Chapter 1: Basic Network and Routing Concepts

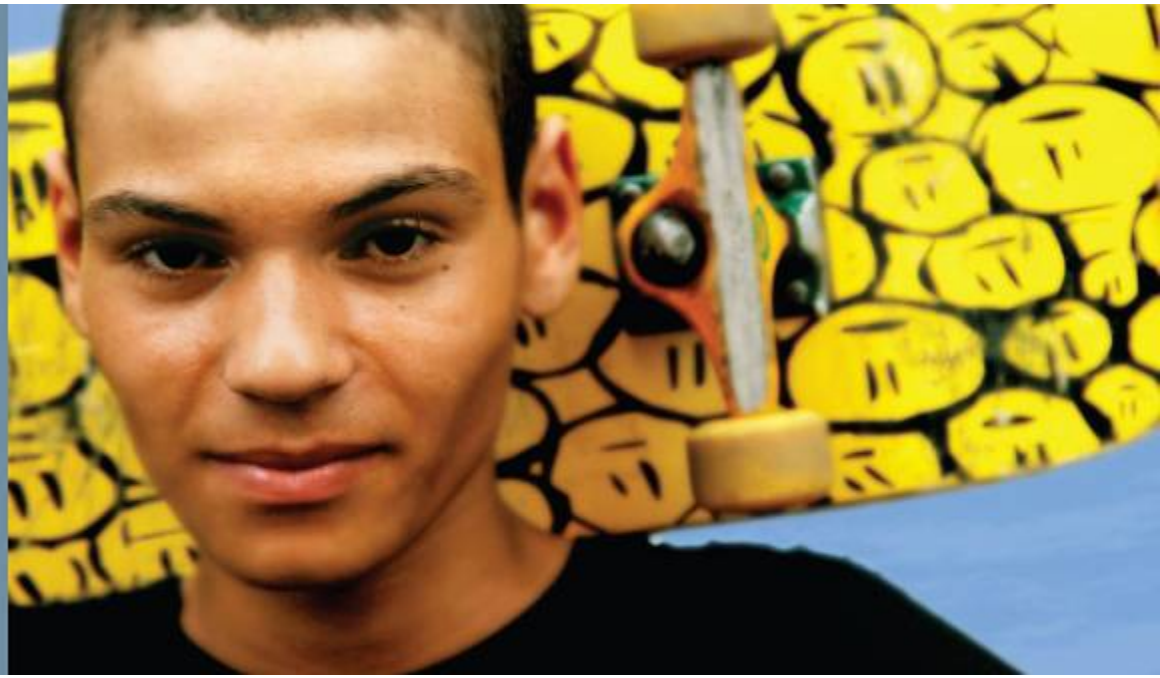
CCNP ROUTE: Implementing IP Routing

Cisco | Networking Academy®
Mind Wide Open™

Chapter 1 Objectives

- Differentiating Between Dynamic Routing Protocols
- How Different Traffic Types, Network Types, and Overlaying Network Technologies Influence Routing
- Differentiating Between the Various Branch Connectivity Options and Describing Their Impact on Routing Protocols
- How to Configure Routing Information Protocol Next Generation (RIPng)

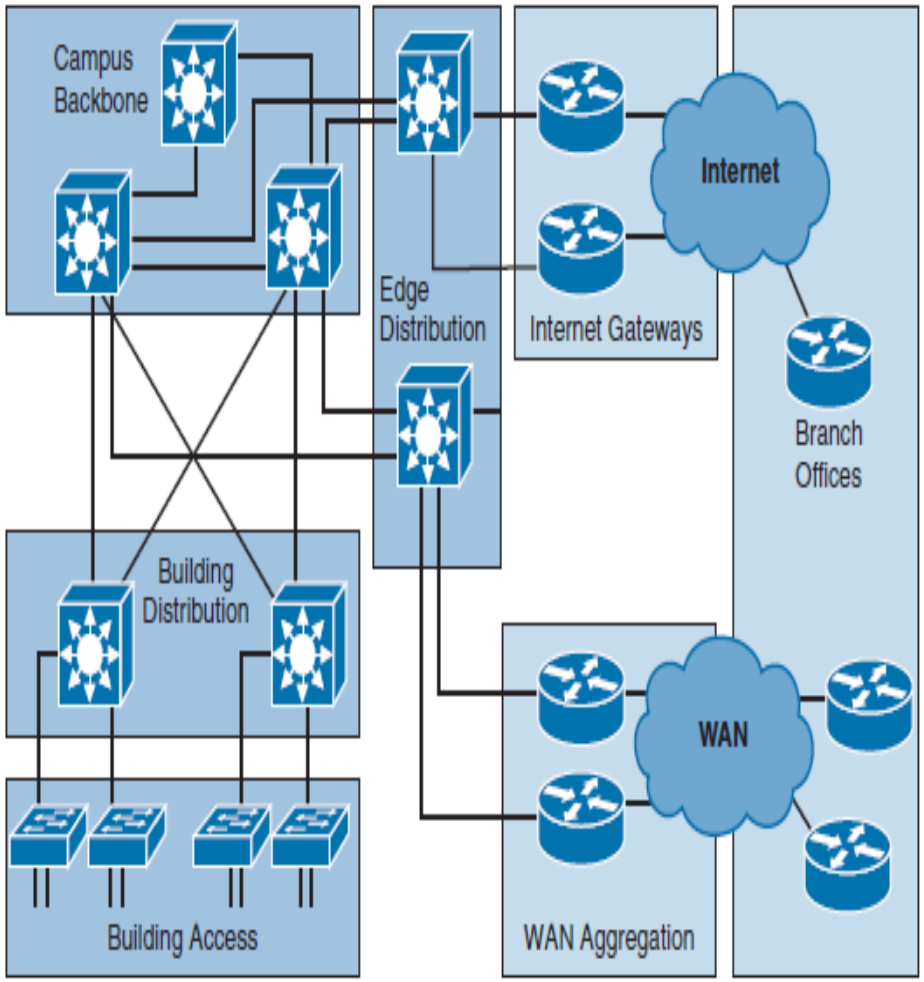
Differentiating Between Dynamic Routing Protocols



Differentiating Between Dynamic Routing Protocols

- Enterprise Network Infrastructure
- Dynamic Routing Protocols in the Enterprise Network Infrastructure
- Choosing a of Dynamic Routing Protocols
- IGP and EGP Routing Protocols
- Types of Routing Protocols
- Importance of convergence
- Route summarization
- Describe what influences routing protocol scalability

Enterprise network infrastructure



Enterprise Campus

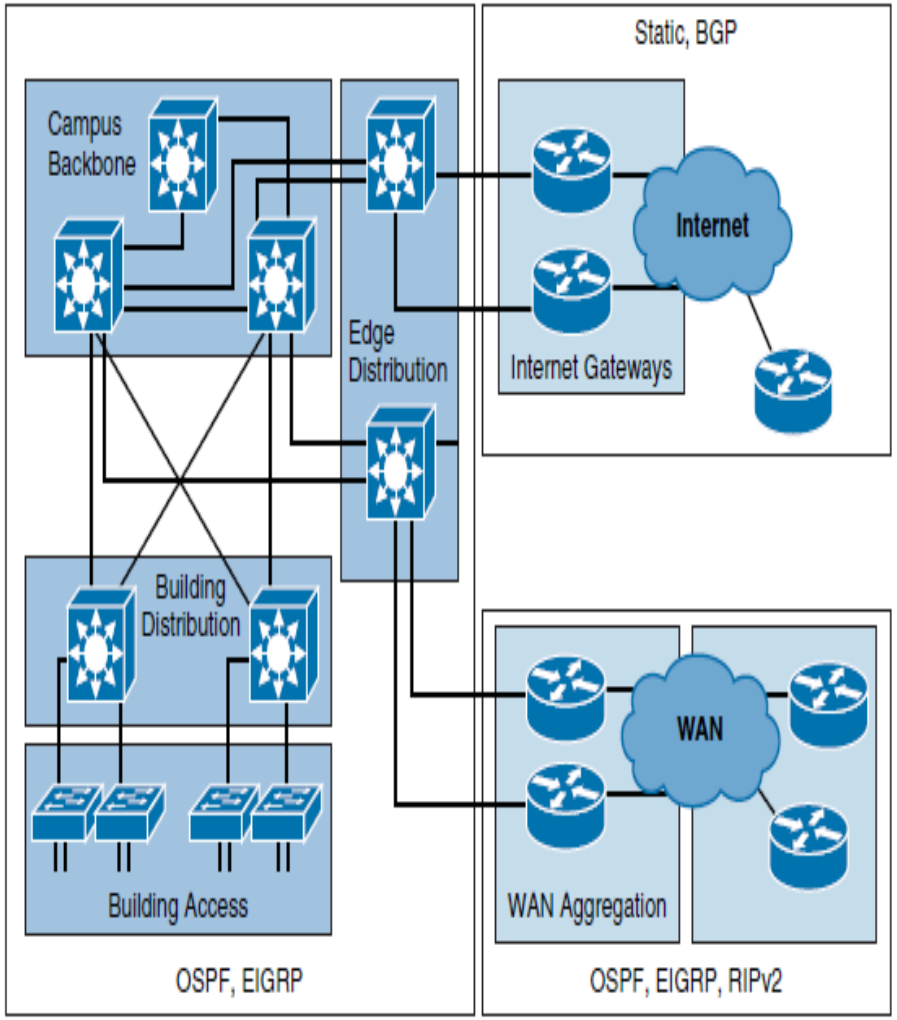
- An enterprise campus provides access to the network communications services and resources to end users and devices.
- It is spread over a single geographic location, spanning a single floor, building, or several buildings in the same locality.
- The campus is commonly designed using a hierarchical model — comprising the core, distribution, and access layers—creating a scalable infrastructure.

Enterprise Edge

- An enterprise edge provides users at geographically disperse remote sites with access to the same network services as users at the main site.
- The network edge aggregates private WAN links that are rented from service providers, and it enables individual users to establish VPN connections.
- In addition, the network edge also provides Internet connectivity for campus and branch users.

Dynamic Routing Protocols in the Enterprise Network Infrastructure

- It is a best practice that you use one IP routing protocol throughout the enterprise, if possible.
- One common example of when multiple routing protocols are used is when the organization is multihomed.
- In this scenario, the most commonly used protocol to exchange routes with the service provider is Border Gateway Protocol (BGP), whereas within the organization, Open Shortest Path First (OSPF) or Enhanced Interior Gateway Routing Protocol (EIGRP) is typically used.
- In a single-homed infrastructures static routes are commonly used between the customer and the ISP.



Choosing a of Dynamic Routing Protocols

Input requirements :

- Size of network
- Multivendor support
- Knowledge level of specific protocol

Protocol characteristics :

- Type of routing algorithm
- Speed of convergence
- Scalability

IGP and EGP Routing Protocols

An autonomous system (AS) represents a collection of network devices under a common administrator.

Routing protocols can be divided based on whether they exchange routes within an AS or between different autonomous systems:

Interior Gateway Protocols (IGP)

- Support small, medium-sized, and large organizations, but their scalability has its limits. Fast convergence, and basic functionality is not complex to configure. The most commonly used IGPs in enterprises are EIGRP, OSPF and RIP is rarely used. IS-IS is also commonly found as ISP IGP

Exterior Gateway Protocols (EGP)

- Used to exchange routes between different autonomous systems. BGP is the only EGP that is used today. The main function of BGP is to exchange a huge number of routes between different autonomous systems.

Types of Routing Protocols

	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	MBGP

Distance vector protocols

- The distance vector routing approach determines the direction (vector) and distance (such as link cost or number of hops) to any link in the network. The only information that a router knows about a remote network is the distance or metric to reach this network and which path or interface to use to get there. Distance vector routing protocols do not have an actual map of the network topology.

