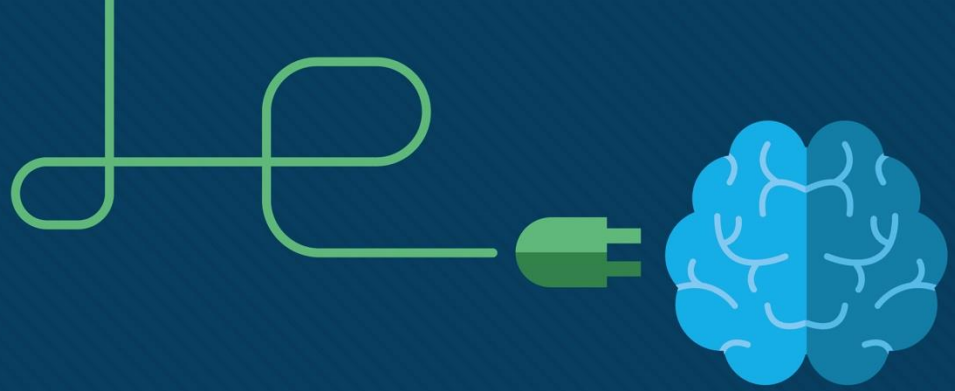


Module 0
Enterprise Networks

ITNET04

WAN Connectivity

Module Objectives

Module Title: Enterprise Networks

Module Objectives:

- Be familiar with the outcomes and policies of the ITNET04 course
- Explain the factors that drive the need to scale a network and the effects to a hierarchical network topology
- Review basic concepts on dynamic routing

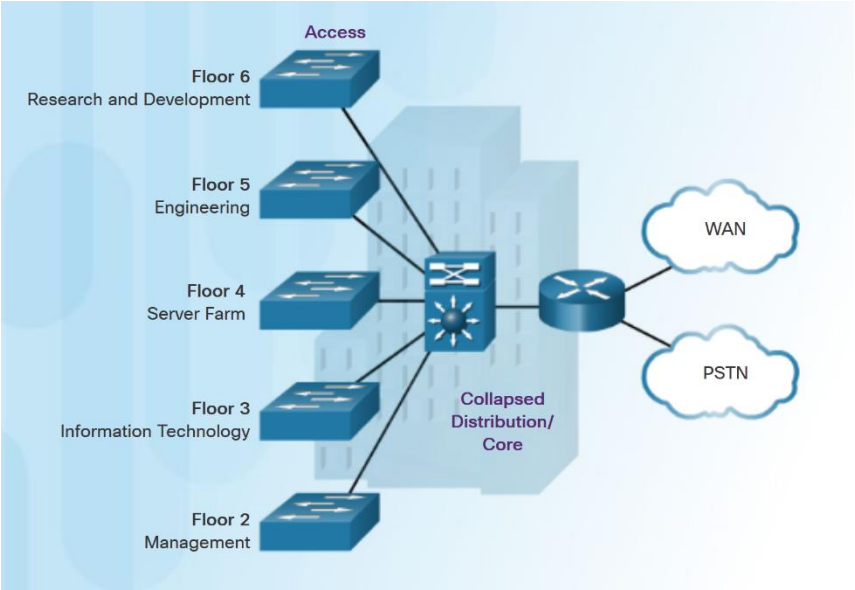
Growing a Network

Recall: What is a ‘WAN’?

