CCNA 200-301

IP Connectivity

Exam Topics

- ARP Operation
- Route Selection
- Frame Rewrite
- IPv4 Static Routing
- IPv4 Default Routing
- IPv4 Floating Static Route
- IPv6 Static Routing
- IPv6 Default Routing

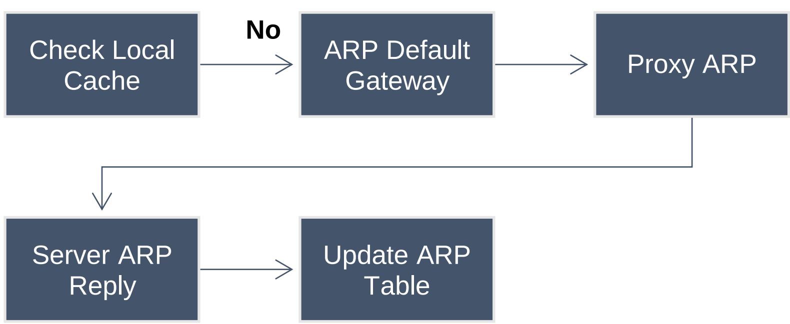
Address Resolution Protocol

The purpose of ARP is to resolve (learn) an unknown MAC address from a known IP address. The host endpoint must know the MAC address of a remote server endpoint before data can be sent. That is required for frame rewrite at all router hops between endpoints. ARP is a foundational network addressing protocol that is part of IP protocol suite. Layer 3 hop is any network device that provides routing services.

The host endpoint first checks for an entry in the local ARP cache that has the server MAC address. The host sends an ARP request to the default gateway if there is no entry in the local ARP cache.

The default gateway then sends a proxy ARP broadcast toward the server. It is an ARP request sent on behalf of the host. Each router hop then broadcasts an ARP request on their local subnet until it arrives at the server. The server sends an ARP reply with the MAC address assigned to server Ethernet network interface. The default gateway receives the ARP reply and updates its local ARP table. In fact, all Layer 3 network devices between endpoints update their ARP table as well. Layer 2 switches in the forwarding path also update their MAC address table.

Figure 1 ARP Process

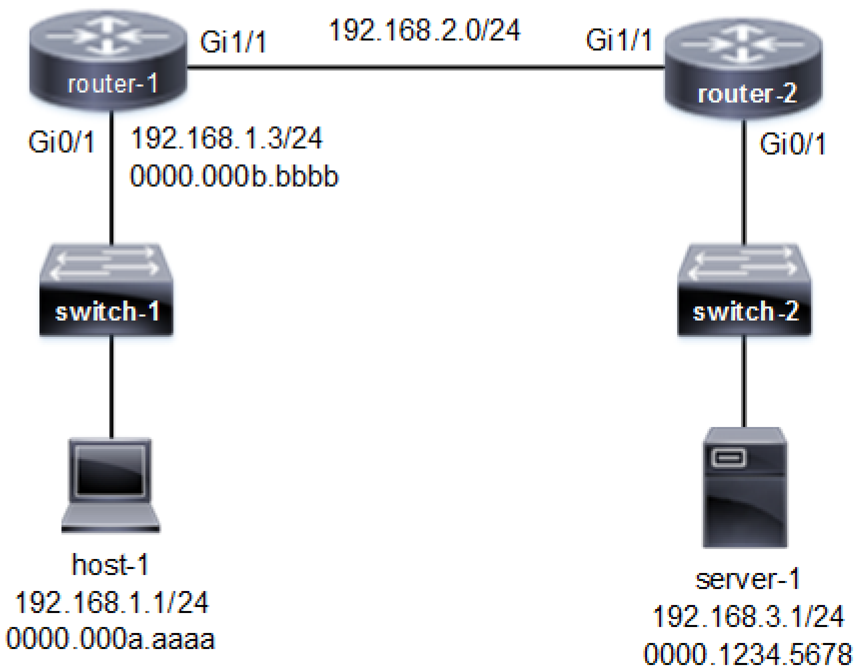


ARP is required for communication between Layer 3 network devices as well. For example, a router must know the MAC address of a neighbor before sending routing updates, proxy ARP requests or data messages. Frame rewrite of MAC addressing is required per hop between Layer 3 network devices.

Example 1: New Host Session

Host-1 would like to initiate a new session with Server-1 on a remote subnet. Where is the ARP request sent?

Figure 2 ARP Request



Answer

When a host endpoint initiates a session with a server on a different subnet, the IP address is resolved first. The DNS request is first sent to resolve or learn the server IP address. DNS server responds to host with IP address of server in the DNS reply packet.

Host-1 then checks the local ARP cache to verify there is not an entry for server-1. ARP entry is comprised of server IP address and associated MAC address. The server is on a different subnet so host-1 sends an ARP request to the default gateway (router-1).

Switch-1 is a Layer 2 device and forwards the ARP request to router-1. The MAC address of router-1 (0000.000c.cccc) is sent to host-1 and added to the local ARP cache. Host-1 then sends a second ARP request to the default gateway requesting the MAC address of server-1.

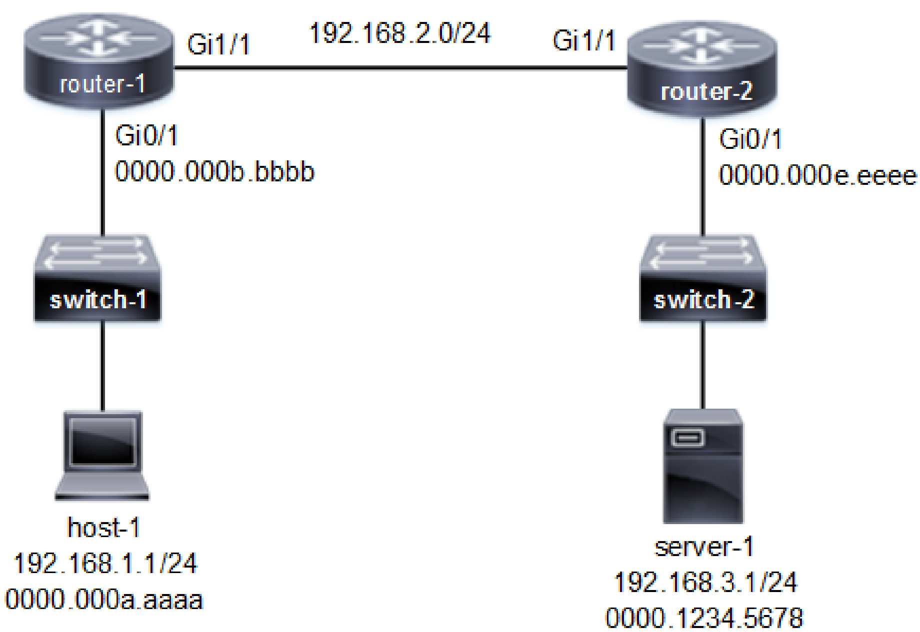
Router-1 checks the local ARP table first to verify if there is an entry for server-1 . If there is no entry for server-1, then router-1 sends proxy ARP request to router-2.

The default gateway IP address is configured with TCP/IP settings for hosts. It is a standard IP parameter that DHCP configures to host and server endpoints. Often hosts will connect to multiple different servers and previous ARP requests have been sent. The default gateway MAC address is already known and has an entry in the local cache.

Example 2: ARP Table Entry

What ARP cache entry is added to host-1 when it pings server-1?

Figure 3 ARP Table Cache



Network ARP table is comprised of IP address to MAC address bindings (mappings) for endpoints and network (intermediate) devices. The default gateway (router-1) responds with the IP address and MAC address assigned to Gi0/0 interface. That is the LAN interface in the same subnet as host-1. The host adds IP address 172.16.2.254/24 and MAC address 0000.000c.cccc to its local ARP cache.

