Configuring IPv6

This chapter describes how to configure IPv6 information on the Cisco 910 Industrial Routers (hereafter referred to as the router).

For information about configuring IPv4 on the router, see Chapter 14, “Configuring IPv4.”

This chapter consists of these sections:

- Understanding IPv6, page 1
- Configuring IPv6, page 5
- Diagnosing IPv6 Connectivity, page 8
- Displaying and Monitoring IPv6, page 9

Understanding IPv6

IPv4 users can move to IPv6 and receive services such as exit-to-exit security, quality of service (QoS), and globally unique addresses. The IPv6 address space reduces the need for private addresses and Network Address Translation (NAT) processing by border routers at network edges.

This section describes IPv6 implementation on the router. These sections are included:

- IPv6 Addresses, page 1
- Supported IPv6 Unicast Routing Features, page 1

IPv6 Addresses

The IPv6 128-bit addresses are represented as a series of eight 16-bit hexadecimal fields separated by colons in the format: n:n:n:n:n:n:n:n. This is an example of an IPv6 address:

2031:0000:130F:0000:0000:09C0:080F:130B

For easier implementation, leading zeros in each field are optional. This is the same address without leading zeros:

2031:0:130F:0:0:9C0:80F:130B

You can also use two colons (::) to represent successive hexadecimal fields of zeros, but you can use this short version only once in each address:

2031:0:130F::09C0:080F:130B

Supported IPv6 Unicast Routing Features

These sections describe the IPv6 protocol features supported by the router:

- 128-Bit Wide Unicast Addresses, page 2
- DNS for IPv6, page 2
128-Bit Wide Unicast Addresses

The router supports aggregatable global unicast addresses, link-local unicast addresses, and Unique Local Address (ULA). It does not support site-local unicast addresses. ULA will replace it.

Aggregatable global unicast addresses are IPv6 addresses from the aggregatable global unicast prefix. The address structure enables strict aggregation of routing prefixes and limits the number of routing table entries in the global routing table. These addresses are used on links that are aggregated through organizations and eventually to the Internet service provider. These addresses are defined by a global routing prefix, a subnet ID, and an interface ID. Current global unicast address allocation uses the range of addresses that start with binary value 001 (2000::/3). Addresses with a prefix of 2000::/3(001) through E000::/3(111) must have 64-bit interface identifiers in the extended unique identifier (EUI)-64 format.

Link local unicast addresses can be automatically configured on any interface by using the link-local prefix FE80::/10(1111 1110 10) and the interface identifier in the modified EUI format. Link-local addresses are used in the neighbor discovery protocol (NDP) and the stateless auto-configuration process. Nodes on a local link use link-local addresses and do not require globally unique addresses to communicate. IPv6 routers do not forward packets with link-local source or destination addresses to other links.

Unique Local Address (ULA) is an IPv6 unicast address that is globally unique and is intended for local communications. They are not expected to be routable on the global Internet and are routable inside of a limited area, such as a site. They may also be routed between a limited set of sites, it addresses with a prefix of FC00::/7.

DNS for IPv6

IPv6 supports Domain Name System (DNS) record types in the DNS name-to-address and address-to-name lookup processes. The DNS AAAA resource record types support IPv6 addresses and are equivalent to an address record in IPv4. The router supports DNS resolution for IPv4 and IPv6.

The statically assigned DNS address has the highest priority than others dynamically assigned DNS address. The priority order in the system is static, IPsec, PPP0–PPP255 (L2TP, PPTP), PPPoE, DHCP, and DHCPv6.

ICMPv6

The Internet Control Message Protocol (ICMP) in IPv6 generates error messages, such as ICMP destination unreachable messages, to report errors during processing and other diagnostic functions. In IPv6, ICMP packets are also used in the neighbor discovery protocol and path MTU discovery.
Configuring IPv6

Neighbor Discovery

The router supports NDP for IPv6, a protocol running on top of ICMPv6, and static neighbor entries for IPv6 stations that
do not support NDP. The IPv6 neighbor discovery process uses ICMP messages and solicited-node multicast addresses
to determine the link-layer address of a neighbor on the same network (local link), to verify the reachability of the
neighbor, and to keep track of neighboring routers.

