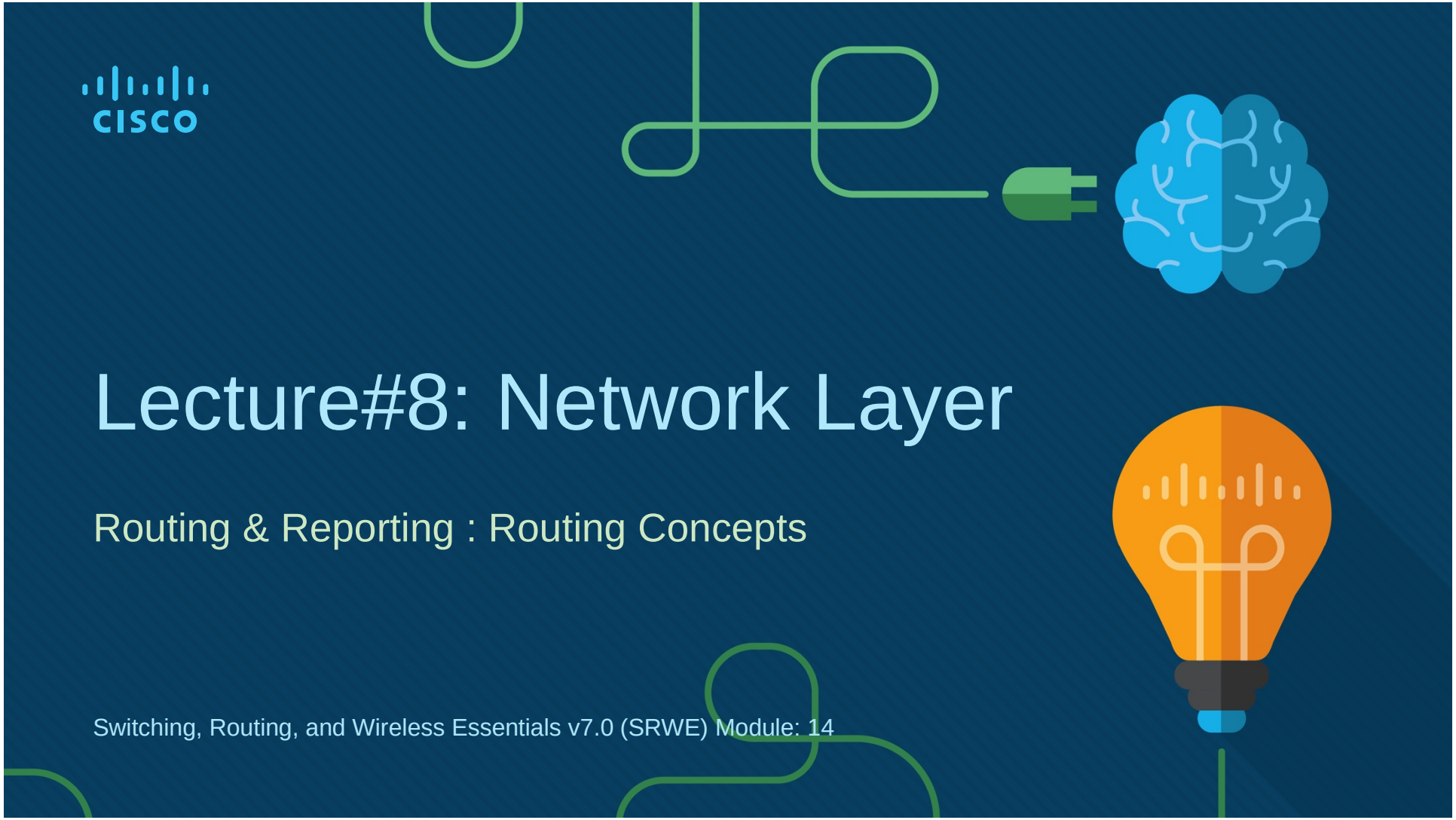


Lecture#8: Network Layer

Routing & Reporting : Routing Concepts

Switching, Routing, and Wireless Essentials v7.0 (SRWE) Module: 14

8.1.1 Path Determination

Path Determination

Two Functions of a Router

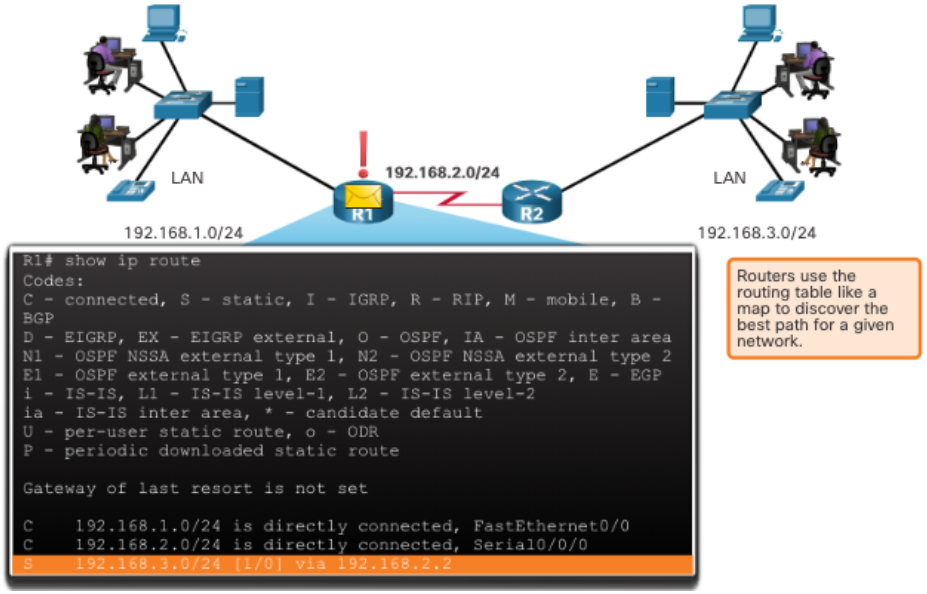
- When a router receives an IP packet on one interface, it determines which interface to use to forward the packet to the destination. This is known as **routing**.
  - The interface that the router uses to forward the packet may be the final destination, or it may be a network connected to another router that is used to reach the destination network.
  - Each network that a router connects to typically requires a separate interface, but this may not always be the case.
- The **primary function** of a router are to determine the best path to forward packets based on the information in its routing table, and to forward packets toward their destination.

Path Determination

Router Functions Example

The router uses its IP routing table to determine which path (route) to use to forward a packet.

- For example, R1 and R2 will use their respective IP routing tables to first determine the best path, and then forward the packet.



Best Path Equals Longest Match

The **best path** in the routing table is also known as the longest match.

- The routing table contains route entries consisting of a prefix (network address) and prefix length.
  - For there to be a match between the destination IP address of a packet and a route in the routing table, a minimum number of far-left bits must match between the IP address of the packet and the route in the routing table.
  - The prefix length of the route in the routing table is used to determine the minimum number of far-left bits that must match.
- The **longest match** is the route in the routing table that has the greatest number of far-left matching bits with the destination IP address of the packet. The longest match is always the **preferred route**.

***Note**: The term prefix length will be used to refer to the network portion of both IPv4 and IPv6 addresses.*

IPv4 Longest Match Example

In the table, an IPv4 packet has the destination IPv4 address 172.16.0.10. The router has three route entries in its IPv4 routing table that match this packet: 172.16.0.0/12, 172.16.0.0/18, and 172.16.0.0/26. Of the three routes, 172.16.0.0/26 has the longest match and would be chosen to forward the packet. For any of these routes to be considered a match there must be at least the number of matching bits indicated by the subnet mask of the route.