Link-state protocols

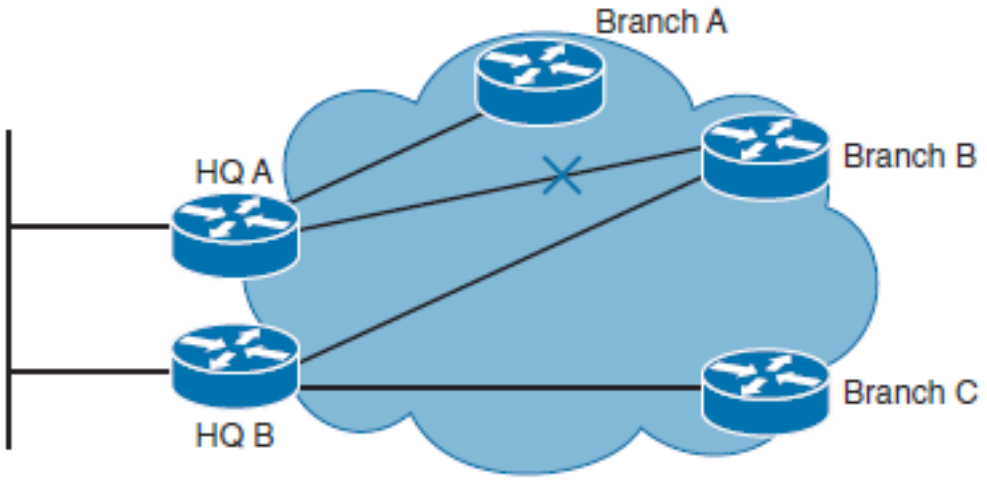
- The link-state approach uses the Shortest Path First (SPF) algorithm to create an abstract of the exact topology of the entire network or at least within its area. A link-state routing protocol is like having a complete map of the network topology. The map is used to determine best path to a destination.

Path vector protocols

- Path information is used to determine the best paths and to prevent routing loops. Similar to distance vector protocols, path vector protocols do not have an abstract of the network topology. Path vector protocols indicate direction and distance, but also include additional information about the specific path of the destination.

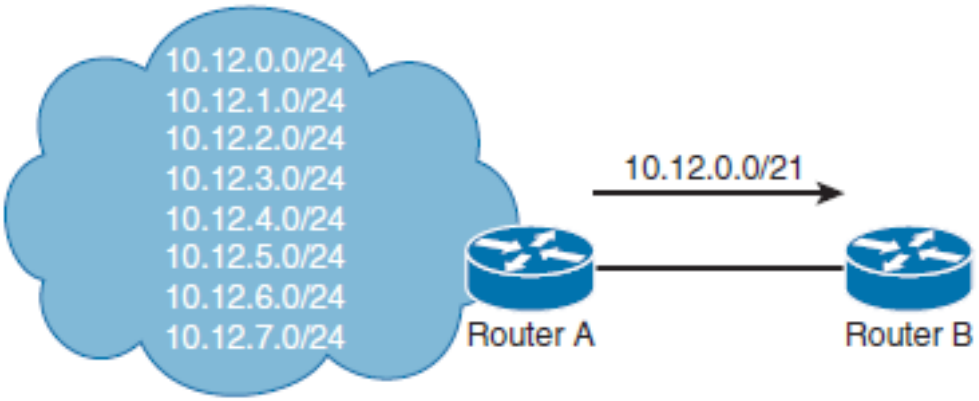
Importance of Convergence

- The process of when routers notice change in the network, exchange the information about the change, and perform necessary calculations to reevaluate the best routes.



- To minimize downtime and quickly respond to network changes, a fast convergence time is desired.

Route Summarization



- Route summarization reduces routing overhead and improve stability and scalability of routing by reducing the amount of routing information that is maintained and exchanged between routers.

Less frequent and smaller updates, as a result of route summarization, also lower convergence time.

Routing Protocol Scalability

Scalability factors include:

- Number of routes
- Number of adjacent neighbors
- Number of routers in the network
- Network design
- Frequency of changes
- Available resources (CPU and memory)

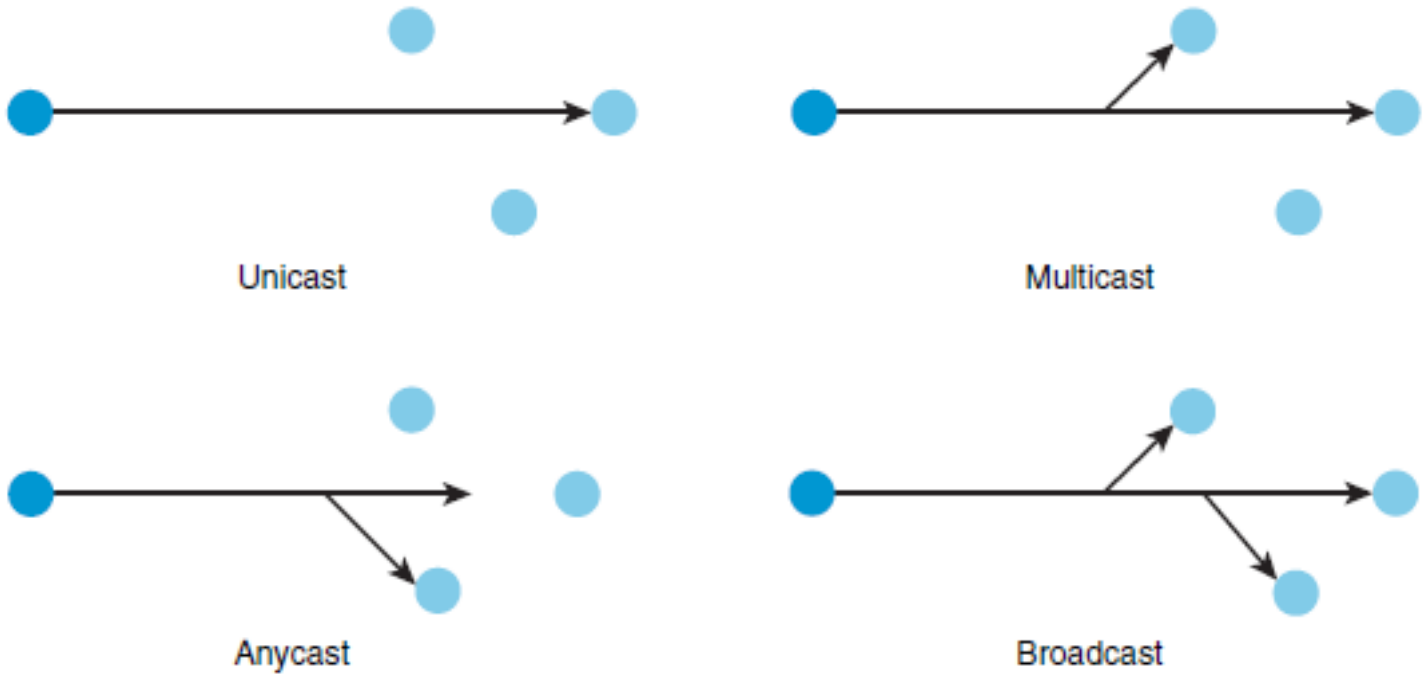
- The scalability of the routing protocol and its configuration options to support a larger network can play an important role when evaluating routing protocols against each other.

Understanding Network Technologies

Understanding Network Technologies

- Differentiate traffic types
- Differentiate IPv6 address types
- Describe ICMPv6 neighbor discovery
- Network Types
- NBMA Networks

Differentiate traffic types



Differentiate traffic types

Unicast

- Unicast addresses are used in a one-to-one context. Unicast traffic is exchanged only between one sender and one receiver.

Multicast

- Multicast addresses identify a group of interfaces across different devices. Traffic that is sent to a multicast address is sent to multiple destinations at the same time.
- IPv6 reserved multicast addresses 224.0.0.0–239.255.255.255.
- IPv6 reserved multicast addresses have the prefix FF00::/8.

Anycast

- An anycast address is assigned to an interface on more than one node. When a packet is sent to an anycast address, it is routed to the nearest interface that has this address. The nearest interface is found according to the measure of distance of the particular routing protocol.

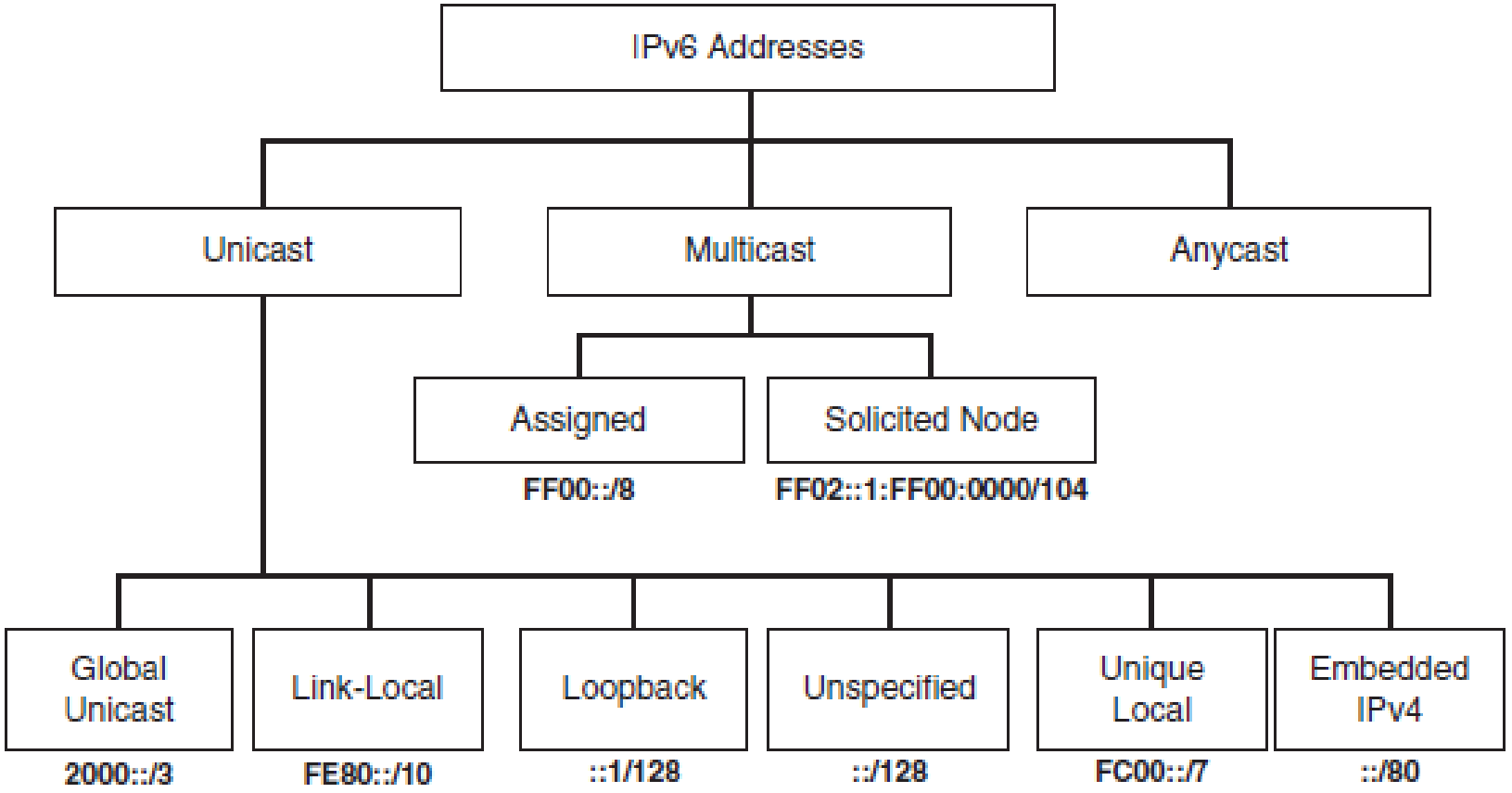
Broadcast

- IPv4 broadcast addresses are used when sending traffic to all devices in the subnet. Local broadcast address 255.255.255.255.
- IPv6 does not use a broadcast address, but uses multicast addresses instead

Well-known IPv4 and Assigned IPv6 Multicast Addresses

IPv4 Multicast Address	Description
224.0.0.5	Used by OSPFv2: All OSPF Routers
224.0.0.6	Used by OSPFv2: All Designated Routers
224.0.0.9	Used by RIPv2
224.0.0.10	Used by EIGRP
IPv6 Multicast Address	**Description**
FF02::5	Used by OSPFv3: All OSPF Routers
FF02::6	Used by OSPFv3: All Designated Routers
FF02::9	Used by RIPng
FF02::A	Used by EIGRP for IPv6

Differentiate IPv6 address types



Describe ICMPv6 neighbor discovery

Router Solicitation (RS)

- Sent by a device to the all IPv6 routers multicast to request a Router Advertisement message from the router.

Router Advertisement (RA)

- Sent by an IPv6 router to the all IPv6 devices multicast. Includes link information such as prefix, prefix-length, and the default gateway address.
- The RA also indicates to the host whether it needs to use a stateless or stateful DHCPv6 server.

Neighbor Solicitation (NS)

- Sent by a device to the solicited node multicast address when it knows the IPv6 address of a device but not its Ethernet MAC address. This is similar to ARP for IPv4.