Routing Table Components

It is important to know how to read a routing table to verify that routing is working correctly. The routing table is generated by a router based on dynamically advertised routes (subnets) sent from neighbors. All locally connected routes and static routes are included as well.

The directly connected route is a subnet based on the IP address assigned to a local interface. It is automatically added to the routing table when the interface is enabled. The local interface associated with the subnet (route) is the exit interface for packets destined to that subnet. Static routes including default and floating static routes are manually configured. All routing tables are comprised of the following components.

1. Routing protocol code is the route source.
2. Network address is the destination subnet.
3. Administrative distance is trustworthiness of the route source.
4. Metric is the calculated path cost to the destination subnet.
5. Next hop is the IP address of a neighbor in the forwarding path.
6. Local interface is the exit interface to the next hop address.
7. Age is the amount of time the route has been installed.

router# **show ip route**

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
o - ODR, P - periodic downloaded static route

Gateway of last resort is 172.16.0.1 to network 0.0.0.0

```
     172.16.0.0/24 is subnetted, 3 subnets, 2 masks
C    172.16.1.0/24 is directly connected, Serial0/0
C    172.16.3.128/27 is directly connected, GigabitEthernet0/0
     192.168.25.0/30 is subnetted, 2 subnets
O    192.168.2.1/24 [110/11] via 192.168.2.2, 00:01:12, Serial0/2
O    192.168.3.64/30 [110/15] via 192.168.1.65, 00:00:9,Serial0/3
S*   0.0.0.0/0 [1/0] via 172.16.0.1
```

Routing Protocol Code

The protocol code assigned to a route signifies the source where the route was learned. It is either a dynamic route, static route or connected route. The output of **show ip route** command displays the routing table.

Table 1 Routing Protocol Codes

Route Source	Protocol Code
OSPF	O
OSPF Inter-Area	IA
EGP	E
EIGRP	D
Static Route	S
Default Route	S*
Connected Route	C
Host (/32)	L

Network Address

This is the network address of a destination subnet for a routing entry. It is referred to as a prefix in the routing table. Each IP packet has an address field for source IP address and destination IP address. They do not change between endpoints. They are host addresses assigned to network interfaces. You cannot assign a network address to a network interface. The router examines destination IP address field of an inbound packet to learn the destination subnet. It then selects a route in the routing table to forward packets.

Administrative Distance

This is the reliability of a route when compared with other route sources. Each route type is assigned an administrative distance (AD). It is a value used by the router for route selection. The route with lowest AD number is installed when routes are advertised from multiple routing protocols .

Metric

This is a value that is assigned to each route that is calculated based on the route type. Metric is only considered for best path selection only when multiple routes exist from the same routing protocol. Each routing protocol calculated metric differently. OSPF is based on path cost or link bandwidth. RIPv2 use hop count (number of hops) between endpoints.

Next Hop Address

There is a next hop address associated with each route for packet forwarding purposes. It is IP address of a connected neighbor interface. All routing decisions are made per hop on a forwarding path. The router logic reads as - *to reach this destination subnet, forward packet out local interface that is connected to next hop neighbor with this IP address.*

Local Interface

Each route entry is associated with a local interface and next hop address used for packet forwarding. The local exit interface associated with that route is connected to next hop neighbor for packets that are destined to a subnet. The router is only concerned with identifying local exit interface to use for packet forwarding.

Age

The route entry has an associated age (min) that is based on the amount of time in the routing table. The route entry starts at zero when first learned and is reset if the table is flushed.

Example

This is an OSPF route entry from a routing table with each component defined. For example, 192.168.12.9 is the destination IP address in the IP header. It is a host address and not a network (subnet) address.

O 192.168.12.8/30 [110/128] via 192.168.12.5, 00:35:36, Serial0/0

- Routing protocol code = O (OSPF)
- Destination subnet = 192.168.12.8/30
- Administrative distance = 110
- Metric = 128
- Next hop address = 192.168.12.5
- Local exit interface = Serial0/0
- Age = 00:35:36

Route Selection

The router selects routes to install in the routing table. Sometimes there are multiple routes advertised from multiple routing protocols to the same destination. The administrative distance of a route determines the route installed in the routing table.

The metric is used to select best path to a destination when multiple paths exist. Metric only applies when there are multiple routes from the same routing protocol to the same destination. The longest match rule selects the route with the longest subnet mask (prefix) from routes already in the routing table.

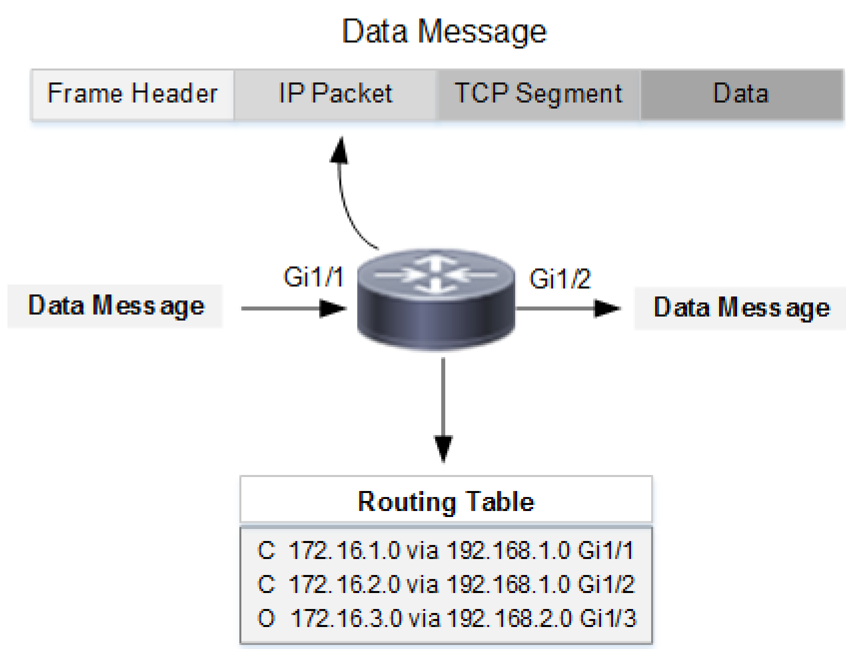
Step 1: Install route = lowest administrative distance

Step 2: Install route = lowest metric (same routing protocol)

Step 3: Select route = longest match rule (subnet mask)

Step 4: Packet discarded when no default route exists

Figure 4 Routing Table Lookup



Administrative Distance

The router builds a routing table with multiple routes (prefixes). Each route type is assigned an administrative distance and calculates a metric. The administrative distance (AD) is a value based on the routing protocol or route source. It is used by routers to select what route is installed in the routing table. The administrative distance and metric assigned to a route will determine what route is installed in the routing table.

The router installs the route with the lowest administrative distance. It is considered when multiple routes exist from multiple routing protocols to the same destination. Administrative distance is configurable to influence route selection.

The route with the lowest AD is considered the most reliable (trustworthy). Directly connected routes have the lowest administrative distance (0) and are the most reliable. The directly connected route is a subnet based on the IP address assigned to a local interface. It is automatically added to the routing table when the interface is enabled.

The following are the default administrative distances for each routing protocol and/or route type. Each routing entry in the routing table includes the administrative distance and metric in brackets [AD / Metric].