Destination IPv4 Address		**Address in Binary**
172.16.0.10		**10101100.00010000.00000000.00**001010
Route Entry	Prefix/Prefix Length	Address in Binary
1	172.16.0.0**/12**	**10101100.0001**0000.00000000.00001010
2	172.16.0.0**/18**	**10101100.00010000.00**000000.00001010
3	172.16.0.0**/26**	**10101100.00010000.00000000.00**001010

IPv6 Longest Match Example

An IPv6 packet has the destination IPv6 address 2001:db8:c000::99. This example shows three route entries, but only two of them are a valid match, with one of those being the longest match. The first two route entries have prefix lengths that have the required number of matching bits as indicated by the prefix length. The third route entry is not a match because its /64 prefix requires 64 matching bits.

Destination	**2001:db8:c000::99/48**	
Route Entry	Prefix/Prefix Length	Does it match?
1	**2001:db8:c0**00::**/40**	Match of 40 bits
2	**2001:db8:c000**::**/48**	Match of 48 bits (longest match)
3	**2001:db8:c000**:5555::**/64**	Does not match 64 bits

Path Determination

Build the Routing Table

- **Directly Connected Networks:** Added to the routing table when a local interface is configured with an IP address and subnet mask (prefix length) and is active (up and up).

- **Remote Networks:** Networks that are not directly connected to the router. Routers learn about remote networks in two ways:

  - **Static Routes** - Added to the routing table when a route is manually configured.
  - **Dynamic Routes** - Added to the routing table when routing protocols dynamically learn about the remote network.

Build the Routing Table (cont.)

- **Default Route:** Specifies a next-hop router to use when the routing table does not contain a specific route that matches the destination IP address. The default route can be entered manually as a static route, or learned automatically from a dynamic routing protocol.

- A default route has a /0 prefix length. This means that no bits need to match the destination IP address for this route entry to be used. If there are no routes with a match longer than 0 bits, the default route is used to forward the packet. The default route is sometimes referred to as a gateway of last resort.

8.1.2 Packet Forwarding

Packet Forwarding Decision Process

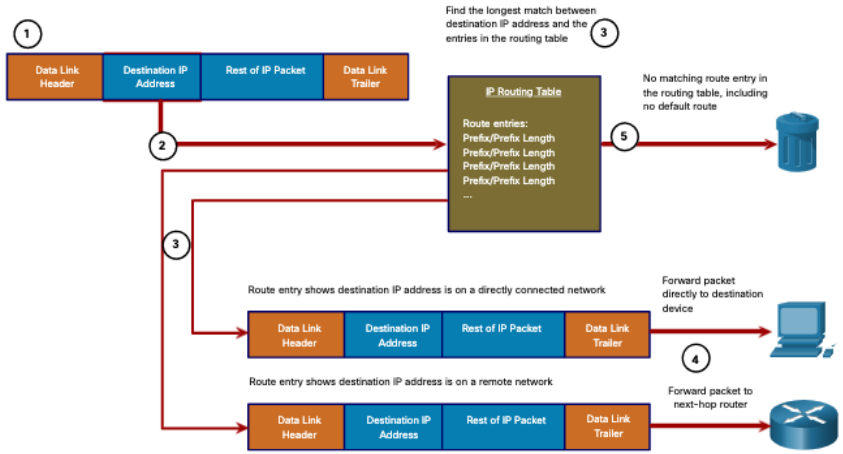
1) The data link frame with an encapsulated IP packet arrives on the ingress interface.

2) The router examines the destination IP address in the packet header and consults its IP routing table.

3) The router finds the longest matching prefix in the routing table.

4) The router encapsulates the packet in a data link frame and forwards it out the egress interface. The destination could be a device connected to the network or a next-hop router.

5) However, if there is no matching route entry the packet is dropped.



Packet Forwarding Decision Process (Cont.)

After a router has determined the best path, it could do the following:

1) Forward the Packet to a Device on a Directly Connected Network

- If the route entry indicates that the egress interface is a directly connected network, the packet can be forwarded directly to the destination device. Typically this is an Ethernet LAN.
- To encapsulate the packet in the Ethernet frame, the router needs to determine the destination MAC address associated with the destination IP address of the packet. The process varies based on whether the packet is an IPv4 or IPv6 packet.

2) Forward the Packet to a Next-Hop Router

- If the route entry indicates that the destination IP address is on a remote network,

Packet Forwarding Decision Process (Cont.)

meaning a device on network that is not directly connected. The packet must be forwarded to the next-hop router. The next-hop address is indicated in the route entry.

- If the forwarding router and the next-hop router are on an Ethernet network, a similar process (ARP and ICMPv6 Neighbor Discovery) will occur for determining the destination MAC address of the packet as described previously. The difference is that the router will search for the IP address of the next-hop router in its ARP table or neighbor cache, instead of the destination IP address of the packet.

3) Drop the Packet - No Match in Routing Table

- If there is no match between the destination IP address and a prefix in the routing table, and if there is no default route, the packet will be dropped

Packet Forwarding

End-to-End Packet Forwarding

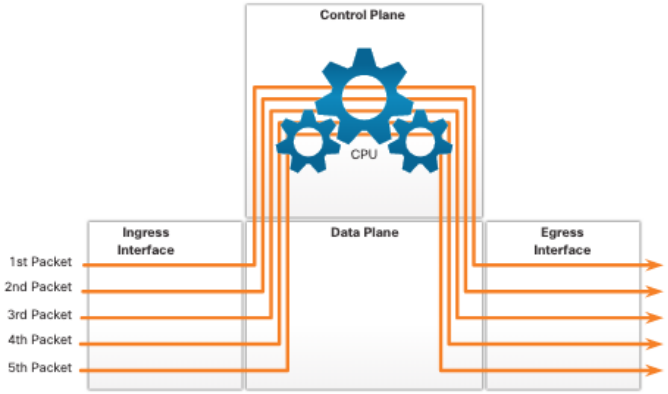
- The **primary responsibility** of the packet forwarding function is to encapsulate packets in the appropriate data link frame type for the outgoing interface.
  - For example, the data link frame format for a serial link could be Point-to-Point (PPP) protocol, High-Level Data Link Control (HDLC) protocol, or some other Layer 2 protocol.
  - The more efficiently a router can perform this task, the faster packets can be forwarded by the router.
- Routers support the following **three packet forwarding** mechanisms:
  - Process switching
  - Fast switching
  - Cisco Express Forwarding (CEF)

Packet Forwarding Mechanisms (Cont.)

Process Switching : An older packet forwarding mechanism still available for Cisco routers.

When a packet arrives on an interface,

- it is forwarded to the control plane where the CPU matches the destination address with an entry in its routing table, and
- then determines the exit interface and forwards the packet.



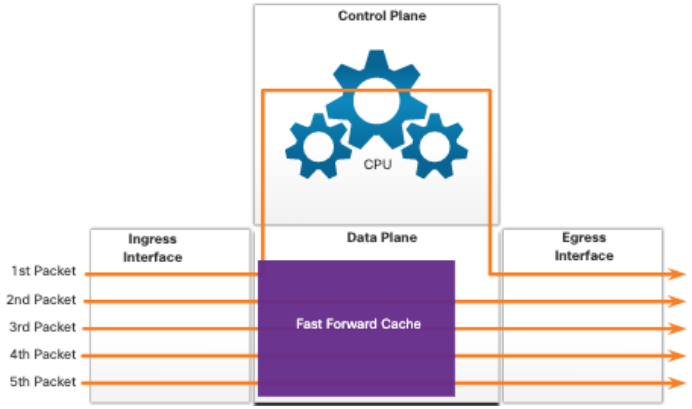
It is important to understand that the router does this for every packet, even if the destination is the same for a stream of packets.