Wide Area Network

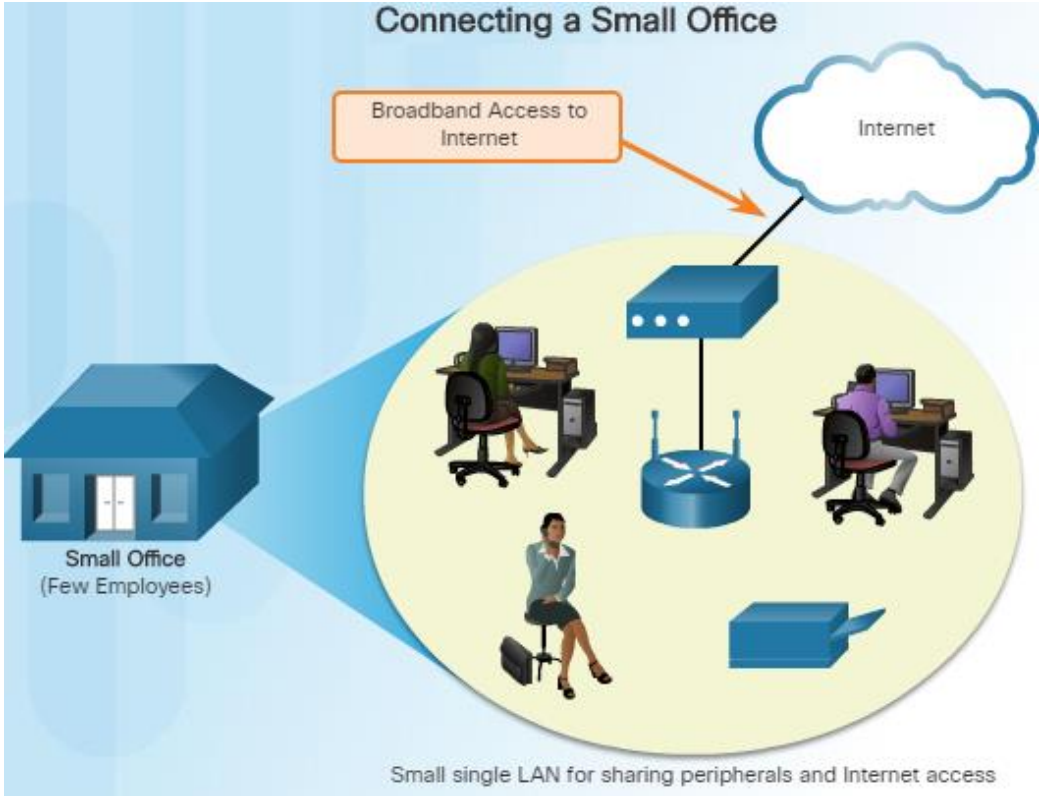
A network connection that spans across a large geographical distance

The Need to Scale the Network



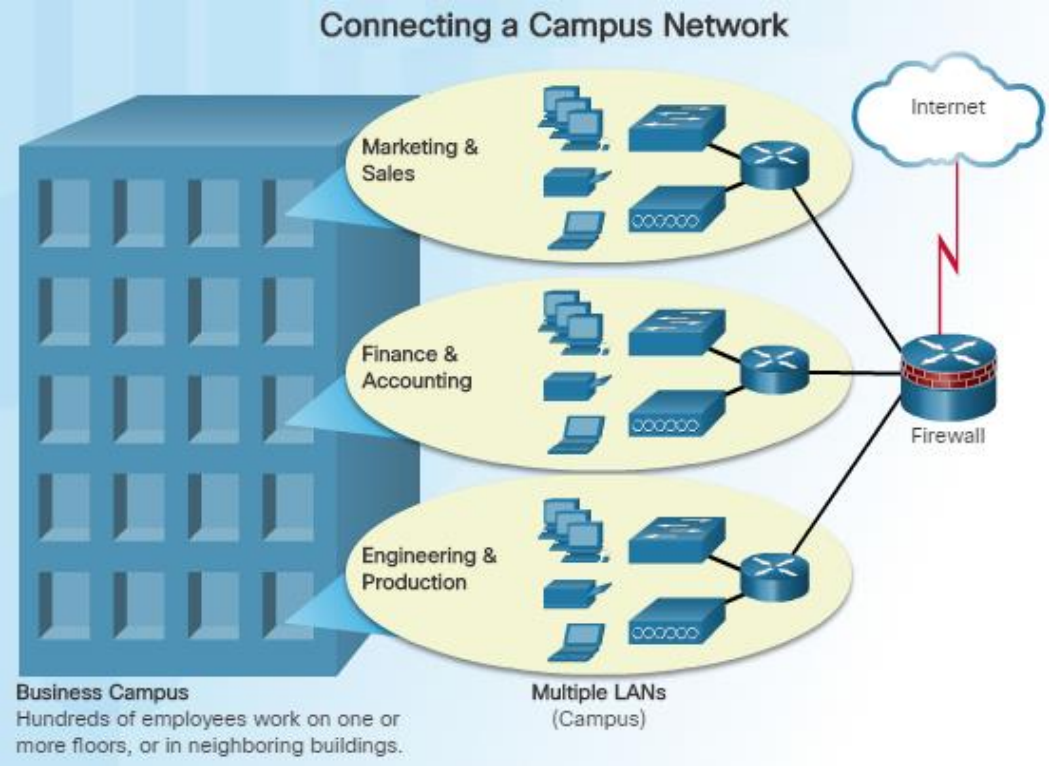
- All enterprise networks must:
  - Support the exchange of various types of network traffic
  - Support critical applications
  - Support converged network traffic
  - Support diverse business needs
  - Provide centralized administrative control
- The LAN is the networking infrastructure that provides access to network resources for end users over a single floor or a building.