Table 2 Administrative Distance (AD)

Route Type	Administrative Distance
Directly Connected	0
Static Route	1
Default Route	1
eBGP	20
EIGRP	90
OSPF	110
IS-IS	115
RIPv2	120
Unknown	255

Example

What is the administrative distance of the route to destination network 192.168.3.0/24?

router# **show ip route**

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
o - ODR, P - periodic downloaded static route

Gateway of last resort is 172.33.0.1 to network 0.0.0.0

        10.1.0.0/24 is subnetted, 5 subnets
C       10.1.1.0/24 is directly connected, Serial0/0
C       10.1.5.0/24 is directly connected, GigabitEthernet0/1
C       10.1.6.0/24 is directly connected, GigabitEthernet0/0
C       10.1.7.0/24 is directly connected, Serial0/1
C       10.1.254.0/24 is directly connected, Loopback0
O       192.168.3.0/24 [110/64] via 192.168.1.1, Serial0/0
```

The command lists all network prefixes to subnet destinations. The router would select the following route to destination subnet 192.168.3.0/24.

O 192.168.3.0/24 [**110**/64] via 192.168.1.1, Serial0/0

OSPF route with next hop 192.168.1.1 has an administrative distance of 110 and metric calculation of 64. Any route assigned an administrative distance of 255 is not installed into the routing table. The router doesn't trust the source of the route and considers it untrustworthy. The local exit interface is Serial0/0 where packets are forwarded to next hop neighbor.

Example: Dynamic Routing Protocols

EIGRP, OSPF, and RIPv2 are advertising routes to the same destination. What route is selected based on the following information?

EIGRP = [90/1252335]

OSPF = [110/10]

RIPv2 = [120/3]

The route with lowest administrative distance is installed in the routing table. EIGRP (90) has a lower administrative distance than OSPF (110) or RIPv2 (120). The result is that EIGRP route is installed in the local routing table. The metric is only considered for best path calculation when multiple routes exist for the same routing protocol to same destination.

Example: Static Route

The following route types are advertising routes to the same destination. What route is selected based on the following information?

OSPF = [110/27]

Static = [1/0]

Default = [1/0]

All routing sources are advertising a route to the same destination subnet. The route with the lowest administrative distance (AD) is installed in the routing table. In this example, the static route and default route have the same lowest AD = 1. The router would select the static route since it is always more specific than a default route.

Example: Connected Route

The following route types are advertising routes to the same destination. What route is selected based on the following information?

Static Route = 172.16.1.0/27

Default Route = 172.16.1.0/27

Connected Route = 172.16.1.0/27

The directly connected route, with AD of zero (0) is considered most reliable route to a destination. The subnet length is only considered when selecting from multiple routes to the same destination already installed in the routing table. It is referred to as longest match rule.

Example: Multiple Route Sources

What route is installed in the routing table from the following routes?

OSPF Route = 172.16.1.0/27

Static Route = 172.16.1.0/27

Default Route = 172.16.1.0/28

Connected Route = 172.16.1.0/29

This example includes a dynamic route (OSPF), static routes and a connected route. The route with lowest administrative distance is the connected route. Each route however has a different subnet mask length, and the router considers them routes to different destinations. All routes are installed in the routing table and administrative distance value is not relevant here.

Path Metric

The administrative distance and metric assigned to a route will determine what route is installed in the routing table. Metric is a path cost assigned to a specific route. Metric is only considered after administrative distance. The route with the lowest metric is installed when there are multiple routes from the **same** routing protocol to the **same** destination.

Each dynamic routing protocol calculates metric differently. For example, OSPF calculates metric for each route that is based exclusively on link bandwidth. Some routing protocols such as OSPF and EIGRP support equal cost load balancing. That is enabled automatically when multiple routes exist from the same routing protocol with the same lowest metric. All routes are installed in the routing table and packets are forwarded across multiple paths to a destination.

Example: OSPF Metric

Each routing table entry includes a square bracket with two values such as [110/128]. The first entry is the administrative distance (110) and the second entry is the metric (128). The route is OSPF and the metric is path cost. There is a static route and a default route as well that are never assigned any metric as denoted with zero (0) in brackets.

router# **show ip route**

```
    192.168.12.0/24 is variably subnetted, 4 subnets, 4 masks
C    192.168.12.64/28 is directly connected, Loopback1
C    192.168.12.32/28 is directly connected, Ethernet0
C    192.168.12.48/28 is directly connected, Loopback0
O    192.168.12.236/30 [110/128] via 192.168.12.233, Serial0
S    172.16.100.0/24 [1/0] via 172.16.2.1
S*    0.0.0.0/0 [1/0] via 172.33.1.1
```

Packet Forwarding

The longest match rule is used to **select a route already installed in the routing table** as a forwarding decision. Each route has a specific prefix (subnet mask) length. The route with the longest prefix is selected from multiple routes within the same subnet range (destination). For example, 172.16.0.0/22 has a longer prefix than 172.16.0.0/18 and would be selected to forward packets to 172.16.0.0 subnet destination.

Example 1: Longest Match Rule

Refer to the routing table. Where will router-1 send packets that have destination IP address of 172.16.1.1?

router-1# **show ip route**

Gateway of last resort is 172.16.0.1 to network 0.0.0.0

```
     172.16.0.0/24 is subnetted, 3 subnets, 3 masks
C      172.16.1.0/25 is directly connected, Serial0/1
C      172.16.1.0/26 is directly connected, Serial0/1
C      172.16.1.0/27 is directly connected, GigabitEthernet0/0
     172.16.254.0/24 is subnetted, 1 subnet
```

The longest match rule is used to select a route already installed in the routing table as a forwarding decision. Each route to a destination has a specific network prefix (subnet mask) length. The route with the longest subnet prefix is selected from multiple routes to the same destination. For example, 172.16.1.0/27 has a longer route prefix than 172.16.1.0/26 and 172.16.1.0/25. As a result, that route prefix is selected for packets with 172.16.1.1 destination IP address.

Example 2: Longest Match Rule

What route is selected for destination IP address 192.168.1.10?

A. 192.168.1.0/28

B. 192.168.1.0/26

C. 192.168.1.0/25

D. 192.168.1.0/27

Answer (A)

The longest match rule would select 192.168.1.0/28 route to destination IP address 192.168.1.10. The packet is forwarded to the next hop and local exit interface associated with the routing entry for that route.

Example 3: Destination Unreachable

Refer to the routing table output for router-1. How will router-1 forward a packet with source IP address 172.16.3.1 and destination IP address 172.16.200.1?

router-1# **show ip route**

Gateway of last resort is not set

```
     172.16.0.0/24 is subnetted, 4 subnets
C       172.16.1.0/24 is directly connected, Serial0/0
C       172.16.2.0/24 is directly connected, Serial0/1
C       172.16.3.0/24 is directly connected, GigabitEthernet0/0
C       172.16.4.0/24 is directly connected, GigabitEthernet0/1
S       172.16.100.0/24 [1/0] via 172.16.2.1
R       172.31.1.0/24 [120/3] via 172.16.1.2
```

The router makes a forwarding decision based on the destination IP address. There is currently no route advertised for 172.16.200.1 in the routing table of router-1. In addition, there is no default route (gateway of last resort) configured either. The router will discard the packet and send an ICMP *destination unreachable* error message.

Example 4: Longest Match Rule

Based on the routing table shown below, when the router receives a packet destined to 192.168.1.65 where will the router forward the traffic?

router# **show ip route**

Gateway of last resort is 172.33.1.1 to network 0.0.0.0

```
     192.168.1.0/24 is variably subnetted, 4 subnets, 4 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
S       192.168.1.128/25 [1/0] via 192.168.2.1
S       192.168.1.64/26 [1/0] via 192.168.2.2
S       192.168.1.32/27 [1/0] via 192.168.2.3
S       10.254.254.254/32 [1/0] via 192.168.2.4
S*      0.0.0.0/0 [1/0] via 172.33.1.1
```

The longest match is in effect when there are multiple routes to the same 192.168.1.65 destination. 192.168.1.64/26 route is the correct prefix with the longest match subnet (/26). It is a static route (S) with 192.168.2.2 as next hop address. The destination IP address 192.168.1.65 is within 192.168.1.128/25 route range as well. The /26 subnet prefix however is longer than the /25 route.

S 192.168.1.64/26 [1/0] via 192.168.2.2

Example 5: Longest Match Rule

What is the next hop selected when forwarding packets to destination IP address 192.168.2.1 based on the routing table?

router-1# **show ip route**