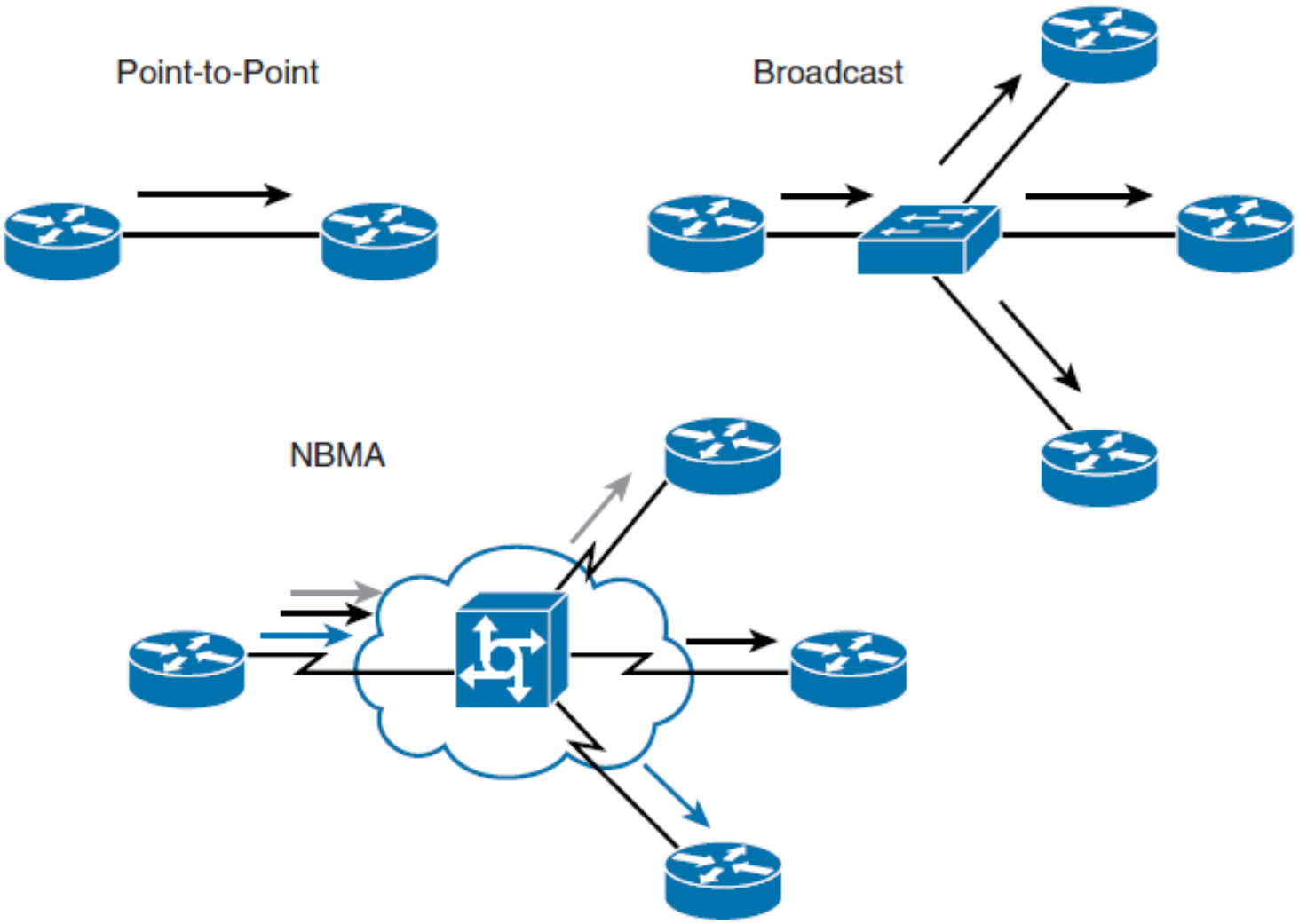
Neighbor Advertisement (NA)

- Sent by a device usually in response to a Neighbor Solicitation message.

Redirect

- This has similar functionality as in IPv4. Sent by a router to inform the source of a packet of a better next-hop router on the link that is closer to the destination.

Network Types



Network Types

Point-to-point network

- A network that connects a single pair of routers.
- A serial link is an example of a point-to-point connection.

Broadcast network

- A network that can connect many routers along with the capability to address a single message to all of the attached routers.
- Ethernet is an example of a broadcast network.

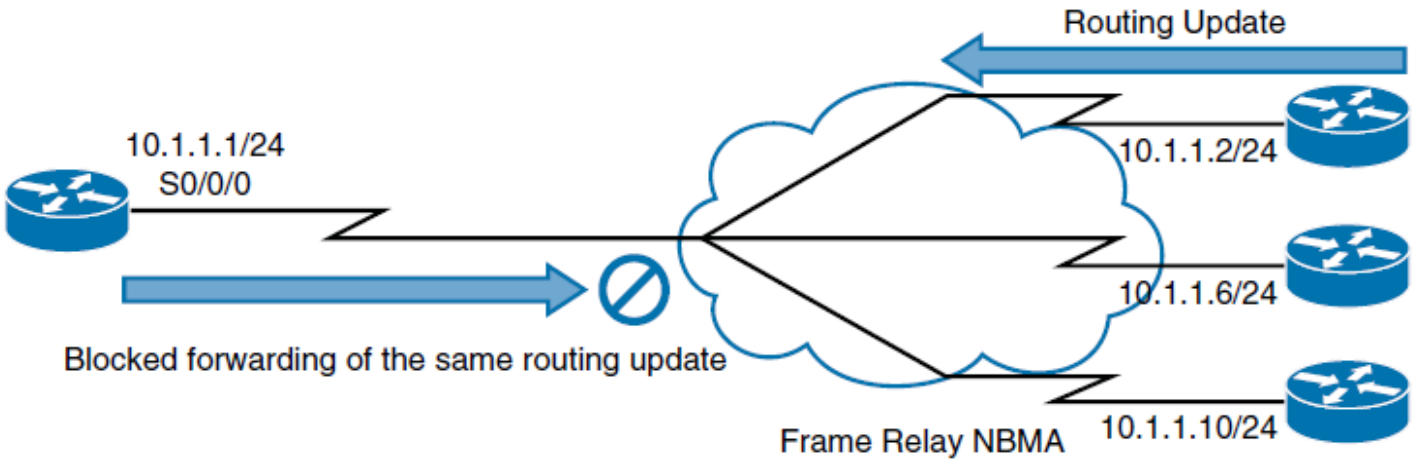
Nonbroadcast Multiaccess (NBMA) network

- A network that can support many routers but does not have broadcast capability.
- The sender needs to create an individual copy of the same packet for each recipient if it wishes to inform all connected packet can be transmitted.
- Frame Relay and Asynchronous Transfer Mode (ATM) are examples of an NBMA network type.

NBMA Networks Issues

Split horizon

- Prevents a routing update that is received on an interface from being forwarded out of the same interface.



NBMA Networks Issues

Neighbor discovery

- OSPF over NBMA neighbors are not automatically discovered.
- You can statically configure neighbors, but an additional configuration is required to manually configure the hub as a Designated Router (DR).
- OSPF treats an NBMA network like Ethernet by default

Broadcast replication

- With routers that support multipoint connections over a single interface that terminates at multiple PVCs, the router must replicate broadcast packets.
- These replicated broadcast packets consume bandwidth and cause significant latency variations in user traffic.

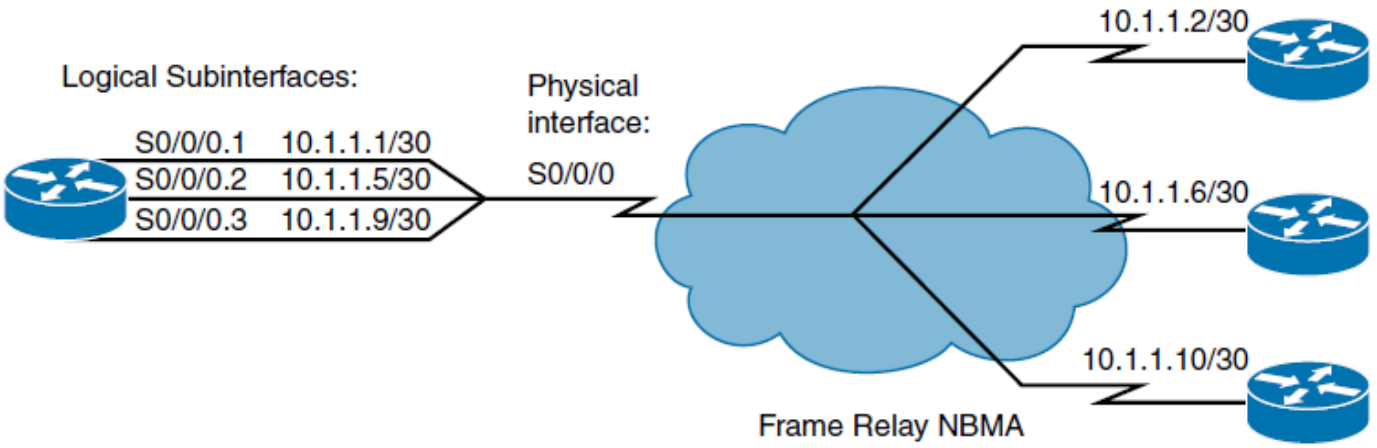
NBMA Networks Issues

Point-to-point subinterfaces

- Each subinterface, which provides connectivity between two routers, uses its own subnet for addressing.

Point-to-multipoint subinterfaces

- One subnet is shared between all virtual circuits.
- Both EIGRP and OSPF need additional configuration to support this underlying technology.



Connecting Remote Locations with Headquarters

Connecting Remote Locations with Headquarters

- Identify options for connecting branch offices and remote locations
- Describe the use of static and default static routes
- Describe basic PPP configuration on point-to-point serial links
- Describe basic Frame Relay on point-to-point serial links
- Explain VRF Lite
- Describe the interaction of routing protocols over MPLS VPNs
- Explain the use of GRE for branch connectivity
- Describe Dynamic Multipoint virtual private networks
- Describe multipoint GRE tunnels
- Describe the Next Hop Resolution Protocol
- Identify the role of IPsec in DMVPN solutions

Principles of Static Routing

A static route can be used in the following circumstances

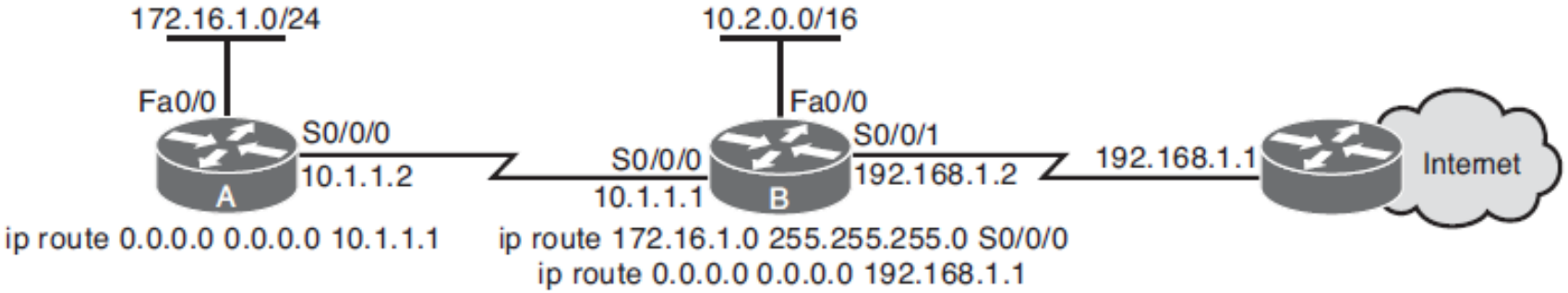
- When it is undesirable to have dynamic routing updates forwarded across slow bandwidth links, such as a dialup link.
- When the administrator needs total control over the routes used by the router.
- When a backup to a dynamically recognized route is necessary.
- When it is necessary to reach a network accessible by only one path (a stub network).
- When a router connects to its ISP and needs to have only a default route.
- When a router is underpowered and does not have the CPU or memory resources necessary to handle a dynamic routing protocol.