Packet Forwarding Mechanisms (Cont.)

Fast Switching : Another, older packet forwarding mechanism which is the successor to process switching. Fast switching uses a fast-switching cache to store next-hop information.

When a packet arrives on an interface,

- It is forwarded to the control plane where the CPU searches for a match in the fast-switching cache.
- If it is not there, it is process-switched and forwarded to the exit interface.

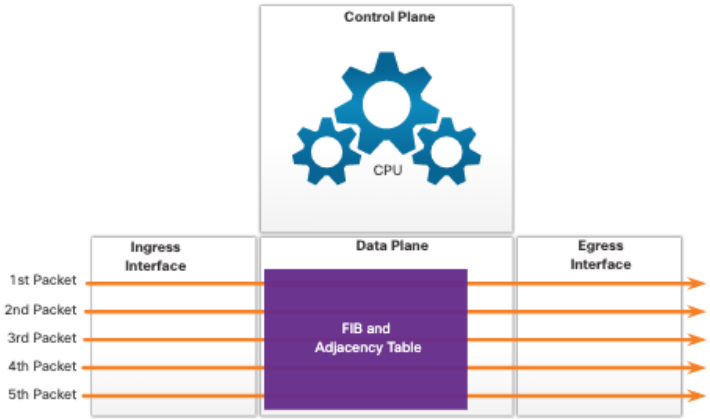


The flow information for the packet is then stored in the **fast-switching cache**. If another packet going to the same destination arrives on an interface, the next-hop information in the cache is **re-used** without CPU intervention.

Packet Forwarding Mechanisms (Cont.)

Cisco Express Forwarding (CEF) : The most recent and default Cisco IOS packet-forwarding mechanism. CEF builds a Forwarding Information Base (FIB), and an adjacency table.

- The table entries are not packet-triggered like fast switching but change-triggered, such as when something changes in the network topology.
- When a network has converged, the FIB and adjacency tables contain all the information that a router would have to consider when forwarding a packet.



8.1.3 IP Routing Table

IP Routing Table

Route Sources

A routing table contains a list of routes to known networks (prefixes and prefix lengths). The source of this information is derived from the following:

- Directly connected networks
- Static routes
- Dynamic routing protocols

The source for each route in the routing table is identified by a code. Common codes include the following:

- **L** - Identifies the address assigned to a router interface.
- **C** - Identifies a directly connected network.
- **S** - Identifies a static route created to reach a specific network.
- **O** - Identifies a dynamically learned network from another router using the OSPF routing protocol.
- ***** - This route is a candidate for a default route.

Routing Table Principles

There are **three routing table principles** as described in the table. These are issues that are addressed by the proper configuration of **dynamic routing protocols** or static routes on all the routers between the source and destination devices.

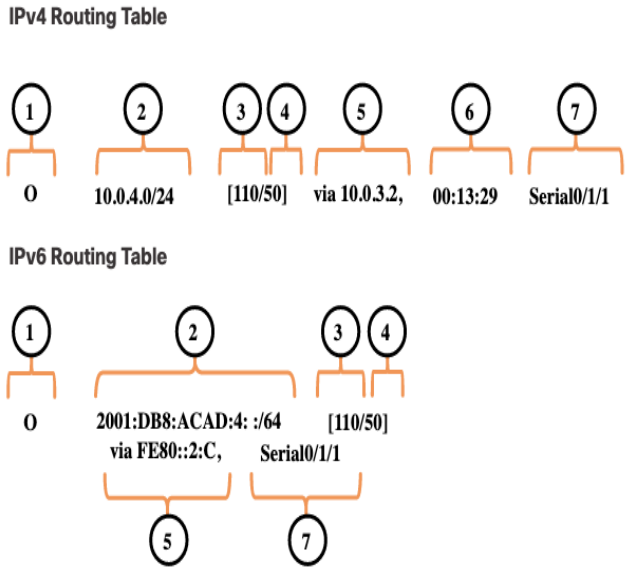
Routing Table Principle	Example
Every router makes its decision alone, based on the information it has in its own routing table.	•R1 can only forward packets using its own routing table. •R1 does not know what routes are in the routing tables of other routers (e.g., R2).
The information in a routing table of one router does not necessarily match the routing table of another router.	Just because R1 has route in its routing table to a network in the internet via R2, that does not mean that R2 knows about that same network.
Routing information about a path does not provide return routing information.	R1 receives a packet with the destination IP address of PC1 and the source IP address of PC3. Just because R1 knows to forward the packet out its G0/0/0 interface, doesn't necessarily mean that it knows how to forward packets originating from PC1 back to the remote network of PC3

IP Routing Table

Routing Table Entries

In the figure, the numbers identify the following information:

- **Route source** - This identifies how the route was learned.
- **Destination network (prefix and prefix length)** - This identifies the address of the remote network.
- **Administrative distance** - This identifies the trustworthiness of the route source. Lower values indicate preferred route source.
- **Metric** - This identifies the value assigned to reach the remote network. Lower values indicate preferred routes.
- **Next-hop** - This identifies the IP address of the next router to which the packet would be forwarded.
- **Route timestamp** - This identifies how much time has passed since the route was learned.
- **Exit interface** - This identifies the egress interface to use for outgoing packets to reach their final destination.



***Note**: The prefix length of the destination network specifies the minimum number of far-left bits that must match between the IP address of the packet and the destination network (prefix) for this route to be used.*

IP Routing Table

Directly Connected Networks

To learn about any remote networks, the router must have at least one active interface configured with an IP address and subnet mask (prefix length). This is known as a ***directly connected network*** or a ***directly connected route***.

Routers add a directly connected route to its routing table when an interface is configured with an IP address and is activated.

- A directly connected network is denoted by a status code of **C** in the routing table. The route contains a network prefix and prefix length.
- The routing table also contains a local route for each of its directly connected networks, indicated by the status code of **L**.
- For IPv4 local routes the prefix length is /32 and for IPv6 local routes the prefix length is /128. This means the destination IP address of the packet must match all the bits in the local route for this route to be a match. The purpose of the local route is to efficiently determine when it receives a packet for the interface instead of a packet that needs to be forwarded.

IP Routing Table

Static Routes

After directly connected interfaces are configured and added to the routing table, static or dynamic routing can be implemented for accessing remote networks. **Static routes** are **manually configured**.

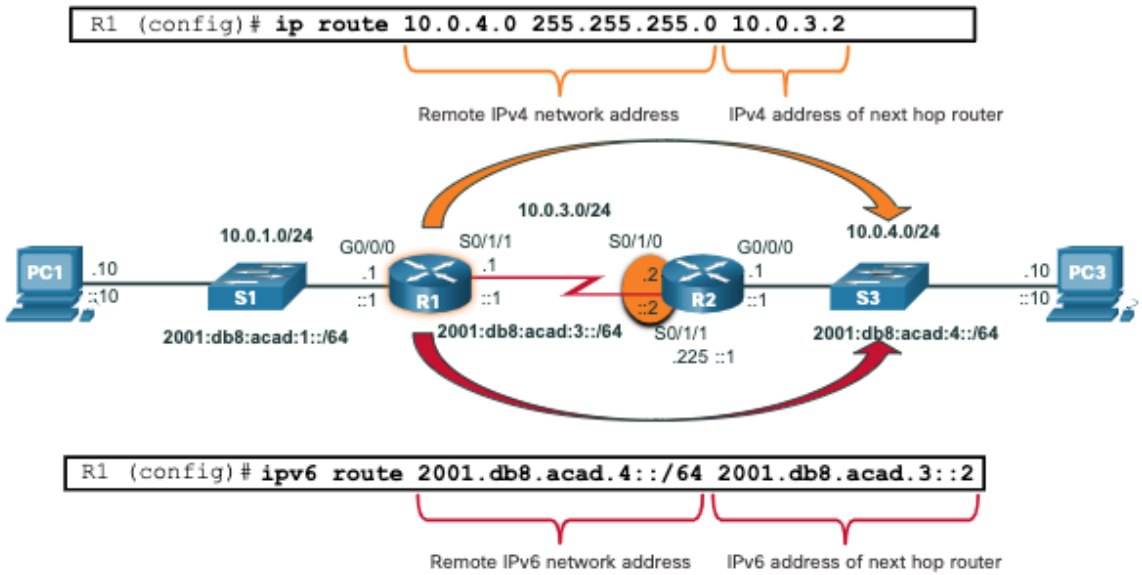
- They define an explicit path between two networking devices.
- They are not automatically updated and must be manually reconfigured if the network topology changes.