The router supports ICMPv6 redirect for routes with mask lengths less than 64 bits. ICMP redirect is not supported for
host routes or for summarized routes with mask lengths greater than 64 bits.

Default Router Preference

The router supports IPv6 default router preference (DRP), an extension in router advertisement messages. DRP improves
the ability of a host to select an appropriate router, especially when the host is multihomed and the routers are on different
links. The router does not support the Route Information Option in RFC 4191.

An IPv6 host maintains a default router list from which it selects a router for traffic to offlink destinations. The selected
router for a destination is then cached in the destination cache. NDP for IPv6 specifies that routers that are reachable or
probably reachable are preferred over routers whose reachability is unknown or suspect. For reachable or probably
reachable routers, NDP can either select the same router every time or cycle through the router list. By using DRP, you
can configure an IPv6 host to prefer one router over another, provided both are reachable or probably reachable.

IPv6 Stateless Autoconfiguration and Duplicate Address Detection

The router uses stateless autoconfiguration to manage link, subnet, and site addressing changes, such as management
of host and mobile IP addresses. A host autonomously configures its own link-local address, and booting nodes send
router solicitations to request router advertisements for configuring interfaces.

IPv6 Applications

The router has IPv6 support for these applications:

- Ping, traceroute, Telnet, and TFTP
- Secure Shell (SSH) over an IPv6 transport
- HTTP server access over IPv6 transport
- DNS resolver for AAAA over IPv4 transport
- SNMP support for IPv6

Static Routes for IPv6

Static routes are manually configured and define an explicit route between two networking devices. Static routes are
useful for smaller networks with only one path to an outside network or to provide security for certain types of traffic in
a larger network.

Dual IPv4 and IPv6 Protocol Stacks

When a device has dual stack capabilities, it can use both IPv4 and IPv6 technologies to connect to remote servers and
destinations in parallel.

Figure 1 shows a router forwarding both IPv4 and IPv6 traffic through the same interface, based on the IP packet and
destination addresses.
Configuring IPv6

Figure 1  Dual IPv4 and IPv6 Support on an Interface

DHCP for IPv6 Address Assignment

DHCPv6 enables DHCP servers to pass configuration parameters, such as IPv6 network addresses, to IPv6 clients. The address assignment feature manages nonduplicate address assignment in the correct prefix based on the network where the host is connected. Assigned addresses can be from one or multiple prefix pools. Additional options, such as default domain and DNS name-server address, can be passed back to the client. Address pools can be assigned for use on a specific interface, on multiple interfaces, or the server can automatically find the appropriate pool.

SNMP and Syslog Over IPv6

To support both IPv4 and IPv6, IPv6 network management requires both IPv6 and IPv4 transports. Syslog over IPv6 supports address data types for these transports.

SNMP and syslog over IPv6 provide these features:

- Support for both IPv4 and IPv6
- IPv6 transport for SNMP and to modify the SNMP agent to support traps for an IPv6 host
- SNMP- and syslog-related MIBs to support IPv6 addressing
- Configuration of IPv6 hosts as trap receivers

For support over IPv6, SNMP modifies the existing IP transport mapping to simultaneously support IPv4 and IPv6. These SNMP actions support IPv6 transport management:

- Opens User Datagram Protocol (UDP) SNMP socket with default settings
- Provides a new transport mechanism called \_SR_IPV6\_TRANSPORT
- sends SNMP notifications over IPv6 transport
- Supports SNMP-named access lists for IPv6 transport
- Supports SNMP proxy forwarding using IPv6 transport
- Verifies SNMP Manager feature works with IPv6 transport

HTTP(S) Over IPv6

The HTTP client sends requests to both IPv4 and IPv6 HTTP servers, which respond to requests from both IPv4 and IPv6 HTTP clients. URLs with literal IPv6 addresses must be specified in hexadecimal using 16-bit values between colons.
The accept socket call chooses an IPv4 or IPv6 address family. The accept socket is either an IPv4 or IPv6 socket. The listening socket continues to listen for both IPv4 and IPv6 signals that indicate a connection. The IPv6 listening socket is bound to an IPv6 wildcard address.