Small Office



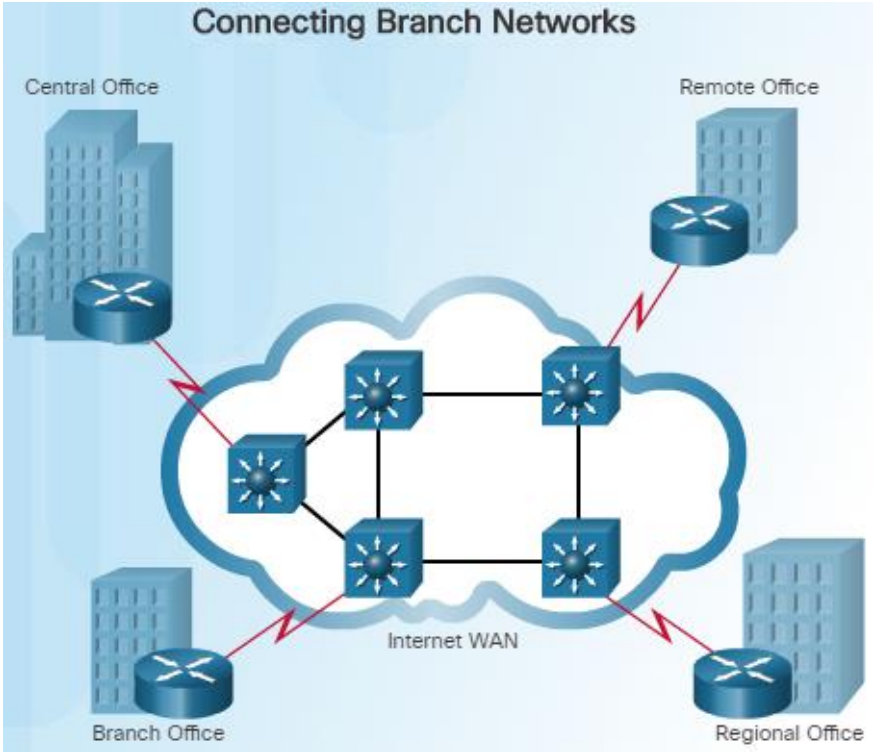
- AnimoTech:
  - Small R&D organization
  - Less than 100 employees
  - Small office uses a LAN with basic services to share information between computers, share printer, and access the Internet
- For other organizations:
  - Connects to the Internet using a consumer-grade subscription
  - Uses support services purchased from the ISP for IT support.