Configuring an IPv4 Static Route

ip route *prefix mask* { *address* | *interface* [*address*]} [**dhcp**] [*distance*] [**name** *next-hop-name*] [**permanent** | **track** *number*] [**tag** *tag*]

ip route **Command**	**Description**
prefix mask	The IPv4 network and subnet mask for the remote network to be entered into the IPv4 routing table.
address	The IPv4 address of the next hop that can be used to reach the destination network.
interface	The local router outbound interface to be used to reach the destination network.
dhcp	(Optional) Enables a Dynamic Host Configuration Protocol (DHCP) server to assign a static route to a default gateway (option 3).
distance	(Optional) The administrative distance to be assigned to this route. Must 1 or greater.
name *next-hop-name*	(Optional) Applies a name to the specified route.
permanent	(Optional) Specifies that the route will not be removed from the routing table even if the interface associated with the route goes down.
track *number*	(Optional) Associates a track object with this route. Valid values for the number argument range from 1 to 500.
tag *tag*	(Optional) A value that can be used as a match value in route maps.

Configuring a Static Default Route




```
RouterA# show ip route
<Output omitted>
Gateway of last resort is not set
C    172.16.1.0 is directly connected, FastEthernet0/0
C    10.1.1.0 is directly connected, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 10.1.1.1
```

Basic PPP Overview

- Point-to-Point Protocol (PPP) has several advantages over its predecessor High-Level Data Link Control (HDLC).
  - Authentication
  - Multi-link
  - Compression
  - Quality

```
R1# configure terminal
R1(config)# interface serial 0/0/0
R1(config-if)# encapsulation ppp
```

PPP Authentication Overview

Router(config-if)# **ppp authentication** { **chap** | **chap pap** | **pap chap** | **pap** } [*if-needed*][*list-name* | **default**] [**callin**]

ip route **Command**	**Description**
chap	Enables CHAP on serial interface.
pap	Enables PAP on serial interface.
chap pap	Enables both CHAP and PAP on serial interface, and performs CHAP authentication before PAP.
pap chap	Enables both CHAP and PAP on serial interface, and performs PAP authentication before CHAP.
if-needed (Optional)	Used with TACACS and XTACACS. Do not perform CHAP or PAP authentication if the user has already provided authentication. This option is available only on asynchronous interfaces.
list-name (Optional)	Used with AAA/TACACS+. Specifies the name of a list of TACACS+ methods of authentication to use. If no list name is specified, the system uses the default. Lists are created with the aaa authentication ppp command.
default (Optional)	Used with AAA/TACACS+. Created with the aaa authentication ppp command.
callin	Specifies authentication on incoming (received) calls only.

PPP Configuration Example

Partial running-config for R1:

```
hostname R1
username R2 password sameone
!
interface Serial0/0/0
 ip address 10.0.1.1 255.255.255.252
 ipv6 address 2001:DB8:CAFE:1::1/64
 encapsulation ppp
 ppp authentication pap
 ppp pap sent-username R2 password sameone
```

Partial running-config for R2:

```
hostname R2
username R1 password 0 sameone
!
interface Serial 0/0/0
 ip address 10.0.1.2 255.255.255.252
 ipv6 address 2001:db8:cafe:1::2/64
 encapsulation ppp
 ppp authentication pap
 ppp pap sent-username R2 password sameone
```

Partial running-config for R1:

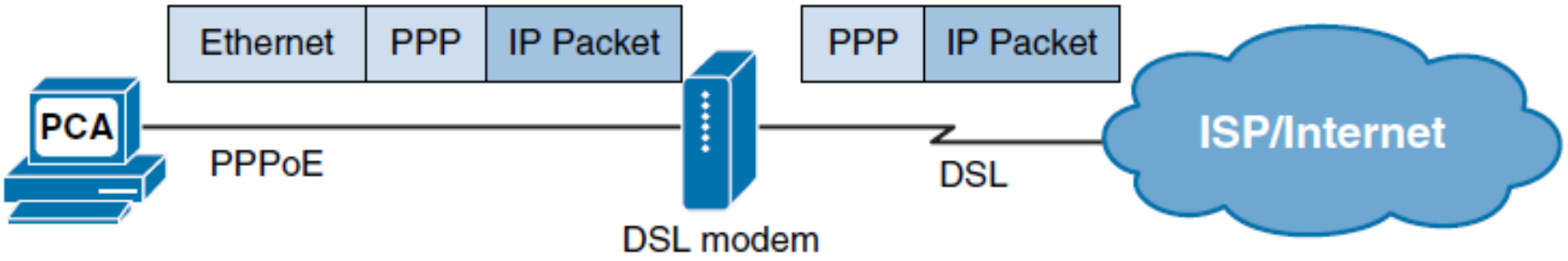
```
hostname R1
username R2 password sameone
!
interface Serial0/0/0
 ip address 10.0.1.1 255.255.255.252
 ipv6 address 2001:DB8:CAFE:1::1/64
 encapsulation ppp
 ppp authentication chap
```

Partial running-config for R2:

```
hostname R2
username R1 password 0 sameone
!
interface Serial 0/0/0
 ip address 10.0.1.2 255.255.255.252
 ipv6 address 2001:db8:cafe:1::2/64
 encapsulation ppp
 ppp authentication chap
```

PPPoE

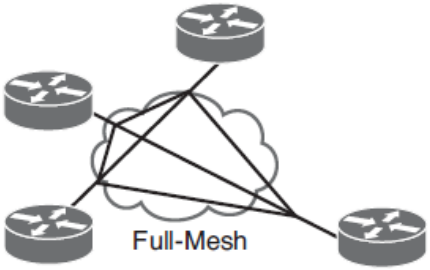
```
interface Dialer 2
 encapsulation ppp          !  1. PPP and IP on the Dialer
 ip address negotiated

_ppp chap hostname Bob      !  2. Authenticate inbound only
 ppp chap password D1@ne

 ip mtu 1492
 dialer pool 1                      !  3. Dialer pool must match

interface Ethernet0/1
 no ip address
 pppoe enable
 pppoe-client dial-pool-number 1    !  3. Dialer pool must match
```

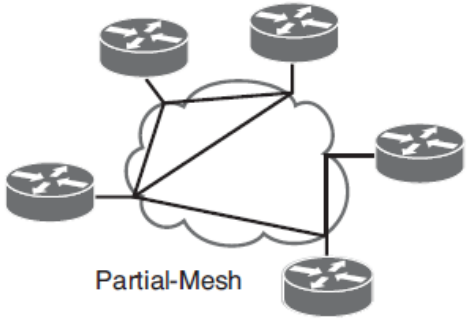


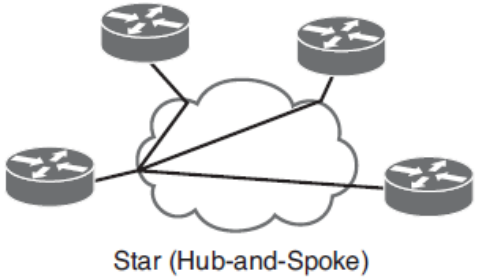
Basic Frame Relay Overview

- Frame Relay provides several benefits over traditional point-to-point leased lines
  - No need for separate physical interface per connection on the router
  - Bandwidth cost is much more flexible
- Frame Relay is a switched WAN technology where virtual circuits (VCs) are created by a service provider (SP) through the network.
  - The VCs are typically PVCs that are identified by a data-link connection identifier (DLCI)
- By default, a Frame Relay network is an NBMA network.
  - To emulate the LAN broadcast capability that is required by IP routing protocols Cisco IOS implements pseudo-broadcasting
  - Dynamic maps always allow pseudo-broadcasting.
- Dynamic maps created via Frame Relay Inverse Address Resolution Protocol (INARP) for IPv4 or Frame Relay Inverse Neighbor Discovery (IND) for IPv6
- Split horizon is disabled by default on Frame Relay physical interfaces.

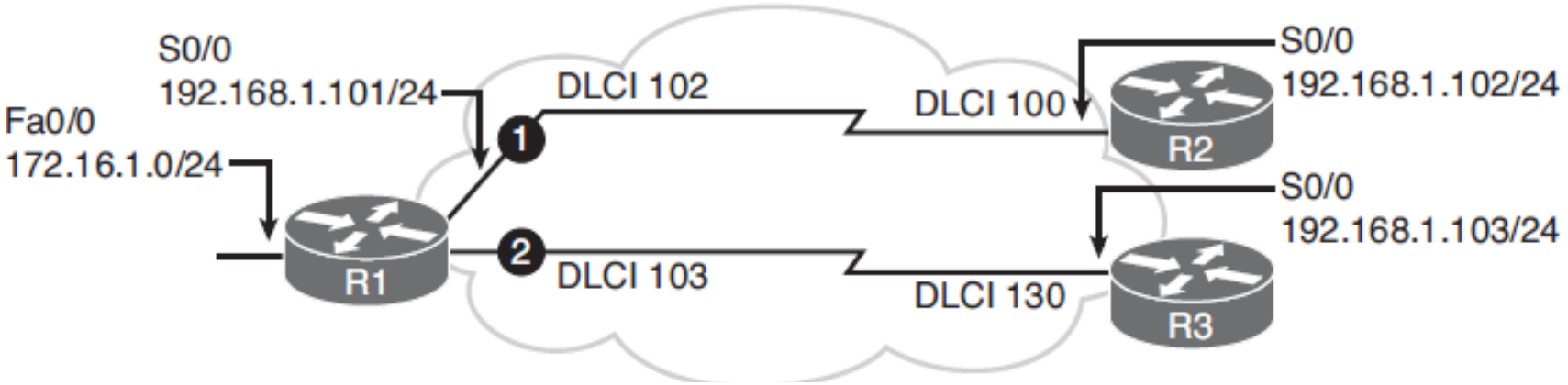
Frame Relay Topologies







Basic Frame Relay Configuration




```
interface Serial0/0
 encapsulation frame-relay
 ip address 192.168.1.101 255.255.255.0
!
router eigrp 110
 network 172.16.1.0 0.0.0.255
 network 192.168.1.0
```

VPN Connectivity Overview

- MPLS-based VPNs
- Tunneling VPNs
  - GRE
  - Ipsec
  - DMVPN

L3 MPLS VPNs

- Traffic forwarding through the MPLS backbone is based on labels that are previously distributed among the core routers.
- With a Layer 3 MPLS VPN, the service provider participates in customer routing.
- The service provider establishes routing peering between the PE and CE routers.
- Then customer routes that are received on the PE router are redistributed into MP-BGP and conveyed over the MPLS backbone to the remote PE router.
- On the remote PE, these customer routes are redistributed back from MP-BGP into a remote PE-CE routing protocol.
- Routing protocols between PE-CE routers on the local and remote sites may be totally different.

L2 MPLS VPNs

- A Layer 2 MPLS VPN CE router interconnects with the PE router at Layer 2 using any Layer 2 protocol with Ethernet being the most common.
- Layer 2 traffic is sent between PE routers, over a pre-established pseudowire.
- Pseudowire emulates a wire between PE routers that carries Layer 2 frames across the IP-MPLS backbone.
- There are two basic Layer 2 MPLS VPN service architectures.
  - Virtual Private Wire Service (VPWS) is a point-to-point technology that allows the transport of any Layer 2 protocol at the PE.
  - The second type of Layer 2 MPLS VPN is Virtual Private LAN Service (VPLS), which emulates an Ethernet multiaccess LAN segment over the MPLS core and provides multipoint- to-multipoint service.

Tunneling VPNs

GRE

- Tunneling protocol developed by Cisco that enables encapsulation of arbitrary Layer 3 protocols inside a point-to-point, tunnel-over-IP network.
- Traffic that is transported over the GRE tunnel is not encrypted
- GRE traffic is usually encapsulated within IPsec.