The underlying TCP/IP stack supports a dual-stack environment. HTTP relies on the TCP/IP stack and the sockets for processing network-layer interactions.

Basic network connectivity (ping) must exist between the client and the server hosts before HTTP connections can be made.

Configuring IPv6

These sections contain this IPv6 forwarding configuration information:

- Configuring IPv6 Addressing and Enabling IPv6 Routing
- Configuring DHCP for IPv6 Address Assignment
- Configuring Default Static Routes for IPv6

Configuring IPv6 Addressing and Enabling IPv6 Routing

This section describes how to assign IPv6 addresses to individual Layer 3 interfaces and to globally forward IPv6 traffic on the router.

In the `ipv6 address` interface configuration command, you must enter the `ipv6-address` and `ipv6-prefix` variables with the address specified in hexadecimal using 16-bit values between colons. The `prefix-length` variable (preceded by a slash `/`) is a decimal value that shows how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).

To forward IPv6 traffic on an interface, you must configure a global IPv6 address on that interface. Configuring an IPv6 address on an interface automatically configures a link-local address and activates IPv6 for the interface. The configured interface automatically joins these required multicast groups for that link:

- solicited-node multicast group FF02::1/104 for each unicast address assigned to the interface (this address is used in the neighbor discovery process.)
- all-nodes link-local multicast group FF02::1
- all-routers link-local multicast group FF02::2
Beginning in privileged EXEC mode, follow these steps to assign an IPv6 address to a Layer 3 interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2. interface interface-id</td>
<td>Enter interface configuration mode, and specify the Layer 3 interface to configure. The interface can be a physical interface, a router virtual interface (SVI), or a Layer 3 EtherChannel.</td>
</tr>
<tr>
<td>3. ipv6 address eui-64 ipv6-prefix/prefix length</td>
<td>Specify a global IPv6 address with an extended unique identifier (EUI) in the low-order 64 bits of the IPv6 address. Specify only the network prefix; the last 64 bits are automatically computed from the router MAC address.</td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>ipv6 address link-local ipv6-address</td>
<td>Specify a link-local address on the interface to be used instead of the link-local address that is automatically configured when IPv6 is enabled on the interface.</td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>ipv6 address autoconf</td>
<td>Specify automatic configuration of IPv6 addresses using stateless autoconfiguration on an interface and enables IPv6 processing on the interface.</td>
</tr>
<tr>
<td>4. exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td>5. exit</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>6. show ipv6 interface interface-id</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>7. copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To remove an IPv6 address from an interface, use the no ipv6 address ipv6-prefix/prefix length eui-64 or no ipv6 address link-local ipv6-address interface configuration command. To remove all manually configured IPv6 addresses from an interface, use the no ipv6 address interface configuration command without arguments.

This example shows how to enable IPv6 with both a link-local address and a global address based on the IPv6 prefix 2001:0DB8:c18:1::/64. The EUI-64 interface ID is used in the low-order 64 bits of both addresses. Output from the show ipv6 interface EXEC command shows how the interface ID (20B:46FF:FE2F:D940) is appexited to the link-local prefix FE80::/64 of the interface.

Router(config)# interface GigabitEthernet 0/1
Router(config-if)# ipv6 address eui-64 2001:0DB8:c18:1::/64
Router(config-if)# exit
Router# show ipv6 interface GigabitEthernet 0/1
GigabitEthernet 0/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::20B:46FF:FE2F:D940
Global unicast address(es):
2001:0DB8:c18:1:20B:46FF:FE2F:D940, subnet is 2001:0DB8:c18:1::/64 [EUI]
Joined group address(es):
FF02::1
FF02::2
FF02::1:FF2F:D940
MTU is 1500 bytes
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
Hosts use stateless autoconfig for addresses.
Configuring DHCP for IPv6 Address Assignment

These sections describe how to configure Dynamic Host Configuration Protocol for IPv6 (DHCPv6) address assignment:

- Enabling DHCPv6 Server Function
- Enabling DHCPv6 Client Function

Enabling DHCPv6 Server Function

See the “Configuring Stateful DHCPv6 Server” section on page -3 and “Configuring Stateless DHCPv6 Server” section on page -3 for detailed information about enabling DHCPv6 server function.