Static routing has **three primary uses**:

- It provides ease of routing table maintenance in smaller networks that are not expected to grow significantly.
- It uses a single default route to represent a path to any network that does not have a more specific match with another route in the routing table. Default routes are used to send traffic to any destination beyond the next upstream router.
- It routes to and from stub networks. A stub network is a network accessed by a single route, and the router has only one neighbor.

Static Routes in the IP Routing Table

The topology in the figure is simplified to show only one LAN attached to each router. The figure shows IPv4 and IPv6 static routes configured on R1 to reach the 10.0.4.0/24 and 2001:db8:acad:4::/64 networks on R2.

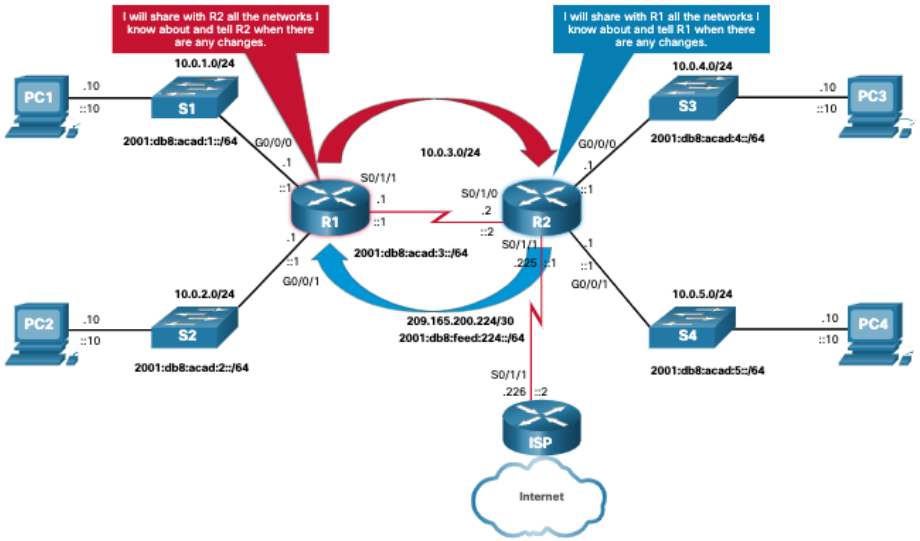


Dynamic Routing Protocols

Dynamic routing protocols are used by routers to **automatically share information** about the reachability and status of remote networks.

Dynamic routing protocols perform several activities, including

- **network discovery** and
- **maintaining routing tables**



IP Routing Table

Dynamic Routes in the Routing Table

OSPF is now being used in our sample topology to dynamically learn all the networks connected to R1 and R2. The routing table entries use the status code of **O** to indicate the route was learned by the OSPF routing protocol. Both entries also include the IP address of the next-hop router, via *ip-address*.

Note: IPv6 routing protocols use the link-local address of the next-hop router.

Note: OSPF routing configuration for IPv4 and IPv6 is beyond the scope of this course.

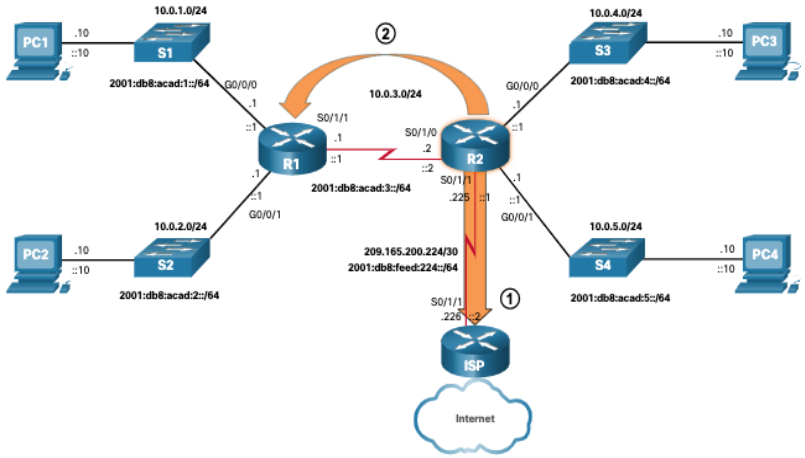
```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP D - EIGRP,
EX - EIGRP external, O - OSPF, IA - OSPF inter area
(output omitted for brevity)
O 10.0.4.0/24 [110/50] via 10.0.3.2, 00:24:22, Serial0/1/1
O 10.0.5.0/24 [110/50] via 10.0.3.2, 00:24:15, Serial0/1/1
R1# show ipv6 route
IPv6 Routing Table - default - 10 entries
(Output omitted)
NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
O 2001:DB8:ACAD:4::/64 [110/50]
   via FE80::2:C, Serial0/1/1
O 2001:DB8:ACAD:5::/64 [110/50]
   via FE80::2:C, Serial0/1/1
```

IP Routing Table

Default Route

The **default route** specifies a next-hop router to use when the routing table does not contain a specific route that matches the destination IP address.

- A default route can be either a static route or learned automatically from a dynamic routing protocol.
- A default route has an IPv4 route entry of 0.0.0.0/0 or an IPv6 route entry of ::/0. This means that zero or no bits need to match between the destination IP address and the default route.



IP Routing Table

Structure of an IPv4 Routing Table

IPv4 was standardized using the now **obsolete classful addressing** architecture. The IPv4 routing table is organized using this same classful structure.

Although the lookup process no longer uses classes, the structure of the IPv4 routing table still retains in this format.

- An **indented entry** is known as a child route. A route entry is indented if it is the subnet of a classful address (class A, B or C network).
- **Directly connected** networks will always be indented (child routes) because the local address of the interface is always entered in the routing table as a /32.
- The **child route** will include the route source and all the forwarding information such as the next-hop address. The classful network address of this subnet will be shown above the route entry, less indented, and without a source code. That route is known as a **parent route**.