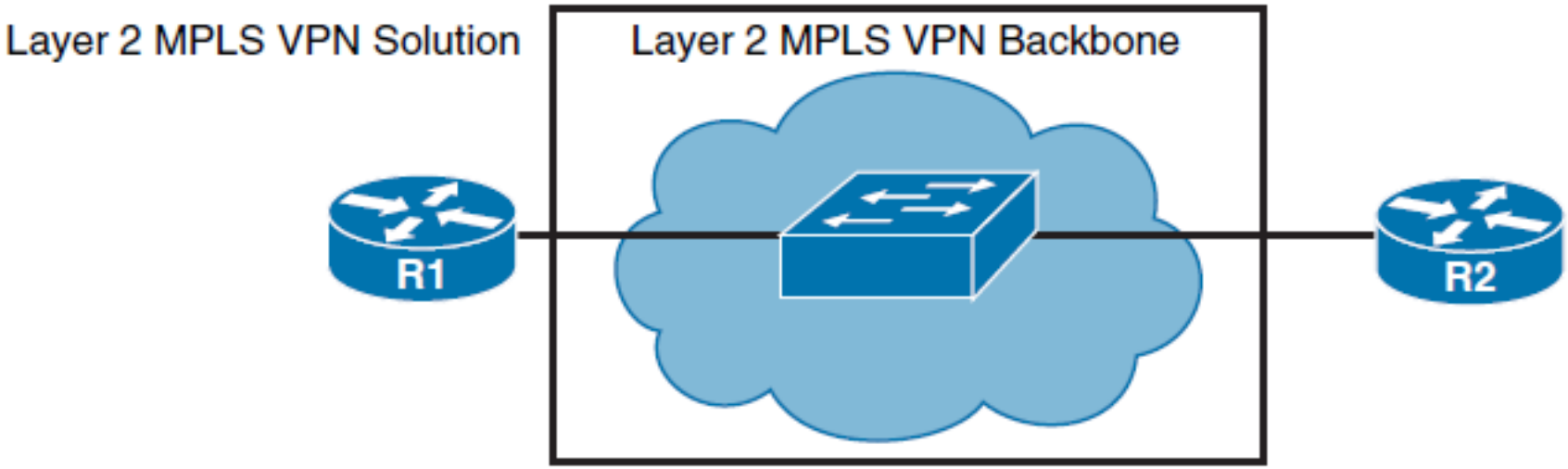
IPsec

- Is a framework that uses a set of cryptographic protocols to secure traffic at Layer 3.

DMVPN

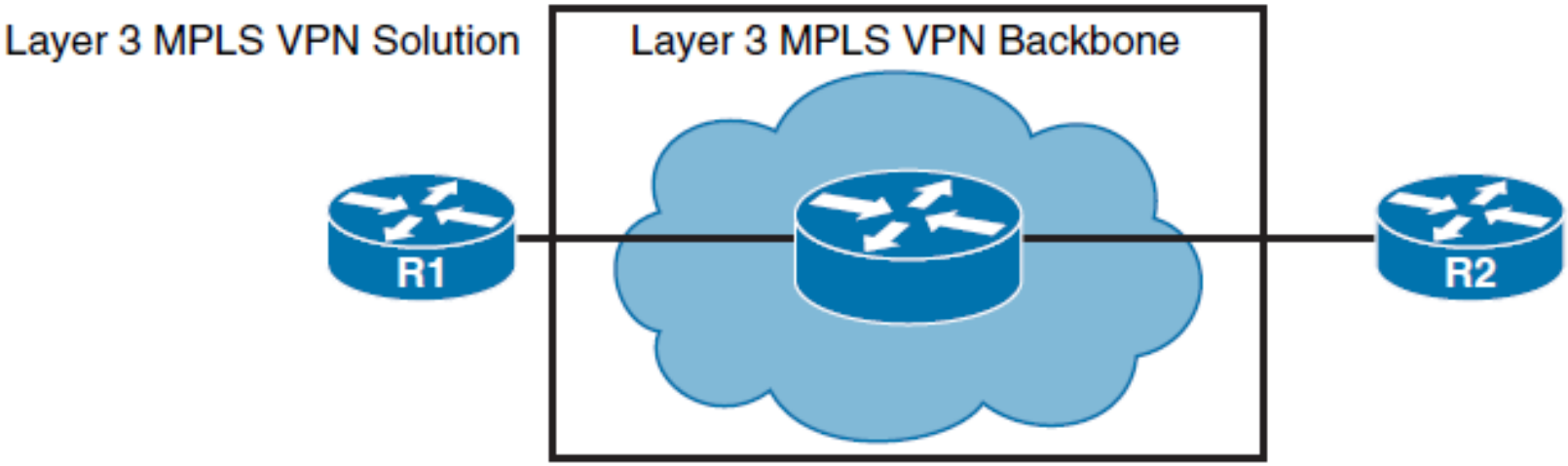
- This solution offers the capability to dynamically establish hub-to-spoke and spoke-to-spoke IPsec tunnels, thus reducing latency and optimizing network performance.
- DMVPN supports dynamic routing protocols between hub and spokes as well as IP multicast. It is also suitable for environments with dynamic IP addresses on physical interfaces such as DSL or cable connections.

Routing Across MPLS VPNs



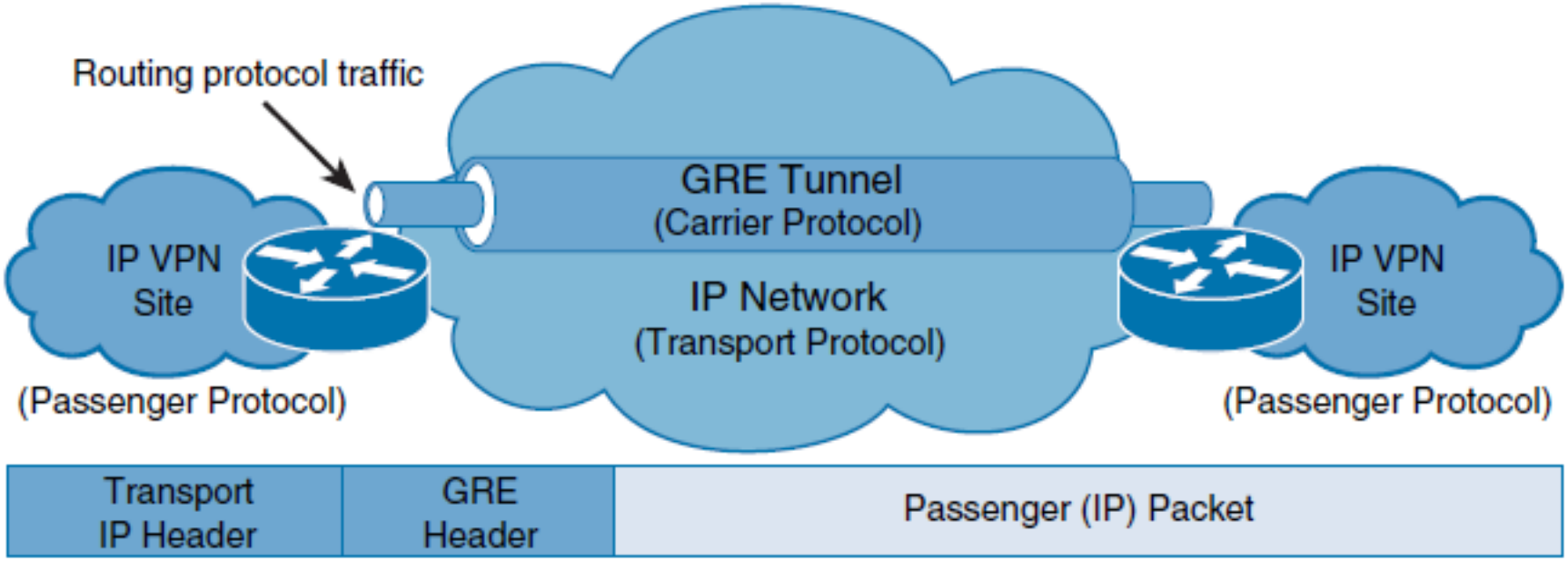
- The Layer 2 MPLS VPN backbone solution is providing the Layer 2 service across the backbone, where R1 and R2 are connected together directly using the same IP subnet.
- If you deploy a routing protocol over the Layer 2 MPLS VPN, neighbor adjacency is established between your R1 and R2 routers. The figure presents the connectivity through the backbone, which can be illustrated as one big switch.

Routing Across MPLS VPNs



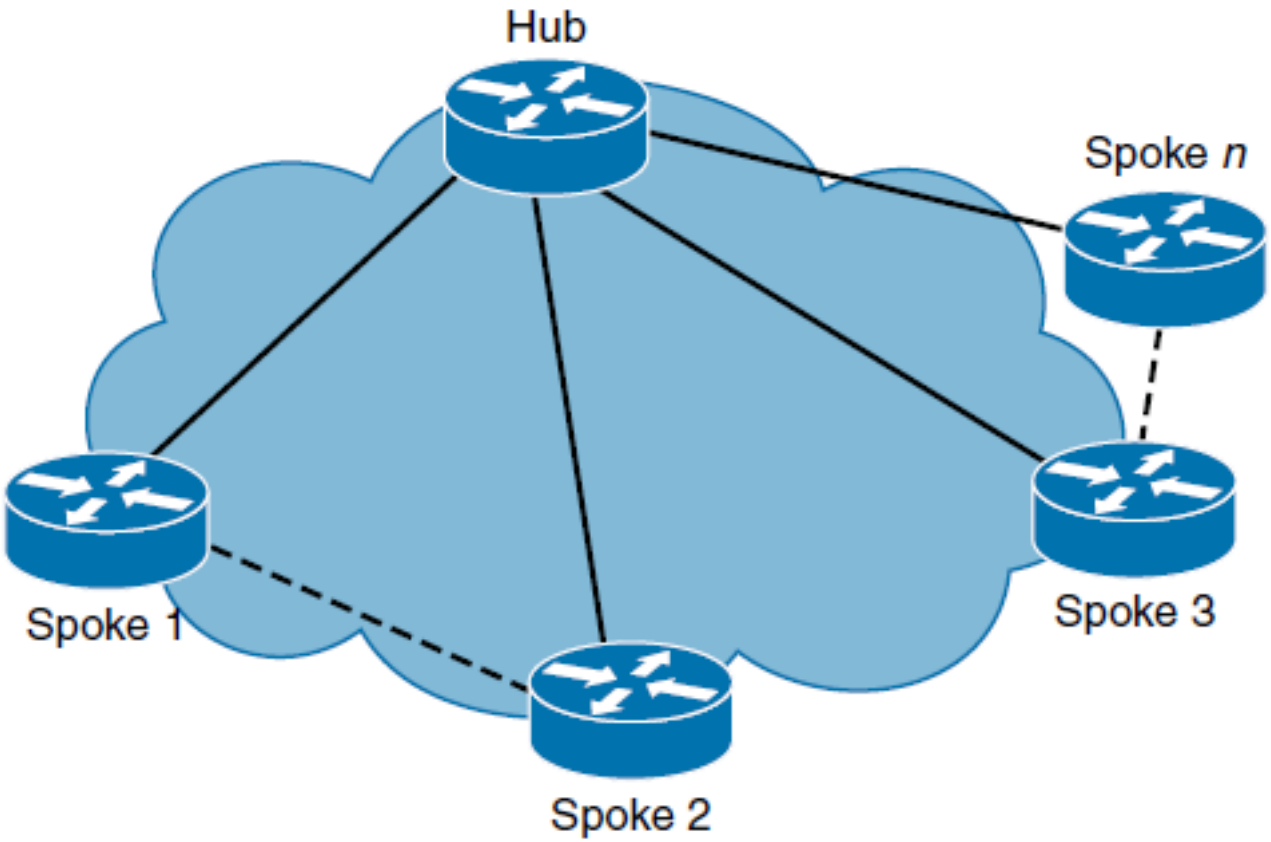
- The Layer 3 MPLS VPN backbone solution is providing the Layer 3 service across the backbone, where R1 and R2 are connected to ISP edge routers.
- A separate IP subnet is used on each side. If you deploy a routing protocol over this VPN, service providers need to participate in it.
- Neighbor adjacency is established between your R1 and the closest PE router and between your R2 and it's closest PE router.

Routing Over GRE Tunnel



- A **passenger protocol** or encapsulated protocol, such as IPv4 or IPv6 that is being encapsulated.
- A **carrier protocol**, GRE in this example, that is defined by Cisco as a multiprotocol carrier protocol.
- A **transport protocol**, such as IP, that carries the encapsulated protocol.