Enabling DHCPv6 Client Function

Beginning in privileged EXEC mode, follow these steps to enable DHCPv6 client function on an interface.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2. interface interface-id</td>
<td>Enter interface configuration mode, and specify the interface to configure.</td>
</tr>
<tr>
<td>3. ipv6 address dhcp</td>
<td>Enable the interface to acquire an IPv6 address from the DHCPv6 server.</td>
</tr>
<tr>
<td>4. exit</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>5. show ipv6 dhcp interface</td>
<td>Verify that the DHCPv6 client is enabled on an interface.</td>
</tr>
</tbody>
</table>

To disable the DHCPv6 client function, use the `no ipv6 address dhcp` interface configuration command.

This example shows how to acquire an IPv6 address:

```
Router(config)# interface gigabitethernet 0/1
Router(config-if)# ipv6 address dhcp
```
Configuring Default Static Routes for IPv6

Beginning in privileged EXEC mode, follow these steps to configure an IPv6 static route:

1. `configure terminal`
   - Enter global configuration mode.

2. `ipv6 route ::/0 {interface-type | interface-id [ipv6_next_hop_address]} [administrative_distance]`
   - Configure a static IPv6 route.
     - `interface-type`—Specify the interface type.
     - `ipv6_next_hop_address`—The IPv6 address of the next hop that can be used to reach the specified network. The IPv6 address of the next hop need not be directly connected; recursion is done to find the IPv6 address of the directly connected next hop. The address must be specified in hexadecimal using 16-bit values between colons.
     - `interface-id`—Specify direct static routes from point-to-point and broadcast interfaces. With point-to-point interfaces, there is no need to specify the IPv6 address of the next hop. With broadcast interfaces, you should always specify the IPv6 address of the next hop, or ensure that the specified prefix is assigned to the link, specifying a link-local address as the next hop. You can optionally specify the IPv6 address of the next hop to which packets are sent.
     - `administrative_distance`—(Optional) An administrative distance. The range is 1 to 254; the default value is 1, which gives static routes precedence over any other type of route except connected routes. To configure a floating static route, use an administrative distance greater than that of the dynamic routing protocol.

3. `exit`
   - Return to privileged EXEC mode.

4. `show ipv6 route`
   - Verify your entries by displaying the contents of the IPv6 routing table.

5. `copy running-config startup-config`
   - (Optional) Save your entries in the configuration file.

To remove a configured static route, use the `no ipv6 route` global configuration command.

This example shows how to configure a default static route with an administrative distance of 130 to an interface:

```
Router(config)# ipv6 route ::/0 gigabitethernet 0/1 130
```

Diagnosing IPv6 Connectivity

Table 20 shows the privileged EXEC commands for diagnosing IPv6 network connectivity on the router.
Configuring IPv6

The following example shows a sample output of the `ping ipv6` command:

```bash
Router# ping ipv6 2001:db8:2::1234 source 2001:db8:2:0:8a75:56ff:fe27:4d01
PING 2001:db8:2::1234 (2001:db8:2::1234) from 2001:db8:2:0:8a75:56ff:fe27:4d01: 56 data bytes
64 bytes from 2001:db8:2::1234: seq=0 ttl=64 time=0.825 ms
64 bytes from 2001:db8:2::1234: seq=1 ttl=64 time=0.714 ms
64 bytes from 2001:db8:2::1234: seq=2 ttl=64 time=0.682 ms
64 bytes from 2001:db8:2::1234: seq=3 ttl=64 time=0.652 ms
64 bytes from 2001:db8:2::1234: seq=4 ttl=64 time=0.687 ms
```