IP Routing Table

Structure of an IPv4 Routing Table

- An indented entry is known as a **child route**. A route entry is indented if it is the subnet of a classful address (class A, B or C network).
- Directly connected networks will always be indented (child routes) because the local address of the interface is always entered in the routing table as a /32.
- The child route will include the route source and all the forwarding information such as the next-hop address.
- The classful network address of this subnet will be shown above the route entry, less indented, and without a source code. That route is known as a **parent route.**

```
Router# show ip route
(Output omitted)
   192.168.1.0/24 is variably..
C     192.168.1.0/24 is direct..
L     192.168.1.1/32 is direct..
O     192.168.2.0/24 [110/65]..
O     192.168.3.0/24 [110/65]..
   192.168.12.0/24 is variab..
C     192.168.12.0/30 is direct..
L     192.168.12.1/32 is direct..
   192.168.13.0/24 is variably..
C     192.168.13.0/30 is direct..
L     192.168.13.1/32 is direct..
   192.168.23.0/30 is subnette..
O     192.168.23.0/30 [110/128]..
Router#
```

IP Routing Table

Structure of an IPv6 Routing Table

The concept of classful addressing was never part of IPv6, so the structure of an IPv6 routing table is very straight forward. Every IPv6 route entry is formatted and aligned the same way.

```
R1# show ipv6 route
(output omitted for brevity)
OE2 ::/0 [110/1], tag 2
   via FE80::2:C, Serial0/0/1
C 2001:DB8:ACAD:1::/64 [0/0]
   via GigabitEthernet0/0/0, directly connected
L 2001:DB8:ACAD:1::1/128 [0/0]
   via GigabitEthernet0/0/0, receive
C 2001:DB8:ACAD:2::/64 [0/0]
  via GigabitEthernet0/0/1, directly connected
L 2001:DB8:ACAD:2::1/128 [0/0]
   via GigabitEthernet0/0/1, receive
C 2001:DB8:ACAD:3::/64 [0/0]
   via Serial0/1/1, directly connected
L 2001:DB8:ACAD:3::1/128 [0/0]
   via Serial0/1/1, receive
O 2001:DB8:ACAD:4::/64 [110/50]
   via FE80::2:C, Serial0/1/1
O 2001:DB8:ACAD:5::/64 [110/50]
   via FE80::2:C, Serial0/1/1
L FF00::/8 [0/0]
   via Null0, receive
R1#
```

IP Routing Table

Administrative Distance

A route entry for a specific network address (prefix and prefix length) can only appear once in the routing table. However, it is possible that the routing table learns about the same network address from more than one routing source. Except for very specific circumstances, only one dynamic routing protocol should be implemented on a router. Each routing protocol may decide on a different path to reach the destination based on the metric of that routing protocol.

This raises a few questions, such as the following:

- How does the router know which source to use?
- Which route should it install in the routing table?

Cisco IOS uses what is known as the administrative distance (AD) to determine the route to install into the IP routing table. The AD represents the "trustworthiness" of the route. The lower the AD, the more trustworthy the route source.

IP Routing Table

Administrative Distance (Cont.)

The table lists various routing protocols and their associated ADs.

Route Source	Administrative Distance
Directly connected	0
Static route	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
OSPF	110
IS-IS	115
RIP	120
External EIGRP	170
Internal BGP	200

8.1.4 Static and Dynamic Routing

Static or Dynamic?

Static and **dynamic** routing are **not mutually exclusive**. Rather, most networks use a combination of dynamic routing protocols and static routes.

Static routes are commonly used in the following scenarios:

- As a default route forwarding packets to a service provider
- For routes outside the routing domain and not learned by the dynamic routing protocol
- When the network administrator wants to explicitly define the path for a specific network
- For routing between stub networks

Static routes are useful for smaller networks with only one path to an outside network. They also provide security in a larger network for certain types of traffic, or links to other networks that need more control.

Static or Dynamic? (Cont.)

Dynamic routing protocols are implemented in any type of network consisting of more than just a few routers.

- Dynamic routing protocols are **scalable** and **automatically** determine better routes if there is a change in the topology.

Dynamic routing protocols are commonly used in the following scenarios:

- In networks consisting of more than just a few routers
- When a change in the network topology requires the network to automatically determine another path
- For scalability. As the network grows, the dynamic routing protocol automatically learns about any new networks.

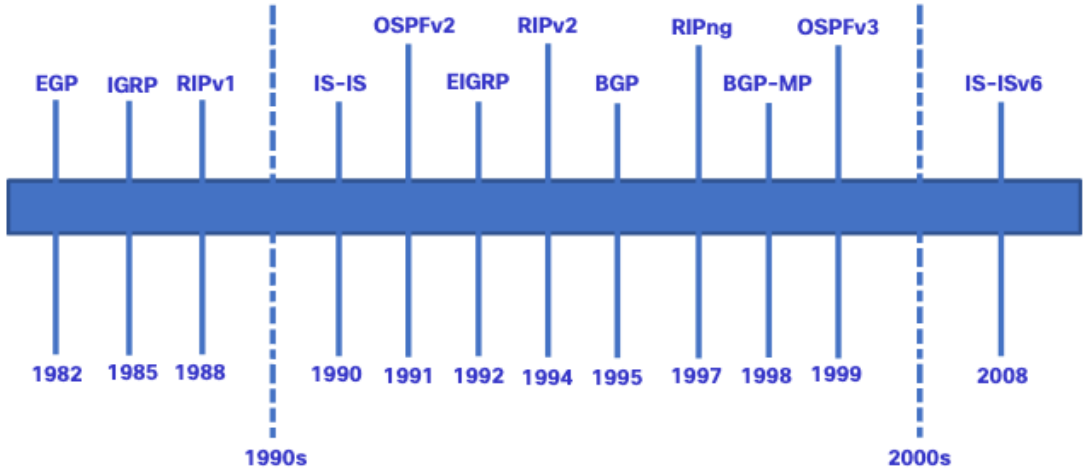
Static or Dynamic? (Cont.)

The table shows a comparison of some the differences between dynamic and static routing.

Feature	Dynamic Routing	Static Routing
Configuration complexity	Independent of network size	Increases with network size
Topology changes	Automatically adapts to topology changes	Administrator intervention required
Scalability	Suitable for simple to complex network topologies	Suitable for simple topologies
Security	Security must be configured	Security is inherent
Resource Usage	Uses CPU, memory, and link bandwidth	No additional resources needed
Path Predictability	Route depends on topology and routing protocol used	Explicitly defined by the administrator

Dynamic Routing Evolution

Dynamic routing protocols have been used in networks since the late 1980s. One of the first routing protocols was RIP. RIPv1 was released in 1988, but some of the basic algorithms within the protocol were used on the Advanced Research Projects Agency Network (ARPANET) as early as 1969. As networks evolved and became more complex, new routing protocols emerged.



Dynamic Routing Evolution (Cont.)

The table classifies the current routing protocols. Interior Gateway Protocols (IGPs) are routing protocols used to exchange routing information within a routing domain administered by a single organization. There is only one EGP and it is BGP. BGP is used to exchange routing information between different organizations, known as autonomous systems (AS). BGP is used by ISPs to route packets over the internet. Distance vector, link-state, and path vector routing protocols refer to the type of routing algorithm used to determine best path.

	Interior Gateway Protocols				**Exterior Gateway Protocols**
	Distance Vector		Link-State		Path Vector
IPv4	RIPv2	EIGRP	OSPFv2	IS-IS	BGP-4
IPv6	RIPng	EIGRP for IPv6	OSPFv3	IS-IS for IPv6	BGP-MP

Dynamic Routing Protocol Concepts

A **routing protocol** is a set of processes, algorithms, and messages that are used to exchange routing information and populate the routing table with the choice of best paths.

The **purpose** of dynamic routing protocols includes the following:

- **Discovery** of remote networks
- **Maintaining** up-to-date routing information
- **Choosing** the best path to destination networks
- **Find** a new best path if the current path is no longer available

Dynamic Routing Protocol Concepts (Cont.)

The main components of dynamic routing protocols include the following:

- **Data structures -** Routing protocols typically use tables or databases for their operations. This information is kept in RAM.
- **Routing protocol messages -** Routing protocols use various types of messages to discover neighboring routers, exchange routing information, and other tasks to learn and maintain accurate information about the network.
- **Algorithm -** An algorithm is a finite list of steps used to accomplish a task. Routing protocols use algorithms for facilitating routing information and for the best path determination.