Dynamic Multipoint Virtual Private Network



DMVPN

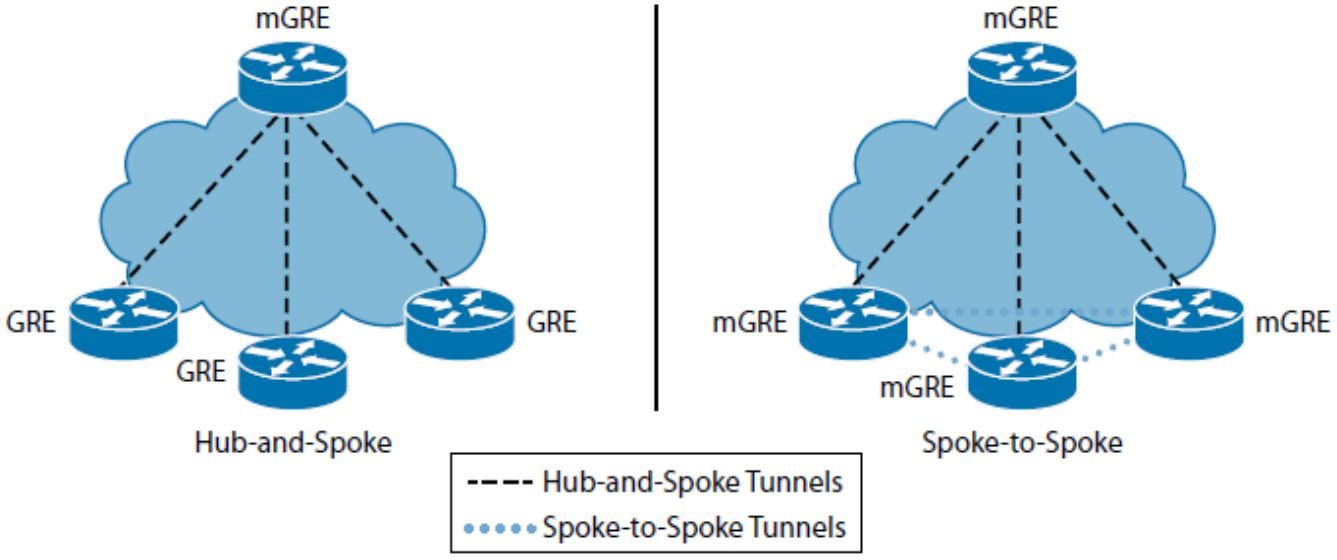
The primary benefits of DMVPNs follow:

- **Hub router configuration reduction**
  - Traditionally, the individual configuration of a GRE tunnel and IPsec would need to be defined for each individual spoke router. The DMPVN feature enables the configuration of a single mGRE tunnel interface and a single IPsec profile on the hub router to manage all spoke routers
- **Automatic IPsec initiation**
  - GRE uses NHRP to configure and resolve the peer destination address. This feature allows IPsec to be immediately triggered to create point-to-point GRE tunnels without any IPsec peering configuration.
- **Support for dynamically addressed spoke routers**
  - When using point-to-point GRE and IPsec hub-and-spoke VPN networks, it is important to know the physical interface IP address of the spoke routers when configuring the hub router.
  - DMVPN enables spoke routers to have dynamic physical interface IP addresses and uses NHRP to register the dynamic physical interface IP addresses of the spoke routers with the hub router.

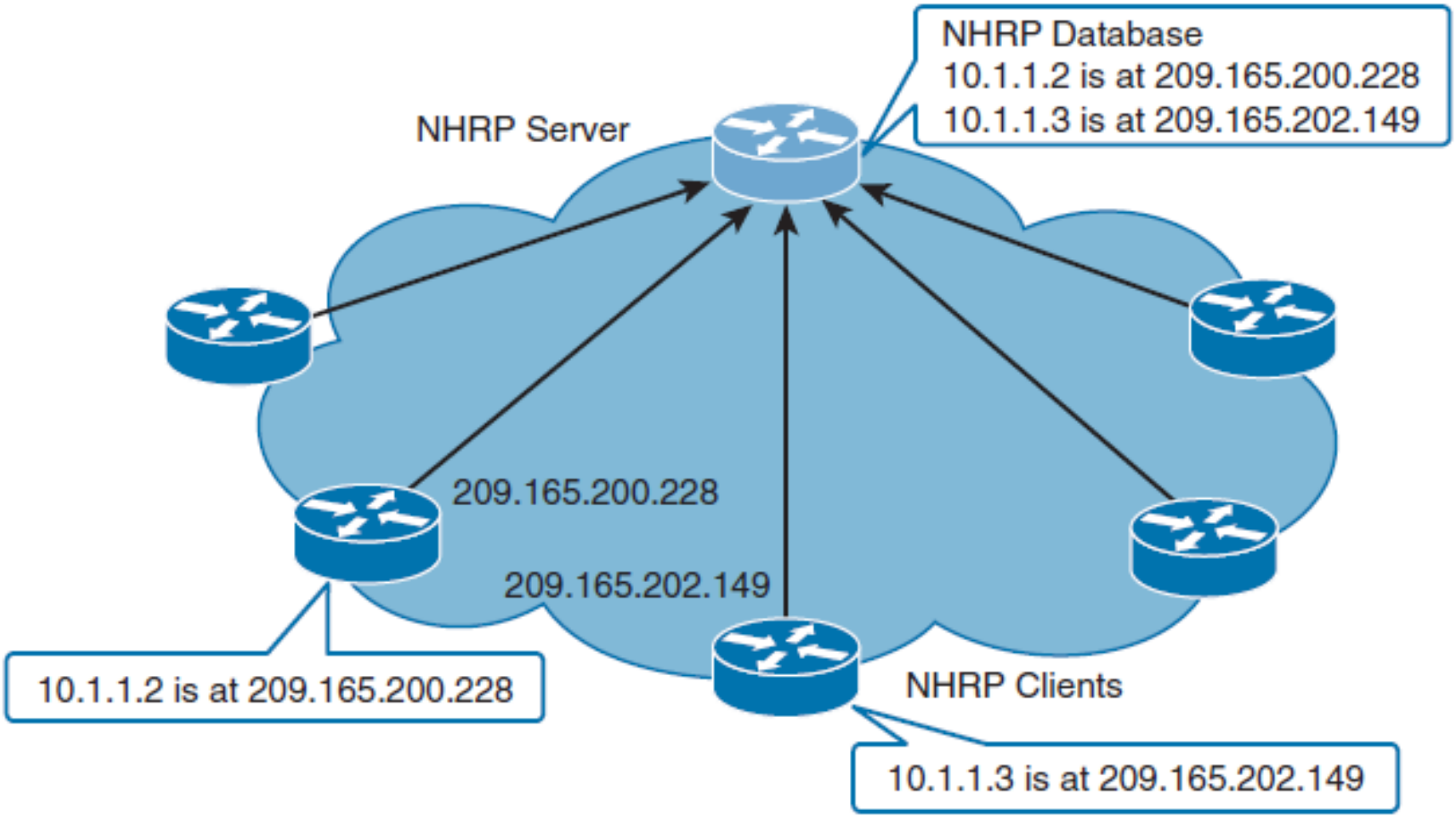
Multipoint GRE

The main characteristics of the mGRE configuration are as follows:

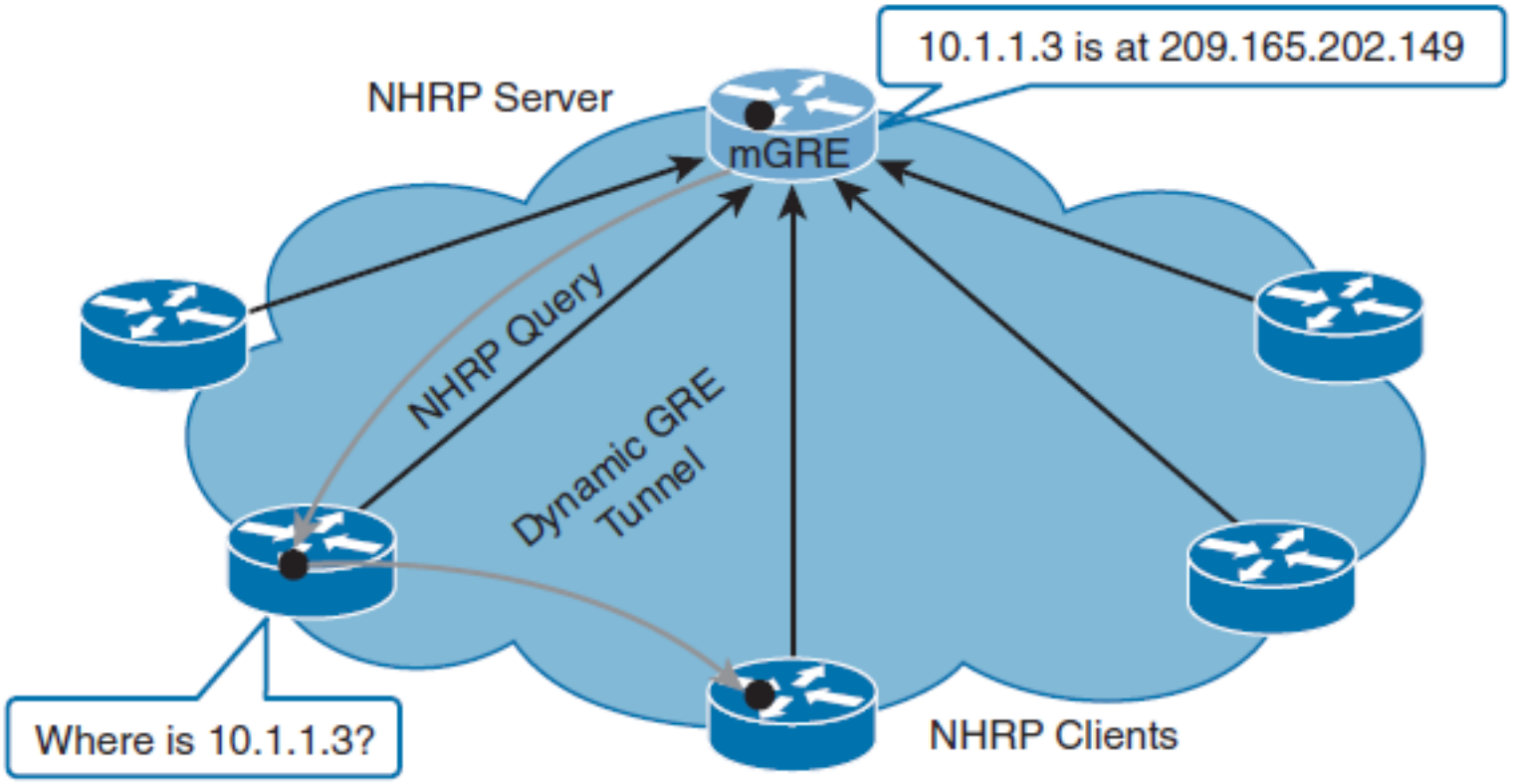
- Only one tunnel interface needs to be configured on a router to support multiple remote GRE peers
- To learn the IP addresses of other peer, devices using mGRE require NHRP to build dynamic GRE tunnels.
- mGRE interfaces also support unicast, multicast, and broadcast traffic.



NHRP



NHRP

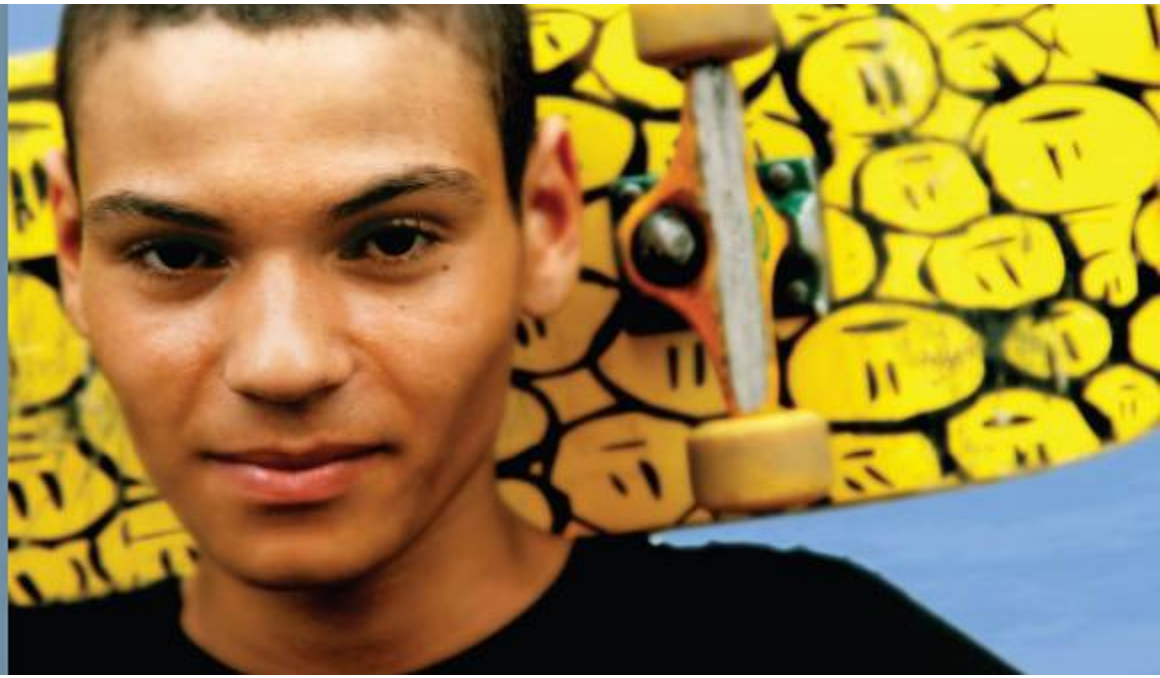


IPsec

IPsec provides four important security services:

- **Confidentiality (encryption)**
  - No one can eavesdrop on the communication. If the communication is intercepted, it cannot be read.
- **Data integrity**
  - The receiver can verify that the data was transmitted through the path without being changed or altered in any way.
- **Authentication**
  - Authentication ensures that the connection is made with the desired communication partner. IPsec uses Internet Key Exchange (IKE) to authenticate users and devices that can carry out communication independently.
- **Antireplay protection**
  - Antireplay protection verifies that each packet is unique and not duplicated.