```
Gateway of last resort is 172.16.0.1 to network 0.0.0.0

     172.16.0.0/24 is subnetted, 3 subnets, 2 masks
C      172.16.1.0/24 is directly connected, GigabitEthernet1/1
C      172.16.2.0/24 is directly connected, GigabitEthernet1/2
C      172.16.3.128/27 is directly connected, GigabitEthernet0/0
     192.168.25.0/30 is subnetted, 2 subnets
D      192.168.25.0/30 [90/2681856] via 192.168.25.2, Serial1/0
D      192.168.25.4/30 [90/1823638] via 192.168.25.5, Serial2/0
     192.168.1.0/24 is variably subnetted, 3 subnets, 2 masks
O    192.168.1.0/24 [110/8] via 192.168.1.254, GigabitEthernet0/3
O    192.168.2.0/24 [110/11] via 192.168.3.2, Serial0/2
O    192.168.3.64/30 [110/15] via 192.168.1.65, Serial0/3
S*     0.0.0.0/0 [1/0] via 172.16.0.1
```

The longest match rule would select the following OSPF route with next hop 192.168.3.2 IP address. In this example it is the only route available.

O 192.168.2.0/24 [110/11] via 192.168.3.2, Serial0/2

Example 6: Longest Match Rule

Router-1 must select route to forward packets with destination IP address 172.16.4.1. What is the routing method, next hop IP address and router interface based on the routing table exhibit?

```
router-1# show ip route

Gateway of last resort is not set

     172.16.0.0/24 is variably subnetted, 4 subnets, 2 masks
C       172.16.1.0/24 is directly connected, GigabitEthernet0/0
C       172.16.200.0/30 is directly connected, Serial0/0
C       172.16.200.16/30 is directly connected, Serial0/1
D    172.16.4.0/25 [90/1234567] via 172.16.200.18, Serial0/1
O    172.16.4.0/27 [110/64] via 172.16.200.2, Serial0/0
O    172.16.4.0/26 [110/32] via 172.16.200.17, Serial0/2
```

Answer

The router selects the route with the longest prefix (subnet) where there are multiple routes to the same destination. It is referred to as the longest match rule. The following OSPF route has the longest prefix (/27) to the destination 172.16.4.0 subnet. The next hop address to forward packets destined for 172.16.4.0 is 172.16.200.2 via Serial0/0 local interface.