Routing protocols determine the best path, or route, to each network. That route is then offered to the routing table. The route will be installed in the routing table if there is not another routing source with a lower AD.

Best Path

The **best path** is selected by a routing protocol based on the value or metric it uses to determine the distance to reach a network. A metric is the quantitative value used to measure the distance to a given network. The best path to a network is the path with the lowest metric.

Dynamic routing protocols typically use their own rules and metrics to build and update routing tables. The following table lists common dynamic protocols and their metrics.

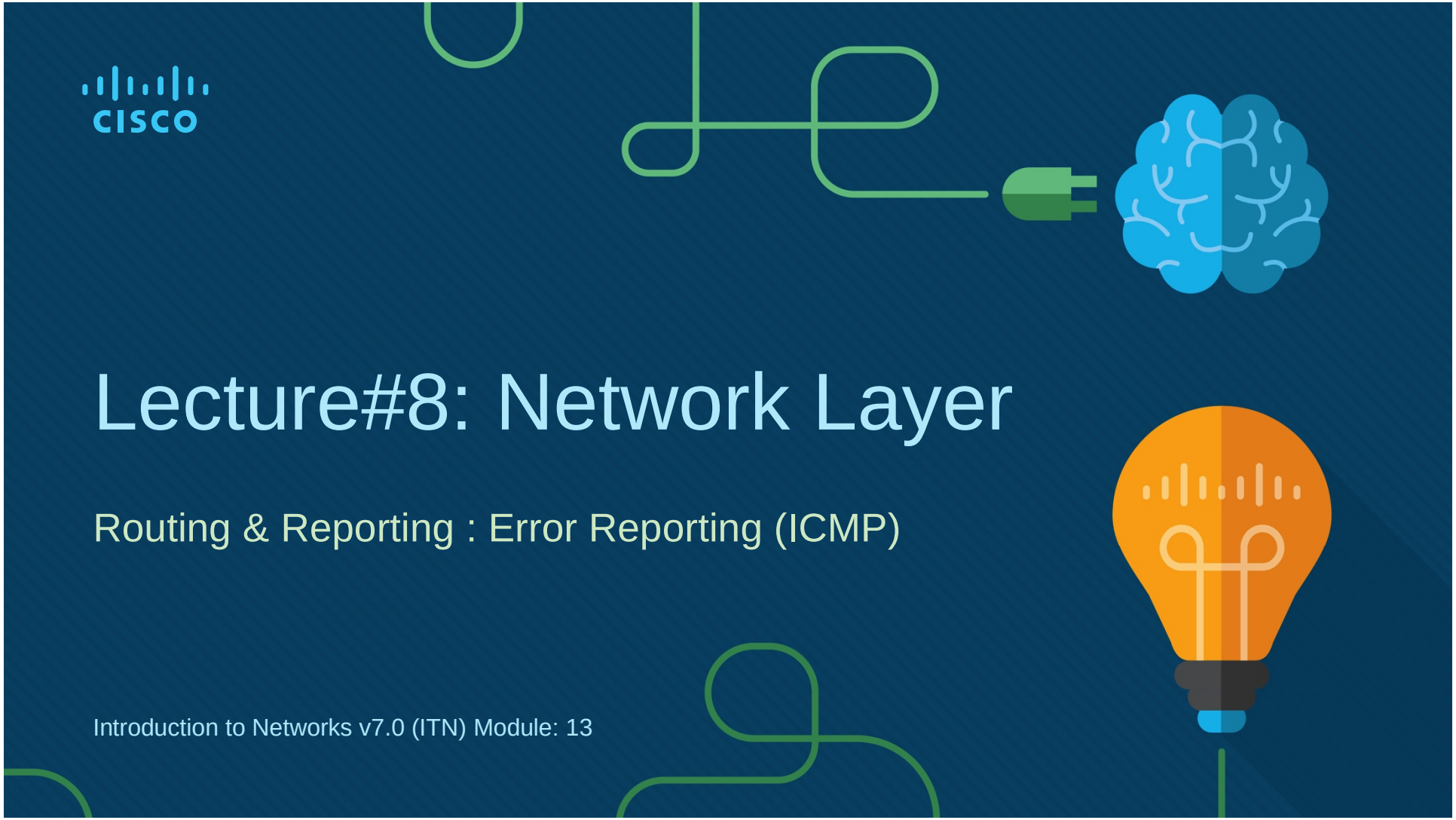
Routing Protocol	Metric
Routing Information Protocol (RIP)	•The metric is “hop count”. •Each router along a path adds a hop to the hop count. •A maximum of 15 hops allowed.
Open Shortest Path First (OSPF)	•The metric is “cost” which is the based on the cumulative bandwidth from source to destination. •Faster links are assigned lower costs compared to slower (higher cost) links.
Enhanced Interior Gateway Routing Protocol (EIGRP)	•It calculates a metric based on the slowest bandwidth and delay values. •It could also include load and reliability into the metric calculation.

Load Balancing

When a router has two or more paths to a destination with equal cost metrics, then the router forwards the packets using both paths equally. This is called equal cost load balancing.

- The routing table contains the single destination network, but has multiple exit interfaces, one for each equal cost path. The router forwards packets using the multiple exit interfaces listed in the routing table.
- If configured correctly, load balancing can increase the effectiveness and performance of the network.
- Equal cost load balancing is implemented automatically by dynamic routing protocols. It is enabled with static routes when there are multiple static routes to the same destination network using different next-hop routers.

Note: Only EIGRP supports unequal cost load balancing.



Lecture#8: Network Layer

Routing & Reporting : Error Reporting (ICMP)

Introduction to Networks v7.0 (ITN) Module: 13

8.2.1 ICMP Messages

ICMP Messages

ICMPv4 and ICMPv6 Messages

- **Internet Control Message Protocol** (ICMP) provides **feedback** about issues related to the processing of IP packets under certain conditions.
  - ICMPv4 is the messaging protocol for IPv4.
  - ICMPv6 is the messaging protocol for IPv6 and includes additional functionality.

- The ICMP messages common to both ICMPv4 and ICMPv6 including:
  - Host reachability, Destination or Service Unreachable, Time exceeded

Note: ICMPv4 messages are not required and are often not allowed within a network for security reasons.

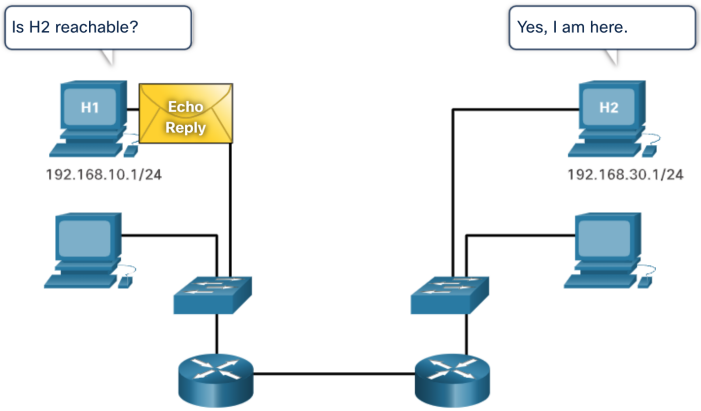
ICMP Messages

Host Reachability

ICMP Echo Message can be used to test the reachability of a host on an IP network.

In the example:

- The local host sends an **ICMP Echo Request** to a host.
- If the host is available, the destination host responds with an **Echo Reply**.



ICMP Messages

Destination or Service Unreachable

- An ICMP **Destination Unreachable message** can be used to notify the source that a destination or service is unreachable.
- The ICMP message will include a code indicating why the packet could not be delivered.