Routing and TCP/IP Operations



Routing and TCP/IP Operations

- MSS, Fragmentation, and PMTUD
- IPv4 Fragmentation and PMTUD
- Bandwidth Delay Product
- TCP Starvation
- Latency
- ICMP Redirect

MSS, Fragmentation, and PMTUD

- An IPv4 packet has a maximum size of 65,535 bytes
- An IPv6 packet with a hop-by-hop extension header and the jumbo payload option can support up to 4,294,967,295 bytes
- However, most transmission links enforce a smaller maximum packet length called the *maximum transmission unit* (MTU).
- When a router receives an IPv4 packet larger than the MTU of the egress or outgoing interface, it must fragment the packet unless the DF (Don't Fragment) bit is set in the IPv4 header.

MSS, Fragmentation, and PMTUD

Fragmentation causes several issues including the following:

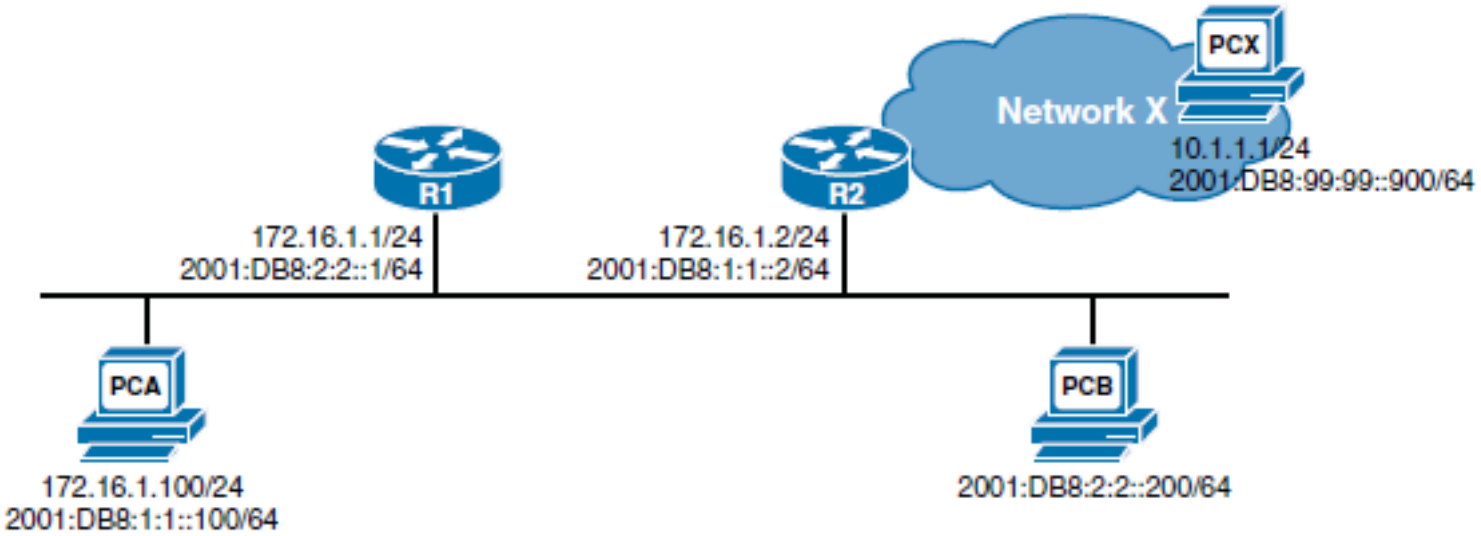
- CPU and memory overhead in fragmentation of the packet
- CPU and memory overhead in destination devices during reassembly of packets
- Retransmission of the entire packet when one fragment is dropped
- Firewalls that do Layer 4 through Layer 7 filtering may have trouble processing IPv4 fragments correctly

IPv4 Fragmentation and PMTUD

- TCP Maximum Segment Size (MSS) defines the largest amount of data that the receiving device is able to accept in a single TCP segment.
- To avoid fragmentation of an IPv4 packet, the selection of the TCP MSS is the minimum buffer size and MTU of the outgoing interface minus 40 bytes. The 40 bytes take into account the 20-byte IPv4 header and the 20-byte TCP header.
- The TCP MSS helps avoid fragmentation at the two ends of the TCP connection but it does not prevent fragmentation due to a smaller MTU on a link along the path.
- Path MTU Discovery (PMTUD) was developed for the purpose of determining the lowest MTU along a path from the packet's source to destination.
- PMTUD is only supported by TCP.

ICMP Redirect

- ICMPV4 Redirect messages are used by routers to notify the sender of a packet that there is a better route available for a particular destination.
- Similar to IPv4, R1 will forward the IPv6 packet to PCB, but unlike ICMP for IPv4, it will send an ICMPv6 redirect message to PCA informing the source of the better route. PCA can now send subsequent IPv6 packets directly to PCB even though it is on a different IPv6 network.



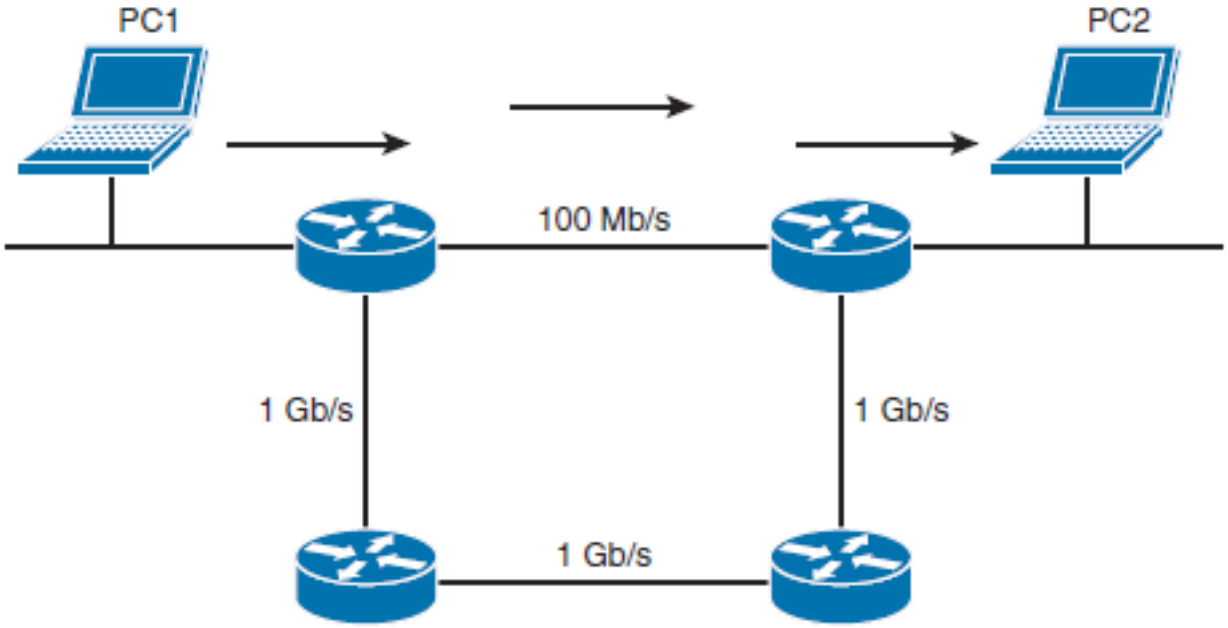
Implementing RIPng

- Describe general RIP characteristics
- Describe how to configure and verify basic RIPng
- Describe how to configure RIPng to share default routes
- Analyze the RIPng database

RIP Overview

- RIP is an IGP that is used in smaller networks.
- It is a distance vector routing protocol that uses hop count as a routing metric.
- There are three versions of RIP: RIPv1, RIPv2, and RIPng. RIPv1 and RIPv2 route in IPv4 networks.
- RIPng routes in IPv6 networks.
- RIP is a standardized IGP routing protocol that works in a mixed-vendor router environment.

RIP Overview



- RIP uses hop count, the number of routers, as the metric.
- If a device has two paths to the destination network, the path with fewer hops will be chosen as the path to forward traffic.
- If a network is 16 or more hops away, the router considers it unreachable.

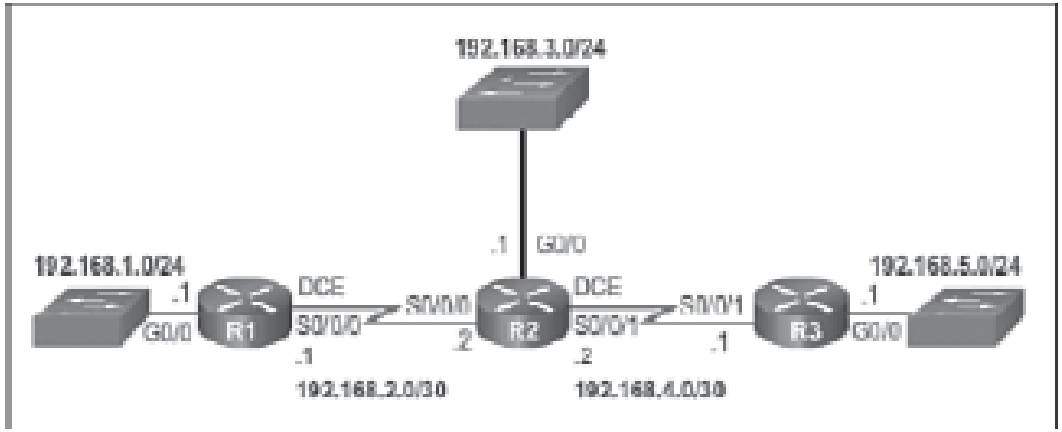
RIP Overview

- As a routing loop-prevention technique, RIP implements split horizon. Split horizon prevents routing information from being sent out the same interface from which it was received.
- Split horizon with poison reverse is a similar technique but sends the update with a metric of 16, which is considered unreachable by RIP.
- RIP is also capable of load balancing traffic over equal-cost paths.
- The default is four equal-cost paths.
- If the maximum number of paths is set to one, load balancing is disabled.