Displaying and Monitoring IPv6

Table 19 shows the privileged EXEC commands for monitoring IPv6 on the router.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ping ipv6 [hostname</td>
<td>ip_address] [repeat repeat-count</td>
</tr>
<tr>
<td></td>
<td>Ping a remote host through IPv6.</td>
</tr>
<tr>
<td></td>
<td>(Optional) Specify repeat count. Default is 5 times.</td>
</tr>
<tr>
<td></td>
<td>(Optional) Specify datagram size. Default is 56 bytes.</td>
</tr>
<tr>
<td></td>
<td>(Optional) Specify source address. Default is none.</td>
</tr>
<tr>
<td></td>
<td>Note If you ping IPv6 link-local at first time, the source option is required.</td>
</tr>
</tbody>
</table>

The following example shows a sample output of the `ping ipv6` command:

```bash
Router# ping ipv6 2001:db8:2::1234 source 2001:db8:2:0:8a75:56ff:fe27:4d01
PING 2001:db8:2::1234 (2001:db8:2::1234) from 2001:db8:2:0:8a75:56ff:fe27:4d01: 56 data bytes
64 bytes from 2001:db8:2::1234: seq=0 ttl=64 time=0.825 ms
64 bytes from 2001:db8:2::1234: seq=1 ttl=64 time=0.714 ms
64 bytes from 2001:db8:2::1234: seq=2 ttl=64 time=0.682 ms
64 bytes from 2001:db8:2::1234: seq=3 ttl=64 time=0.652 ms
64 bytes from 2001:db8:2::1234: seq=4 ttl=64 time=0.687 ms
```

Table 20 shows the privileged EXEC commands for monitoring IPv6 on the router.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show hosts</td>
<td>Display IPv4/IPv6 DNS server.</td>
</tr>
<tr>
<td>show ipv6 interface interface-id</td>
<td>Display IPv6 interface status and configuration.</td>
</tr>
<tr>
<td>show ipv6 neighbors</td>
<td>Display IPv6 neighbor cache entries.</td>
</tr>
<tr>
<td>show ipv6 prefix-list</td>
<td>Display a list of IPv6 prefix lists.</td>
</tr>
<tr>
<td>show ipv6 route</td>
<td>Display the IPv6 route table entries.</td>
</tr>
<tr>
<td>show ipv6 traffic</td>
<td>Display IPv6 traffic statistics.</td>
</tr>
<tr>
<td>show ip http server connection</td>
<td>Display the current connections to the HTTP server, including the local and remote IP addresses being accessed.</td>
</tr>
</tbody>
</table>

This is an example of the output from the `show ipv6 interface` privileged EXEC command:

```bash
Router# show ipv6 interface
Vlan1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::20B:46FF:FE2F:D940
Global unicast address(es):
    3FFE:CO00:0:1:20B:46FF:FE2F:D940, subnet is 3FFE:CO00:0:1::/64 [EUI]
Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF2F:D940
MTU is 1500 bytes
```
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
<output truncated>

This is an example of the output from the `show ipv6 neighbor` privileged EXEC command:

Router# `show ipv6 neighbors`  
IPv6 Address Interface Link-layer-Addr Device State  
fe80::20c:29ff:fe8c:27da gigabitethernet0/1 00:0c:29:8c:27:da router STALE

This is an example of the output from the `show ipv6 traffic` privileged EXEC command.

Router# `show ipv6 traffic`  
IPv6 statistics:  
Rcvd: 7 total  
0 truncated  
0 bad header, 0 bad source  
0 unknown protocol, 0 not a router  
0 total reassembled  
0 reassembly timeouts, 0 reassembly failures  
Sent: 8 generated, 0 forwarded  
0 no route,  
Mcast: 7 received, 14 sent

ICMP statistics:  
Rcvd: 7 input, 0 input error  
0 unreachable  
0 parameter problems  
0 too big  
0 echo request, 0 echo reply  
0 group query, 0 group report, 0 group reduce  
7 router solicit, 0 router advert, 0 redirects  
0 neighbor solicit, 0 neighbor advert  
Sent: 8 output  
0 unreachable  
0 parameter problems  
0 too big  
0 echo request, 0 echo reply  
0 group query, 0 group report, 0 group reduce  
0 router solicit, 0 router advert, 0 redirects  
2 neighbor solicit, 0 neighbor advert