```
O    172.16.4.0/27 [110/64] via 172.16.200.2, Serial0/0
```

All routes that have a different prefix length are considered different destinations by the router. The router will install multiple routes from different routing protocols as a result. The administrative distance only applies to routes that have the same destination (same prefix length).

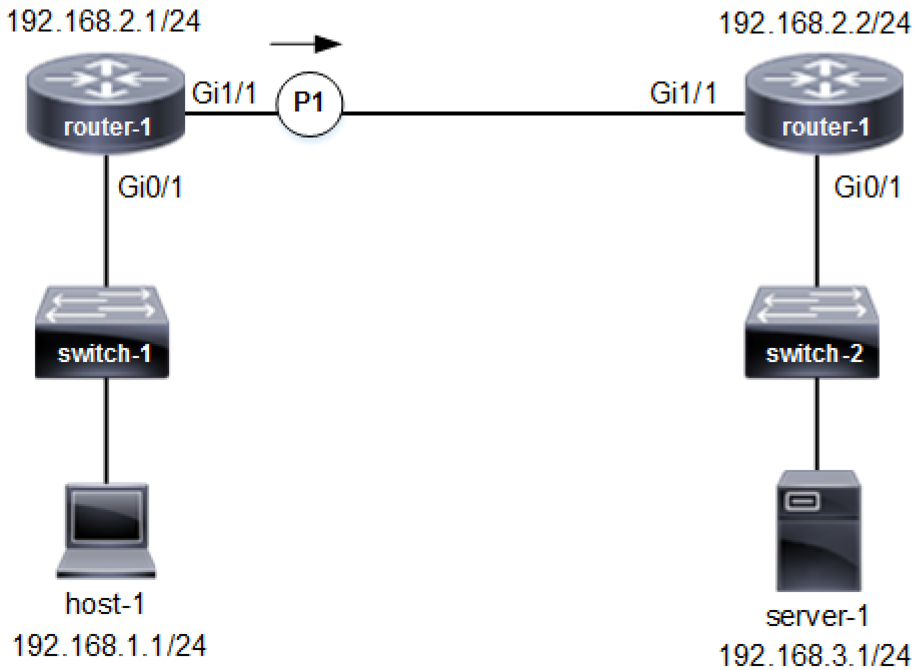
Per-Hop IP Addressing

The source and destination IP address do not change between endpoints. They are written to the IP header at an originating endpoint only. For example, packets originating at host-1 would have source IP address of the host. The same packets would have destination IP address of the server. Conversely, packets in the reverse direction would have server as source IP address and host as destination IP address. The same occurs with Telnet session initiated from a router for example. The local router and neighbor router are endpoints for IP addressing.

Example: IP Packet Header

Refer to the network topology drawing. The host is sending data to an application on server-1. What is source and destination IP address of packets at **P1** based on per hop addressing rules?

Figure 5 Per Hop IP Addressing



There is a per hop forwarding path from host-1 to server-1. The source and destination IP address do not change between host and server. The source IP address is 192.168.1.1 (host) and destination IP address is 192.168.3.1 (server). MAC addressing is updated by each router hop.

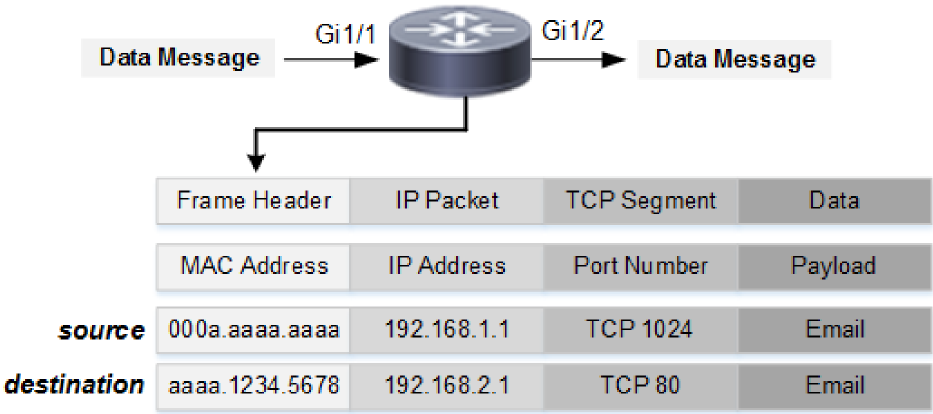
- Source IP address = 192.168.1.1
- Destination IP address = 192.168.3.1

Frame Rewrite

As packets traverse the network through each routing hop there is frame rewrite. When a data message arrives, the router examines IP header to select a route for forwarding. Once the route is selected from the routing table, then frame rewrite occurs.

The router strips off the Ethernet frame header and rewrites a new frame with source and destination MAC address. Source MAC address is the local exit Ethernet interface of router. The next hop neighbor Ethernet interface MAC address is written to the new frame as destination MAC address.

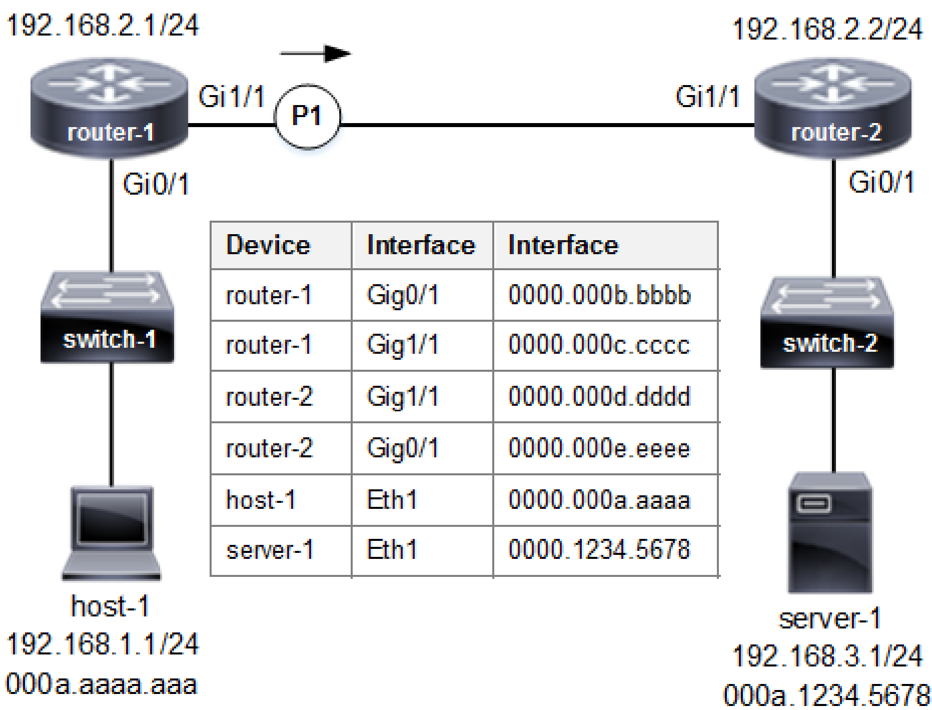
Figure 6 Frame Rewrite



Example 1: Frame Rewrite

Refer to the network drawing. What is the source and destination MAC address of the frame at **P1** when it is forwarded to router-2?

Figure 7 Ethernet Frame Rewrite



Device	Interface	Interface
router-1	Gig0/1	0000.000b.bbbb
router-1	Gig1/1	0000.000c.cccc
router-2	Gig1/1	0000.000d.dddd
router-2	Gig0/1	0000.000e.eeee
host-1	Eth1	0000.000a.aaaa
server-1	Eth1	0000.1234.5678

Consider that MAC addressing is required so that data messages arrive at the correct destination. For example, the local switch connected to a server would examine the incoming frame of a data message.

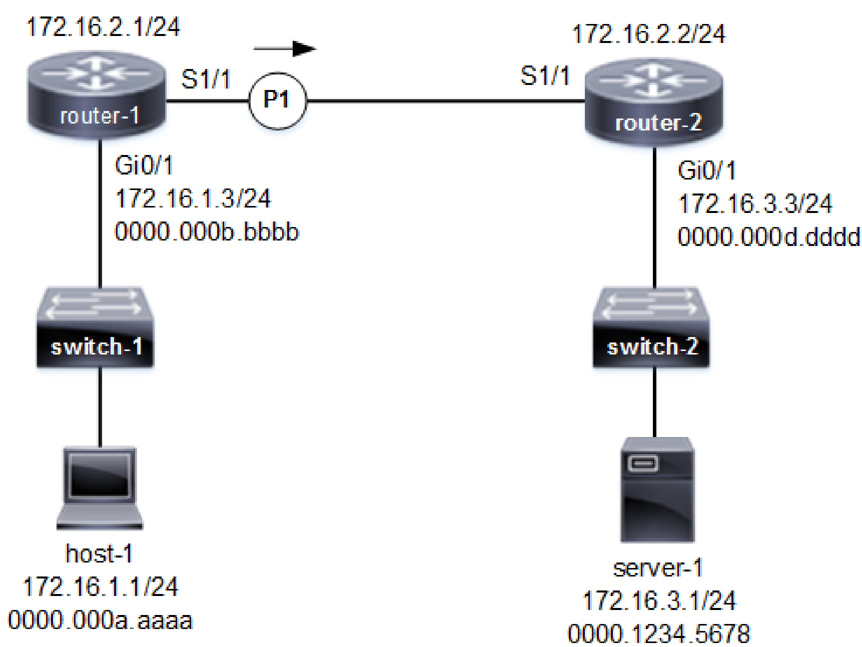
It is the destination MAC address that is used for forwarding frames to the destination server. Layer 3 devices rewrite source and destination MAC address per hop. The source MAC address for this example is derived from router-1 interface Gi1/1. The destination MAC address is derived from router-2 interface Gi1/1 and obtained from an ARP table lookup.

- Source MAC address = 0000.000c.cccc
- Destination MAC address = 0000.000d.dddd

Example 2: Frame Rewrite

Refer to the network topology drawing and output from the **show arp** command on router-1. What frame rewrite occurs at **P1** before packet is forwarded to router-2?

Figure 8 Frame Rewrite on Serial Interfaces



router-1# **show arp**

Protocol	Address	Age	Hardware Addr.	Type	Interface
Internet	172.16.1.3	-	0000.000b.bbbb	ARPA	GigabitEthernet0/1
Internet	172.16.1.1	12	0000.000a.aaaa	ARPA	GigabitEthernet0/1
Internet	172.16.2.2	12	0000.000d.dddd	ARPA	
Internet	172.16.3.1	12	0000.1234.5678	ARPA	

Answer

The output from **show arp** command lists the IP address and associated hardware address. That includes all ARP requests performed by router-1. Match the IP address from the network topology drawing with MAC address in the ARP table.

There is an Aging field with (**-**) indicates the MAC address of interface Gi0/1 on router-1. It does not age out from the table. The default ARP entry aging timer is 240 minutes. At that point the entry is flushed and new ARP request is required. The Interface field signifies where the MAC address was learned.

The router will update (rewrite) the source and destination MAC address. The router rewrites the source MAC address with the MAC address of router-1 interface Gi0/1. The destination MAC address is rewritten with interface Gi0/1 on router-2.

Serial interfaces do not have a MAC address. The router would assign the MAC address of the Ethernet interface where frames arrived (were learned) for source MAC address.

ARP Table Entry

Internet	172.16.1.3	**-**	0000.000b.bbbb	ARPA	GigabitEthernet0/1
Internet	172.16.2.2	12	0000.000d.dddd	ARPA	

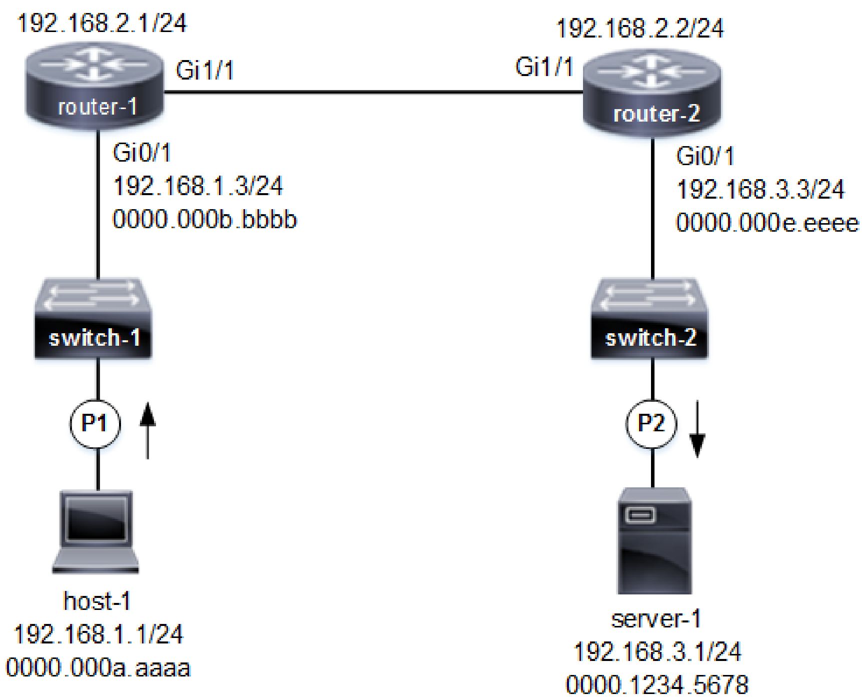
Frame Rewrite

source MAC address = 0000.000b.bbbb
destination MAC address = 0000.000d.dddd

Example 3: Frame Rewrite

Refer to the network drawing. What is the source and destination MAC address at **P1**? What is the source and destination IP address at **P2**?

Figure 9 Per Hop Frame Rewrite



The source and destination MAC address are rewritten at each router hop. The switch only examines the source and destination MAC address. Host-1 sends a packet at **P1** with MAC address of network interface as source MAC address (0000.000a.aaaa). The destination MAC address at **P1** is router-1 interface Gi0/0 (0000.000b.bbbb). Layer 2 switches are never the destination for a MAC address. They only forward frames and must know the destination MAC address.

The source and destination IP address do not change as packets traverse the network. The source IP address is 192.168.1.1 (host) and destination IP address is 192.168.3.1 (server).