Comparing Features in RIPv2 and RIPng

Feature	RIPv2	RIPng
Advertise routes	IPv4	IPv6
Transport protocol	UDP (port 520)	UDP (port 521)
Multicast address used	224.0.0.9	FF02::9
VLSM support	Yes	Yes
Metric Administrative Distance	Hop count (maximum of 15) 120	Hop count (maximum of 15) 120
Routing updates	Every 30 seconds and with topology change	Every 30 seconds and with topology change
Authentication support	Yes	Yes

RIPv2 Configuration




```
R1(config)# router rip
R1(config-router)# network 192.168.1.0
R1(config-router)# network 192.168.2.0
R1(config-router)# version 2
R1(config-router)#
```

RIPv2 Configuration

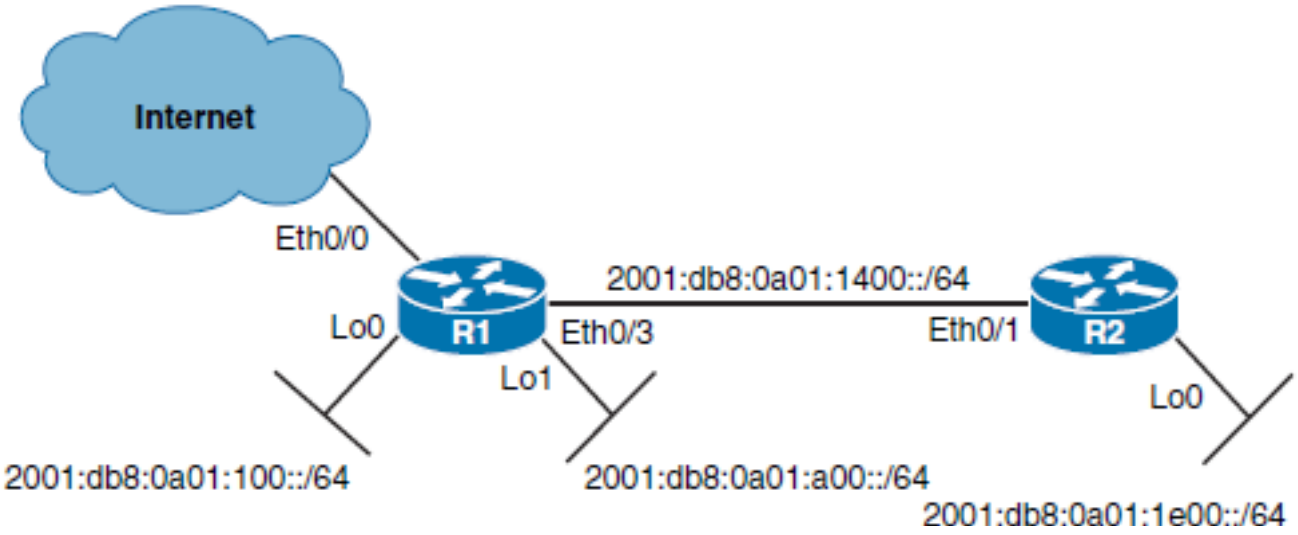
- By default, RIPv2 automatically summarizes networks at major network boundaries, summarizing routes to the classful network address
- When route summarization is disabled, the software sends subnet routing information across classful network boundaries.

```
Router(config-router)# no auto-summary
```

- The **ip summary-address rip** *ip-address network-mask* interface command is used to summarize an address or subnet under a specific interface.

```
Router(config-if)# ip summary-address rip 10.2.0.0 255.255.0.0
```

Configuring RIPng




```
R2> enable
R2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)# ipv6 unicast-routing
```

```
R2(config)# ipv6 router rip CCNP_RIP
```

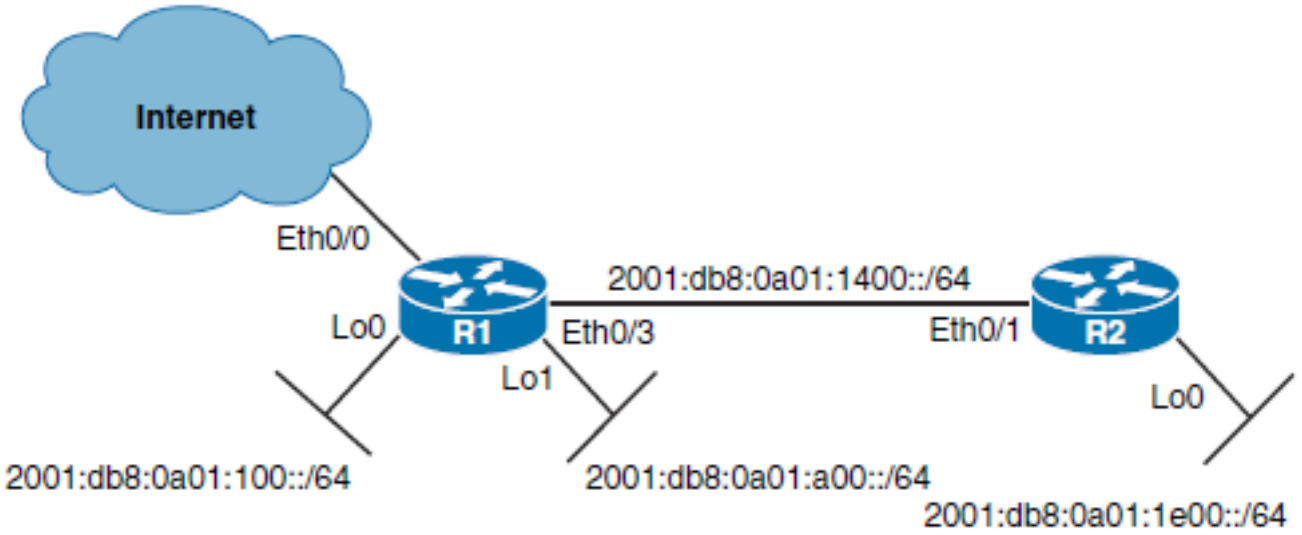
```
R2(config)# interface ethernet 0/1
R2(config-if)# ipv6 rip CCNP_RIP enable
R2(config-if)# interface loopback 0
R2(config-if)# ipv6 rip CCNP_RIP enable
```

Verify RIPng Configuration

```
R2# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "rip CCNP_RIP"
  Interfaces:
    Loopback0
    Ethernet0/1
  Redistribution
    None
```

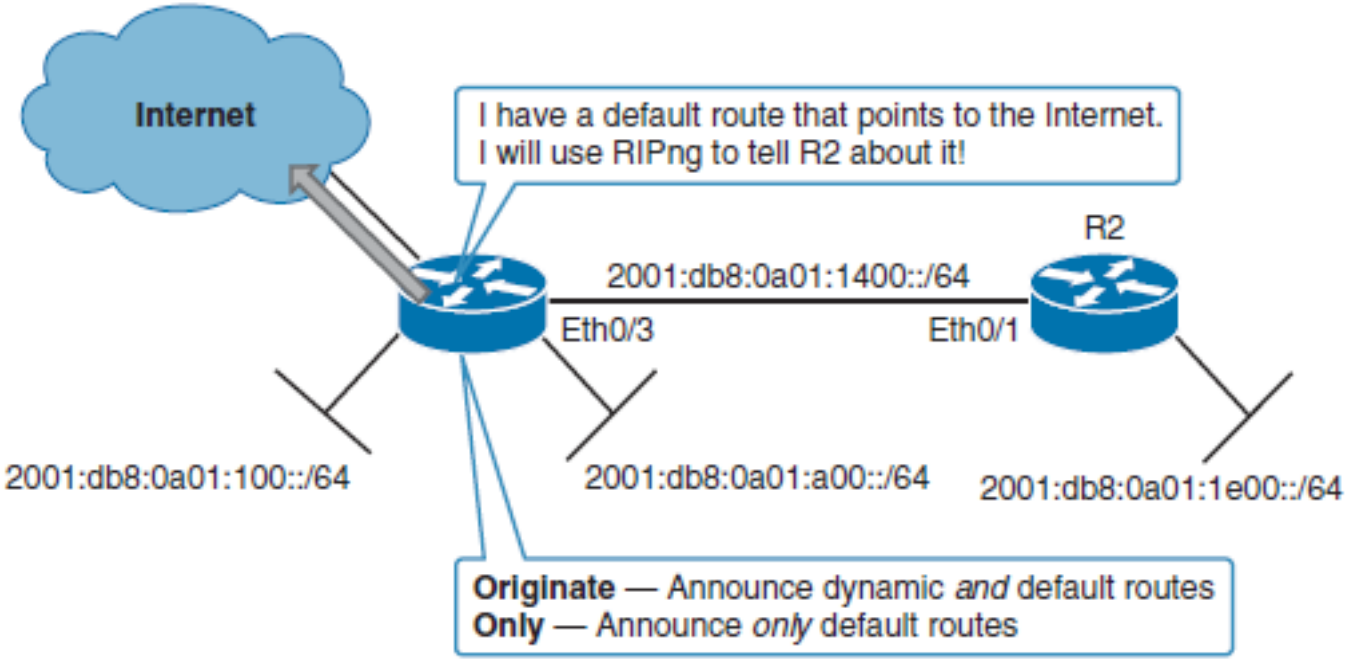
```
R2# show ipv6 route
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
R   2001:DB8:A01:100::/64 [120/2]
     via FE80::A8BB:CCFF:FE00:130, Ethernet0/1
R   2001:DB8:A01:A00::/64 [120/2]
     via FE80::A8BB:CCFF:FE00:130, Ethernet0/1
C   2001:DB8:A01:1400::/64 [0/0]
     via Ethernet0/1, directly connected
```

RIPng Summarization




```
R1(config)# interface Ethernet 0/3
R1(config-router)# ipv6 rip CCNP_RIP 2001:db8:A01::/52
```

Propagating a Default Route




```
R1(config-if)# ipv6 rip name default-information originate | only
```

```
R1(config)# interface Ethernet 0/3
R1(config-if)# ipv6 rip CCNP_RIP default-information originate
```

RIPng Verification Commands

```
R2#show ipv6 rip
RIP process "CCNP_RIP", port 521, multicast-group FF02::9, pid 138
     Administrative distance is 120. Maximum paths is 16
     Updates every 30 seconds, expire after 180
     Holddown lasts 0 seconds, garbage collect after 120
     Split horizon is on; poison reverse is off
     Default routes are not generated
     Periodic updates 308, trigger updates 1
     Full Advertisement 0, Delayed Events 0
  Interfaces:
    Loopback0
    Ethernet0/1
  Redistribution:
    None
R2#
```

```
R2# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "rip CCNP_RIP"
  Interfaces:
    Loopback0
    Ethernet0/1
  Redistribution:
    None
```

RIPng Verification Commands

```
R2# show ipv6 route rip
IPv6 Routing Table - default - 9 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
R    ::/0 [120/2]
     via FE80::A8BB:CCFF:FE00:130, Ethernet0/1
R    2001:DB8:A01:100::/64 [120/2]
     via FE80::A8BB:CCFF:FE00:130, Ethernet0/1
R    2001:DB8:A01:A00::/64 [120/2]
     via FE80::A8BB:CCFF:FE00:130, Ethernet0/1
```

```
R2# show ipv6 rip next-hops
 RIP process "CCNP_RIP", Next Hops
  FE80::A8BB:CCFF:FE00:7430/Ethernet0/1 [3 paths]
R2#
```

Investigating the RIPng Database

```
R2# show ipv6 rip database
RIP process "CCNP_RIP", local RIB
 2001:DB8:A01:100::/64, metric 2, installed
     Ethernet0/1/FE80::A8BB:CCFF:FE00:7430, expires in 155 secs
 2001:DB8:A01:A00::/64, metric 2, installed
     Ethernet0/1/FE80::A8BB:CCFF:FE00:7430, expires in 155 secs
 2001:DB8:A01:1400::/64, metric 2
     Ethernet0/1/FE80::A8BB:CCFF:FE00:7430, expires in 155 secs
R2#
```

- The RIP process (there can be multiple RIPng processes on a single router).
- The route prefix.
- The route metric, in which RIPng uses hop count as a metric. In the example, all three routes have a metric of 2. This means the destination network is 2 hops away, counting itself as a hop.
- Installed and expired, in which the keyword “installed” means the route is in the routing table. If a network becomes unavailable, the route will become “expired” after the dead timer expires. An expired route value (in seconds), during which the route will be advertised as expired, is listed.
- Expires in, in which if the countdown timer reaches 0, the route is removed from the routing table and marked expired. This timer, the dead timer, is by default three times the hello timer—180 seconds.

Chapter 1 Summary

- The role of static routes and dynamic routing protocols in enterprise networks.
- The differences between IGP and EGP routing protocols.
- The three types of routing protocols: distance vector, link-state and path vector.
- The importance of convergence time and how route summarization reduced convergence time and improves scalability.
- The four traffic types: unicast, multicast, anycast, and broadcast.
- The differences between point-to-point, broadcast, and NBMA networks.
- How point-to-point subinterfaces are used to overcome the limitations of NBMA networks.
- How VPNs are used to provide security of a public Internet.
- Common types of VPNs: MPLS-based VPNs, GRE+IPsec, and DMVPN.
- How a customer establishes connectivity with a service provider using a routing protocol and a layer 3 MPLS VPN.
- How static GRE tunnels can establish virtual point-to-point links and support dynamic routing protocols.
- Using DMVPN to provide fully meshed VPN connectivity with a simple hub-andspoke configuration.
- How DMVPN relies on NHRP, mGRE, and IPsec.
- The differences and similarities between RIPv2 and RIPng.
- How to configure RIPng.
- How to propagate a default route in RIPng.

Chapter 1 Labs

- **CCNPv7_ROUTE_Lab1-1_RIPng**

Acknowledgment

- Some of images and texts are from Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide by Diane Teare, Bob Vachon and Rick Graziani (1587204568)

- Special Thanks to *Bruno Silva*