A few Destination Unreachable codes for ICMPv4 are :

- 0 - Net unreachable
- 1 - Host unreachable
- 2 - Protocol unreachable
- 3 - Port unreachable

A few Destination Unreachable codes for ICMPv6 are :

- 0 - No route to destination
- 1 - Communication with the destination is administratively prohibited (e.g., firewall)
- 2 – Beyond scope of the source address
- 3 - Address unreachable
- 4 - Port unreachable

- **Note**: ICMPv6 has similar but slightly different codes for Destination Unreachable messages.

ICMP Messages

Time Exceeded

- When the **Time to Live** (TTL) field in a packet is decremented to 0, an ICMPv4 Time Exceeded message will be sent to the source host.
- ICMPv6 also sends a Time Exceeded message. Instead of the IPv4 TTL field, ICMPv6 uses the IPv6 Hop Limit field to determine if the packet has expired.

```
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 192.168.1.1: TTL expired in transit.
Reply from 192.168.1.1: TTL expired in transit.
Reply from 192.168.1.1: TTL expired in transit.
Reply from 192.168.1.1: TTL expired in transit.

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

- **Note**: Time Exceeded messages are used by the **traceroute** tool.

ICMPv6 Messages

ICMPv6 has new features and improved functionality not found in ICMPv4, including four new protocols as part of the Neighbor Discovery Protocol (ND or NDP).

Messaging between an IPv6 router and an IPv6 device, including dynamic address allocation are as follows:

- Router Solicitation (RS) message
- Router Advertisement (RA) message

Messaging between IPv6 devices, including duplicate address detection and address resolution are as follows:

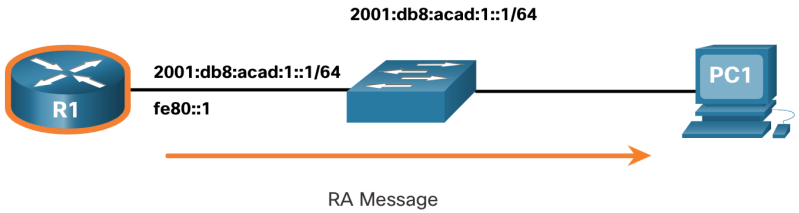
- Neighbor Solicitation (NS) message
- Neighbor Advertisement (NA) message

Note: ICMPv6 ND also includes the redirect message, which has a similar function to the redirect message used in ICMPv4.

ICMPv6 Messages (Cont.)

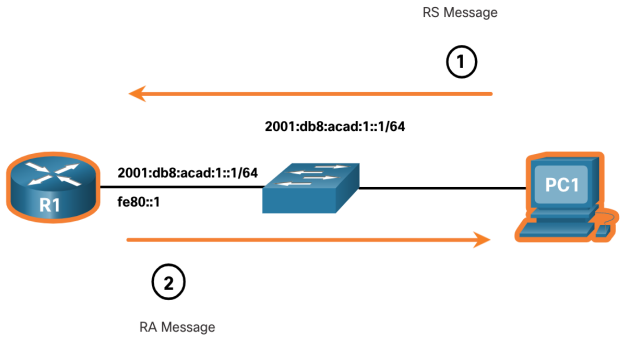
- RA messages are sent by IPv6-enabled routers every 200 seconds to provide addressing information to IPv6-enabled hosts.

- RA message can include addressing information for the host such as the prefix, prefix length, DNS address, and domain name.
- A host using Stateless Address Autoconfiguration (SLAAC) will set its default gateway to the link-local address of the router that sent the RA.



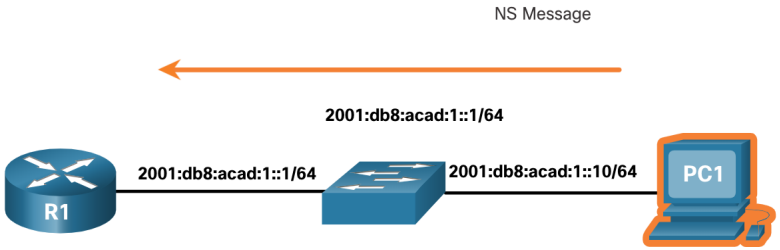
ICMPv6 Messages (Cont.)

- An IPv6-enabled router will also send out an RA message in response to an RS message.
- In the figure, PC1 sends a RS message to determine how to receive its IPv6 address information dynamically.
  - R1 replies to the RS with an RA message.
  - PC1 sends an RS message, “Hi, I just booted up. Is there an IPv6 router on the network? I need to know how to get my IPv6 address information dynamically.”
  - R1 replies with an RA message. “Hi all IPv6-enabled devices. I’m R1 and you can use SLAAC to create an IPv6 global unicast address. The prefix is 2001:db8:acad:1::/64. By the way, use my link-local address fe80::1 as your default gateway."



ICMPv6 Messages (Cont.)

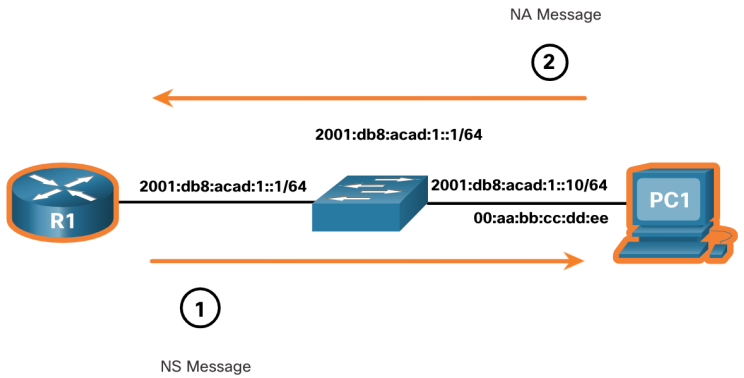
- A device assigned a global IPv6 unicast or link-local unicast address, may perform duplicate address detection (DAD) to ensure that the IPv6 address is unique.
- To check the uniqueness of an address, the device will send an NS message with its own IPv6 address as the targeted IPv6 address.
- If another device on the network has this address, it will respond with an NA message notifying to the sending device that the address is in use.



***Note**: DAD is not required, but RFC 4861 recommends that DAD is performed on unicast addresses.*

ICMPv6 Messages (Cont.)

- To determine the MAC address for the destination, the device will send an NS message to the solicited node address.
- The message will include the known (targeted) IPv6 address. The device that has the targeted IPv6 address will respond with an NA message containing its Ethernet MAC address.
- In the figure, R1 sends a NS message to 2001:db8:acad:1::10 asking for its MAC address.



8.2.2 Ping and Traceroute Tests

Ping – Test Connectivity

- The **ping** command is an IPv4 and IPv6 testing utility that uses ICMP echo request and echo reply messages to test connectivity between hosts and provides a summary that includes the success rate and average round-trip time to the destination.

- If a reply is not received within the timeout, ping provides a message indicating that a response was not received.