P1: source MAC address = 0000.000a.aaaa
P1: destination MAC address = 0000.000b.bbbb

P2: source IP address = 192.168.1.1 (host-1)
P2: destination IP address = 192.168.3.1 (server-1)

Endpoints: Follow the Packet

The following explains how communication is enabled between endpoints after DHCP server assigns IP addressing. In fact, DHCP, DNS and ARP are address-based protocols used for TCP session setup. Once there is TCP session established, routing can occur and data is sent between endpoints as shown with Figure 10.

1. The host sends a DNS request for the IP address of server.

2. The host sends an ARP broadcast request to the default gateway (router-1 interface IP address) for its MAC address.

3. There is a unicast packet sent from router-1 to host with the MAC address assigned to default gateway interface.

4. ARP entry is added to the local ARP table of router-1 with the host IP address and MAC address.

5. The host sends the first ICMP echo request to router-1 with destination MAC address of the default gateway and destination IP address of the server.

    - source MAC address = host
    - destination MAC address = router-1
    - source IP address = host
    - destination IP address = server

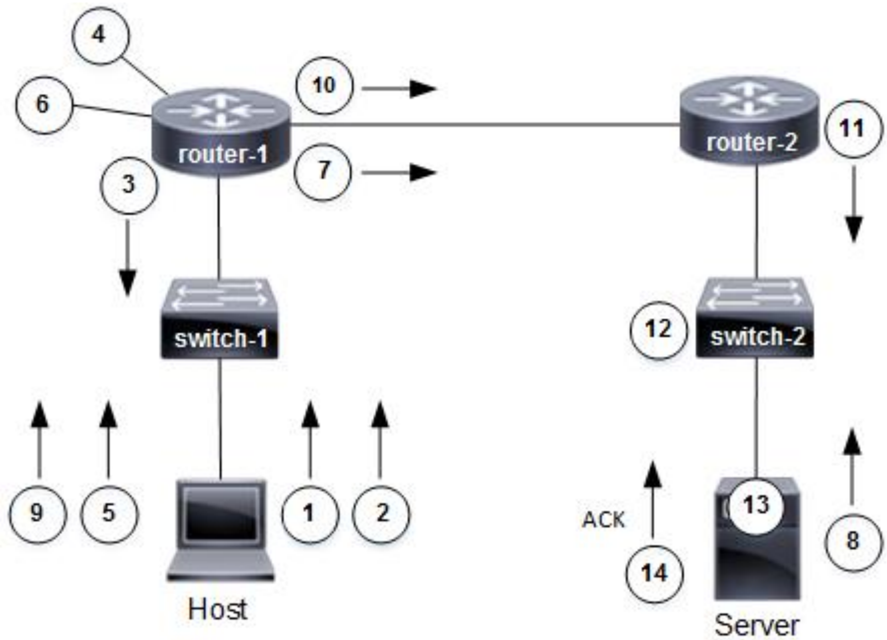
6. There is an ARP table lookup on router-1 for the server MAC address. Since ARP table on router-1 has no entry for the server, first ICMP echo request packet is dropped.

7. Proxy ARP request is sent from router-1 to the server for its MAC address.

8. The server sends an ARP reply to router-1 with server MAC address and router-1 updates the local ARP table.

9. The host sends a second ICMP echo request to router-1.

Figure 10 Follow the Packet



10. ARP table lookup is performed on router-1 for the server MAC address. In addition there is a routing table lookup for server subnet. The router then rewrites (updates) packet IP address field and frame MAC address field. The packet is then forwarded to next hop address of router-2.

    - source MAC address = router-1
    - destination MAC address = router-2
    - source IP address = host
    - destination IP address = server

11. The packet arrives at router-2 where there is an ARP table lookup for the server MAC address. In addition there is a routing table lookup for server subnet to forward packets. The router rewrites the packet and frame, before it is forwarded out the router interface connected to switch-2.

    - source MAC address = router-2
    - destination MAC address = server
    - source IP address = host
    - destination IP address = server

12. The packet arrives at switch-2 where there is a MAC address table lookup for the server MAC address. The packet is forwarded out of the switch port assigned to the server.

13. The server receive the packet and all headers are stripped off before payload is forwarded to the application.

14. The server sends TCP ACK to the host for the next TCP window sequence of packets for TCP-based applications only.

IPv4 and IPv6 Static Routing

The purpose of a route is to enable end-to-end network connectivity between endpoints. There is always a forward and reverse path between endpoints. The routing table is comprised of multiple routes that are often from different sources. The route type can be classified as either connected, static or dynamic. The distinction is in how the local router learns of the route. For example, connected routes are automatically learned while static and default routes are manually configured.

Dynamic routes are learned from a directly connected neighbor that advertises locally known routes. Most routes point to a subnet however there are also host routes that are based on a host address. It is routers and Layer 3 switches that are configured with routing services. There are firewalls as well that support routing services. Consider as well that static and dynamic routing support both IPv4 and IPv6 address space.

Connected Route

Connected routes are not manually configured or dynamic. They are automatically added to a routing table. The route entry includes a local network interface. Local router interfaces are configured with an IP address that is within a particular subnet. Anytime routing services are enabled, you will notice at least some connected routes in the routing table. The router installs a corresponding local host route as well for each connected interface. It is assigned a /32 subnet mask that indicates a host route. For example, consider a local physical interface assigned 192.168.1.1/24 address. The connected route added to the routing table is the following route entry. Connected routes have an administrative distance of zero (0) and metric of zero (0).

C   192.168.1.0/24 is directly connected, Ethernet1/0

L   192.168.1.1/32 is directly connected, Ethernet1/0

IPv4 Static Route

Static and connected routes are the most common route types. The static route is an explicitly configured route. It is automatically added to the routing table upon configuration. It has an administrative distance of 1 and metric of zero (0). That is lower than any dynamically learned route, so they are preferred over dynamic routes to the same destination. Static routes are not advertised to neighbors unless they are advertised through a dynamic routing protocol.

S 172.16.1.1 [1/0] via 192.168.1.1

The static route is more specific than a default route and selected for a route to the same destination.

- The static route reads from left to right - *to reach this destination subnet, forward packets to this next hop address or exit this local interface*.
- The next hop is the IP address of connected neighbor network interface.
- Local exit interface is an alternative to next hop address for packet forwarding.
