throttle the unsolicited multicast RA.

Related Topics

Verifying IPv6 Client Mobility, on page 5
Monitoring IPv6 Client Mobility, on page 5

IPv6 Address Learning

There are three ways for IPv6 client to acquire IPv6 addresses:

- Stateless Address Auto-Configuration (SLAAC)
- Stateful DHCPv6
- Static configuration

For these methods, the IPv6 client always sends NS DAD (duplicate address detection) to ensure that there is no duplicated IP address on the network. The device snoops the clients NDP and DHCPv6 packets to learn about its client IP addresses and then updates the controllers database. The database then informs the controller for the clients new IP address.

Related Topics

Verifying IPv6 Client Mobility, on page 5
Monitoring IPv6 Client Mobility, on page 5

Handling Multiple IP Addresses

In the case when the new IP address is received after RUN state, whether an addition or removal, the controller updates the new IP addresses on its local database for display purposes. Essentially, the IPv6 uses the existing or same PEM state machine code flow as in IPv4. When the IP addresses are requested by external entities, for example, from Prime Infrastructure, the controller will include all the available IP addresses, IPv4 and IPv6, in the API/SPI interface to the external entities.

An IPv6 client can acquire multiple IP addresses from stack for different purposes. For example, a link-local address for link local traffic, and a routable unique local or global address.

When the client is in the DHCP request state and the controller receives the first IP address notification from the database for either an IPv4 or IPv6 address, the PEM moves the client into the RUN state.

When a new IP address is received after the RUN state, either for addition or removal, the controller updates the new IP addresses on its local database for display purposes.

When the IP addresses are requested by external entities, for example, from Prime Infrastructure, the controller provides the available IP addresses, both IPv4 and IPv6, to the external entities.

Related Topics

Verifying IPv6 Client Mobility, on page 5
Monitoring IPv6 Client Mobility, on page 5

IPv6 Configuration

The device supports IPv6 client as seamlessly as the IPv4 clients. The administrator must manually configure the Vlans to enable the IPV6, IPv6's snooping and throttling functionality. This will enable the NDP packets to throttle between the device and its various clients

Related Topics

Verifying IPv6 Client Mobility, on page 5
Monitoring IPv6 Client Mobility, on page 5

High Availability

The switch will sync with the wireless clients when the clients IP address is hard to learn. When a switchover happens, the IPv6 neighbor binding table is synced to standby state. However, the wireless client will itself disassociate and reassociate to a new active state once the switchover is complete and the neighbor binding table is updated with latest information for that client.

If, during the reassociation, the client moves to another AP then the original entry in the binding table is marked as down for sometime and will be aged-out.

For the new entries joining the switch from another AP, the new IP address is learned and notified to the controller's database.

Note This feature is available only for the Cisco Catalyst 3850 Switch.

Related Topics

Verifying IPv6 Client Mobility, on page 5
Monitoring IPv6 Client Mobility, on page 5

Verifying IPv6 Client Mobility

The commands listed in the Table 1 applies to the IPv6 client mobility.

Table 1: Commands for Verifying IPv6 Client Mobility on Cisco 5760 WLC

Command	Description
debug mobility ipv6	Enables all the wireless client IPv6 mobility debugs.
debug **client** **mac-address** **(mac-addr)**	Displays wireless client debugging. Enter a MAC address for debugging information.

Related Topics

Using Router Advertisment, on page 2
RA Throttling and NS suppression, on page 3
IPv6 Address Learning, on page 4
Handling Multiple IP Addresses, on page 4
IPv6 Configuration, on page 4
High Availability, on page 5
Monitoring IPv6 Client Mobility, on page 5

Monitoring IPv6 Client Mobility

The commands in Table 2 are used to monitor IPv6 Client mobility on the device.

Table 2: Monitoring IPv6 Client Mobility Commands

Commands	Description
show wireless client summary	Displays the wireless specific configuration of active clients.
show wireless client mac-address `(mac-addr)`	Displays the wireless specific configuration of active clients based on their MAC address.

Related Topics

Verifying IPv6 Client Mobility, on page 5
Using Router Advertisment, on page 2
RA Throttling and NS suppression, on page 3
IPv6 Address Learning, on page 4
Handling Multiple IP Addresses, on page 4
IPv6 Configuration, on page 4
High Availability, on page 5

Additional References

Related Documents

Related Topic	Document Title
IPv6 command reference	*IPv6 Command Reference (Catalyst 3850 Switches)*
Mobility configuration	*Mobility Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information For IPv6 Client Mobility

This table lists the features in this module and provides links to specific configuration information:

Feature	Release	Modification
IPv6 Client Mobility Functionality	Cisco IOS XE 3.2SE	This feature was introduced.