```
S1#ping 192.168.20.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms
```

- It is common for the first ping to timeout if address resolution (ARP or ND) needs to be performed before sending the ICMP Echo Request.

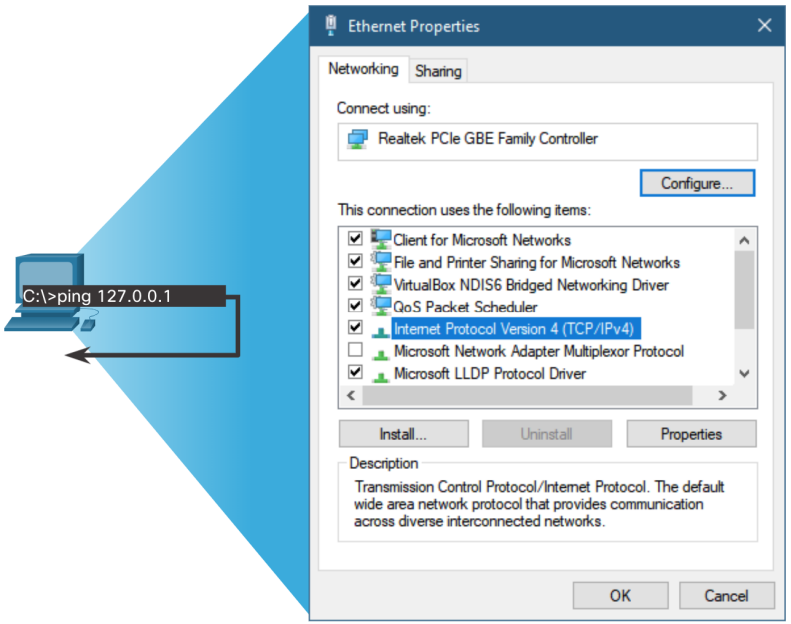
```
R1#ping 2001:db8:acad:1::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:acad:1::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Ping the Loopback

Ping can be used to test the internal configuration of IPv4 or IPv6 on the local host. To do this, **ping** the local loopback address of 127.0.0.1 for IPv4 (::1 for IPv6).

- A response from 127.0.0.1 for IPv4, or ::1 for IPv6, indicates that IP is properly installed on the host.
- An error message indicates that TCP/IP is not operational on the host.

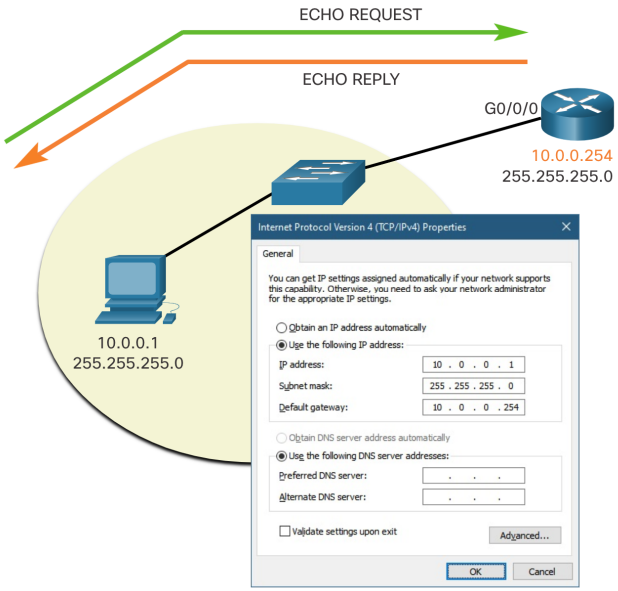


Ping the Default Gateway

The **ping** command can be used to test the ability of a host to communicate on the local network.

The default gateway address is most often used because the router is normally always operational.

- A successful **ping** to the default gateway indicates that the host and the router interface serving as the default gateway are both operational on the local network.
- If the default gateway address does not respond, a **ping** can be sent to the IP address of another host on the local network that is known to be operational.

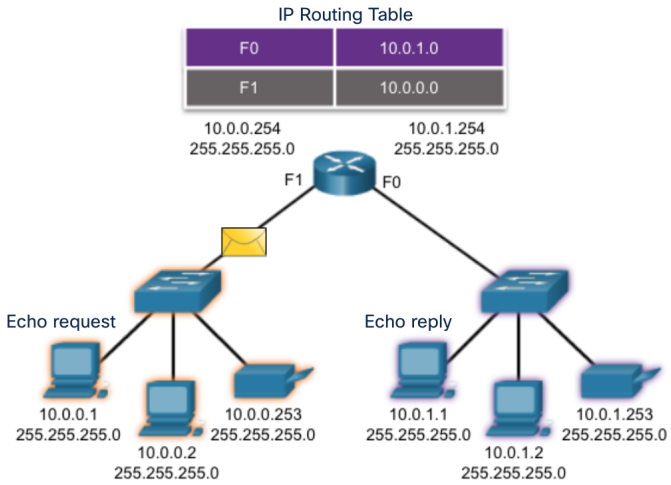


Ping a Remote Host

Ping can also be used to test the ability of a local host to communicate across an internetwork.

- A local host can ping a host on a remote network. A successful **ping** across the internetwork confirms communication on the local network.

Note: Many network administrators limit or prohibit the entry of ICMP messages therefore, the lack of a **ping** response could be due to security restrictions.



Traceroute – Test the Path

- Traceroute (**tracert**) is a utility that is used to test the path between two hosts and provide a list of hops that were successfully reached along that path.
- Traceroute provides round-trip time for each hop along the path and indicates if a hop fails to respond. An asterisk (*) is used to indicate a lost or unreplied packet.
- This information can be used to locate a problematic router in the path or may indicate that the router is configured not to reply.

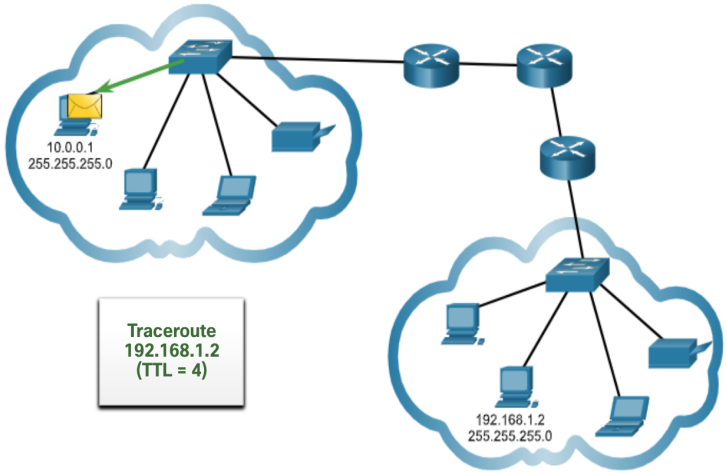
```
R1#traceroute 192.168.40.2
Type escape sequence to abort.
Tracing the route to 192.168.40.2

  1   192.168.10.2    1 msec    0 msec    0 msec
  2   192.168.20.2    2 msec    1 msec    0 msec
  3   192.168.30.2    1 msec    0 msec    0 msec
  4   192.168.40.2    0 msec    0 msec    0 msec
```

- **Note**: Traceroute makes use of a function of the TTL field in IPv4 and the Hop Limit field in IPv6 in the Layer 3 headers, along with the ICMP Time Exceeded message.

Traceroute – Test the Path (Cont.)

- The first message sent from traceroute will have a TTL field value of 1. This causes the TTL to time out at the first router. This router then responds with a ICMPv4 Time Exceeded message.
- Traceroute then progressively increments the TTL field (2, 3, 4...) for each sequence of messages. This provides the trace with the address of each hop as the packets time out further down the path.
- The TTL field continues to be increased until the destination is reached, or it is incremented to a predefined maximum.



Ping and Traceroute Tests

Packet Tracer – Verify IPv4 and IPv6 Addressing

In this Packet Tracer, you will do the following:

- Complete the Addressing Table Documentation
- Test Connectivity Using Ping
- Discover the Path by Tracing the Route

Ping and Traceroute Tests

Packet Tracer – Use Ping and Traceroute to Test Network Connectivity

In this Packet Tracer, you will do the following:

- Test and Restore IPv4 Connectivity
- Test and Restore IPv6 Connectivity


CISCO