- Static routing must be configured in both directions to forward packets. There is always an originating path and return path to enable end-to-end connectivity between endpoints.
- Endpoints are assigned an IP address that has a destination subnet.
- Compared with dynamic routing there is more security, no routing updates and less CPU usage. Manually configured routes are managed and provide deterministic packet forwarding.

Static Route Configuration

Static routes are configured from global configuration mode. The advantages are added security with manual routes and less updates compared with dynamic routing protocols. The next hop to a destination network (subnet) is configured as an IP address or local exit interface.

Figure 11 Static Routing Components

The following example forwards all packets destined for 72.16.3.0/24 subnet to 172.16.12.1 next hop address. The router does a routing table recursive lookup for an exit interface associated with that next hop. That is a connected route since it is directly associated with a local interface. The neighbor has a connected interface within same subnet.

router(config)# **ip route 172.16.3.0 255.255.255.0 172.16.12.1**

Local Exit Interface

Alternatively, you can configure a local exit interface instead of next hop address for routing. You would configure the local interface that is directly connected to the next hop neighbor.

Figure 12 Static Route Local Interface

destination	subnet mask	local interface

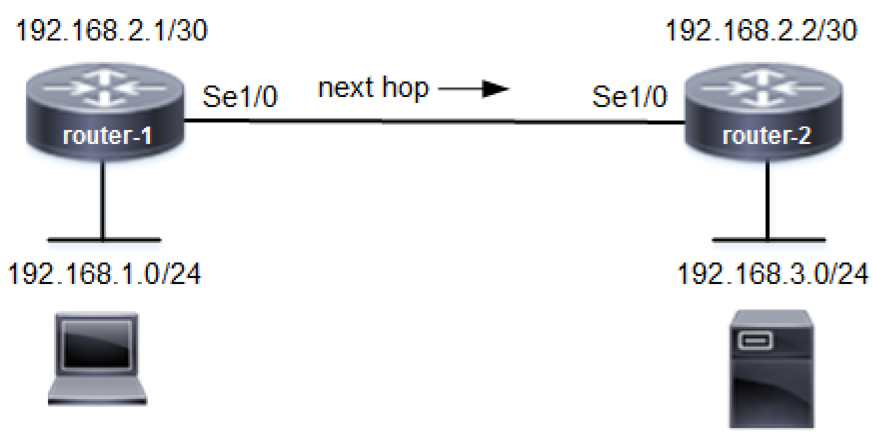
The following example configures a static route with next hop as a local exit interface. All packets destined for 192.168.1.0/24 are forwarded out of local interface Gigabitethernet0/1. The local interface is connected to a neighbor on the same subnet with a route to the destination.

router(config)# **ip route 192.168.1.0 255.255.255.0 Gig0/1**

Example: Static Route

Refer to the network drawing. What are two configuration methods could enable a static route to 192.168.3.0/24 subnet?

Figure 13 Static Route



Answer

The following two options would enable routing from 192.168.1.0/24 subnet to 192.168.3.0/24 subnet.

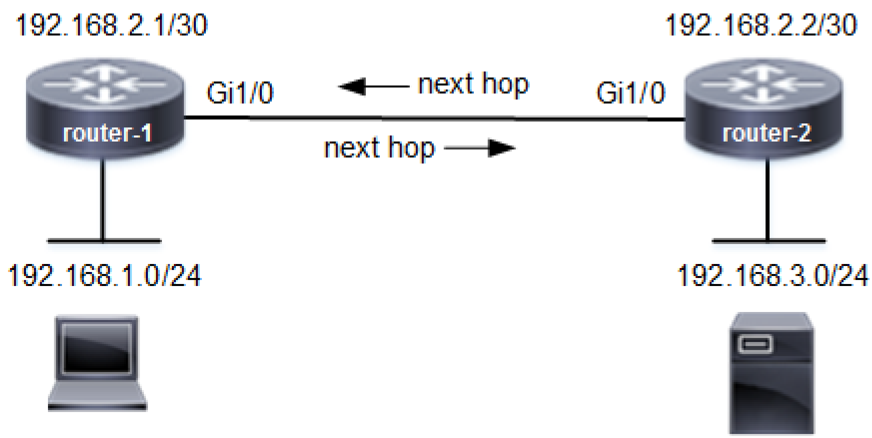
router-1(config)# **ip route 192.168.3.0 255.255.255.0 192.168.2.2**
router-1(config)# **ip route 192.168.3.0 255.255.255.0 Serial1/0**

The first command configures a static route on router-1 with next hop address of 172.16.2.2. The optional IOS command configures next hop as local exit interface Serial1/0 on router-1. Wildcard masks are not used when configuring static routes.

Example 2: Bidirectional Path Forwarding

Refer to the network topology drawing. There are no dynamic routing protocols enabled on router-1 or router-2. What routing configuration is required to enable routing between host and server subnets?

Figure 14 Bidirectional Forwarding Path



There are no dynamic routing protocols such as OSPF that automatically advertise routes between neighbors. All routes between endpoints must have a return or reverse path. The solution is to configure a static route on each router for both directions.

router-1(config)# **ip route 192.168.3.0 255.255.255.0 192.168.2.2**
router-2(config)# **ip route 192.168.1.0 255.255.255.0 192.168.2.1**

When hosts send data to the server, router-1 will use the static route with next hop address to reach the server subnet. Conversely, when the server returns data, router-2 will use the static route with next hop to the host subnet. The following describes router logic for all packets that are originating at a host.

Source Path

The first IOS command reads - *to reach server destination subnet 192.168.3.0 forward packets to next hop 192.168.2.2 address.*

Reverse Path

The second IOS command reads - *to reach host destination subnet 192.168.1.0 forward packets to next hop 192.168.2.1 address.*

IPv6 Static Route

Cisco network devices support static routing for network interfaces that are assigned an IPv6 address. The IOS syntax is different since it is based on IPv6 addressing. There are the same components however of destination network and next hop address or local interface. The structure of 128-bit IPv6 addressing is quite different from IPv4 addressing. The subnet mask of an IPv6 address is slash notation instead of dotted decimal (255.255.255.0).

Table 3 IPv6 Route Type Examples

Route Type	Example
network prefix	/64
default route	ipv6 route ::/0 2001:DB8:3C4D:2::1
point-to-point address	/126
host route	/128
floating static	ipv6 route 2001:DB8::/32 Fa1/0 200
static route	ipv6 route 2001:DB8:3C4D::/64 Gi1/1
fully specified static	ipv6 route 2001:DB8:3C4D::/64 Gi1/1 FE80::2
host route	/128
directly connected static	ipv6 route 2001:DB8::/32 serial 1/0

IPv6 packet forwarding must first be enabled globally on the network device with **ipv6 unicast-routing** command. The following configure an IPv6 static route to destination network 2001:DB8:3C4D:1::/64 with next hop address 2001:DB8:3C4D:2::1.

ipv6 unicast-routing
ipv6 route 2001:DB8:3C4D:1::/64 2001:DB8:3C4D:2::1

The following command configure an IPv6 static route with next hop as a local interface. The router forwards all packets out local interface Gig0/0 destined for network address (subnet) 2001:DB8:3C4D:1::/64.

ipv6 route 2001:DB8:3C4D:1::/64 Gigabitethernet0/0

The other option for configuring an IPv6 static route include the next hop IPv6 address that is fully specified. It applies only to a broadcast (Ethernet) network. The local interface must be specified as well when the next hop is an IPv6 link-local (FE80::2) address.

ipv6 route 2001:DB8:3C4D::/64 Gig0/0 FE80::2

IPv4 Floating Static Route

Any static route configured with a higher administrative distance than a static route is a floating static route. It is installed in the routing table only when the standard static route is not available. That could result from a link failure for example. The static route has a lower administrative distance (1) compared with the floating static route. As a result, it is selected and installed as the primary route.

The floating static route is typically configured to forward traffic across a backup link for failover purposes. The floating static route with the higher administrative distance (AD) of **200** for example, becomes active only when the primary static route is not available. In fact, any administrative distance higher than 1 would work. The following floating static route configured as a backup link on a router.

ip route 172.16.1.0 255.255.255.0 192.168.12.1 200

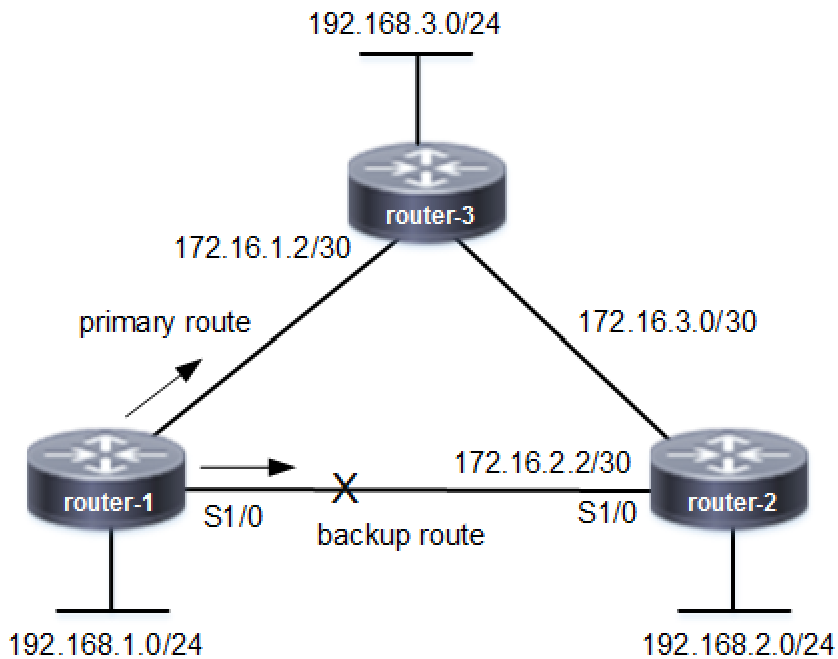
- Destination subnet = 172.16.1.0
- Subnet mask = 255.255.255.0 (/24)
- Next hop IP address = 192.168.12.1
- Administrative distance = 200

There is a high number often assigned to a floating static route. That prevents it from being inadvertently installed in the routing table ahead of a dynamic route. That could occur for example, with an OSPF route that has administrative distance of 110. Assigning AD 100 to a floating static route would install it instead of an OSPF route to the same destination.

Example: Floating Static Route

Refer to the network drawing. What IOS command will configure a floating (backup) static route with AD 200 on router-1 to destination network 192.168.3.0/24?

Figure 15 Floating Static Route



Answer

The primary link has a direct route from router-1 to 192.168.3.0/24 via next hop 172.16.1.2 address on router-3. The floating static route is installed in the routing table when the primary link fails. Traffic destined for subnet 192.168.3.0 is then forwarded to router-2 using next hop 192.168.2.2 address.

The administrative distance of a static route is 1. The following IOS command will configure a floating static route on router-1 to subnet 192.168.3.0/24 with administrative distance of 200. You could assign any value greater than 1 to the static route. The much higher AD guarantees that routes with a high AD are not inadvertently replaced by the floating static route.

ip route 192.168.3.0 255.255.255.0 172.16.2.2 200

- Destination network address = 192.168.3.0
- Subnet mask = 255.255.255.0 (/24)
- Next hop IP address = 172.16.2.2
- Administrative distance = 200

IPv4 Default Route

The default route is referred to as gateway of last resort in the routing table. All packets are forwarded to the default route when there is no route in the routing table. There is a next hop IP address specified with the default route.

The default route reads from left to right – *forward all traffic to this next hop address when there is no route in the routing table to the destination network*. The default route is often configured as an external route for forwarding packets to the internet. They are used as well for some branch offices that only have a single link.

There is only a single route to all remote destinations. That minimizes the routing table size and router CPU utilization. The administrative distance of default and static routes is 1. In addition, both have the same metric of zero. The following configuration is a default route with next hop address of 172.33.1.1 to the internet. The default route will forward all packets with an unknown destination to the next hop address.

ip route 0.0.0.0 0.0.0.0 172.33.1.1

The router will discard packets when there is no destination route in the routing table and no default route exists. ICMP *destination unreachable* error message is then sent to the source. This is an example of a default route installed in the routing table.

S* 0.0.0.0/0 [1/0] via 172.33.1.1

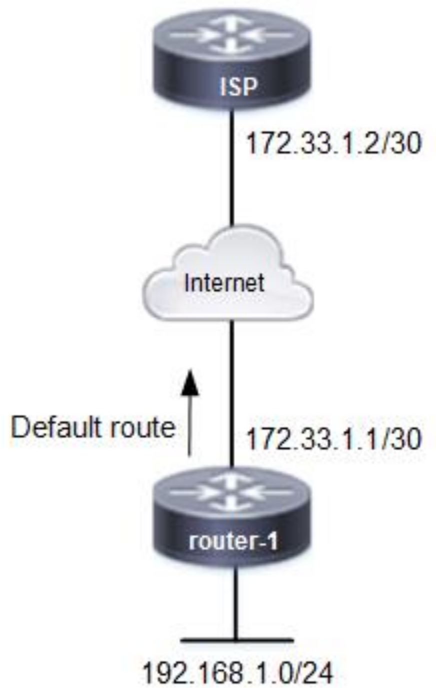
Cisco network devices also support default routing with interfaces that have an IPv6 address. The following configuration is an IPv6 default route with next hop 2001:DB8:3C4D:2::1 address. The next hop address is assigned to the interface of an ISP router for an internet connection.

router(config)# **ipv6 unicast-routing**
router(config)# **ipv6 route ::/0 2001:DB8:3C4D:2::1**

Example 1: Default Route

Refer to the network topology drawing. What route is required on router-1 to forward all internet traffic to ISP?

Figure 16 Default Forwarding Path to the Internet



Answer

The default route is used to forward packets when no specific route exists in the routing table to a destination. The default route on router-1 forwards all traffic to ISP next hop 172.16.2.2 when the destination is unknown.

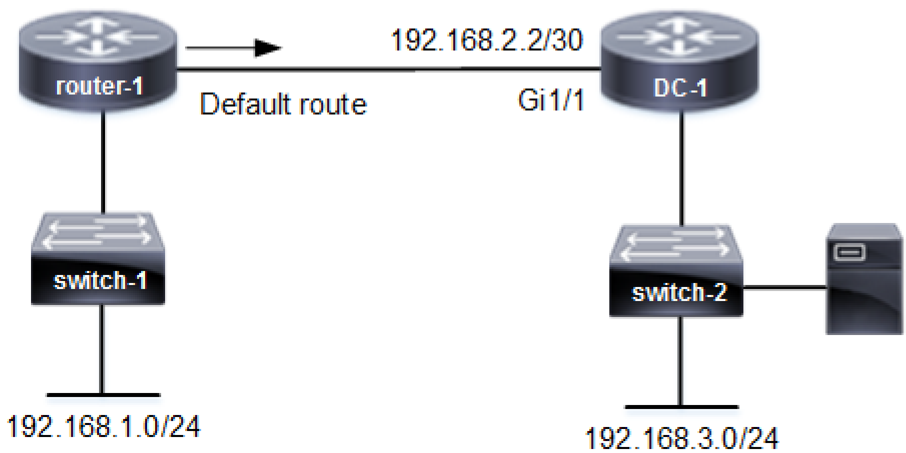
router-1(config)# **ip route 0.0.0.0 0.0.0.0 172.33.1.2**

It is common to assign a default route for internet access instead of having external routes in a local routing table. The ISP router is responsible for all return path traffic. The router will discard the packet when there is no destination route in the routing table and no default route is configured. The router sends an ICMP Destination Unreachable error message to the source.

Example 2: Default Route

Refer to the network topology drawing. What is the easiest solution to enable routing between router-1 and the corporate data center?

Figure 17 Default Route to the Data Center



Answer

The easiest solution for connecting a branch office (router-1) to a data center is with a default route. All packets with an external destination are forwarded to the data center.

The following IOS global command configures a default route. All traffic is forwarded to next hop 192.168.2.2 address. That is the IP address of the data center router (DC-1) interface Gi1/1.

router-1(config)# **ip route 0.0.0.0 0.0.0.0 192.168.2.2**

The use of static routes would require multiple configurations for each destination. The default route will forward all packets arriving for any destination address to the next hop IP address.