Campus Network

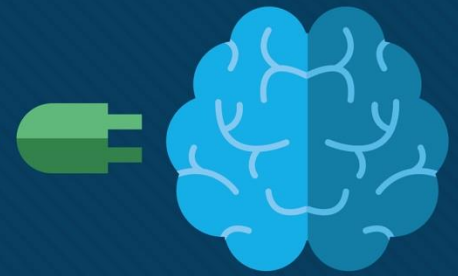


- The company grows to incorporate new services and employee groups to improve their services.
- The company is now classified as a small to medium-sized organization with employees who occupy multiple floors of an office building.
- There is now a need to tune the network for performance and fault-tolerance

What's Next? Branch Networks



- If a company continues to be successful, it can eventually open offices in new locations
- The company will need to provide connectivity with remote sites to enable access to the data center which houses various databases and servers.
- The branch offices that are in nearby cities can use private dedicated lines through their local service provider.
- Offices that are located in other countries must use the Internet for their connection.



Module 0
Routing Concepts Review

ITNET04

WAN Connectivity

Module Objectives

Module Title: Routing Concepts Review

Module Objectives:

- Describe the structure of a routing table.
- Explain how routers select the best route and forward packets to the destination
- Explain static and dynamic routing concepts.

0.1 IP Routing Table

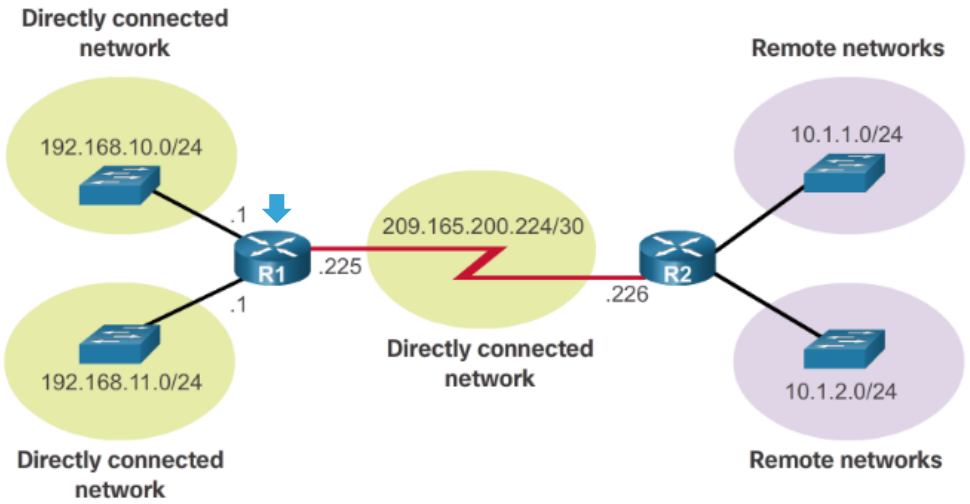
The Role of Routers

- **Recall:** A router is a network device that is used to move packets between logical

- The primary functions of a router:
  - Determine the best path to forward packets based on the information in its routing table
  - Forward packets toward their destination

The Routing Table

- Each router maintains a routing table – a data structure stored in RAM to track the list of known networks and how to reach them.
- The routing table contains:
  - **Directly Connected Networks:** Networks that a router is a member of through one of its interfaces
  - **Remote Networks:** Networks that it must use a neighboring router to reach



The Routing Table

- The **`show ip route`** **and** **`show ipv6 route`** commands are used to display the contents of the IPv4 and IPv6 routing tables, respectively:

```
RTR-Main>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
...

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.12/32 is directly connected, GigabitEthernet0/0
     192.168.2.0/25 is subnetted, 2 subnets
S       192.168.2.0/25 [1/0] via 192.168.1.2, GigabitEthernet0/1.10
S       192.168.2.128/25 [1/0] via 192.168.1.2, GigabitEthernet0/1.10
     192.168.3.0/26 is variably subnetted, 2 subnets, 2 masks
D       192.168.3.0/26 [90/30720] via 192.168.1.13, 00:00:01, GigabitEthernet0/0
D       192.168.3.64/27 [90/30720] via 192.168.1.13, 00:00:01, GigabitEthernet0/0
S*   0.0.0.0/0 [1/0] via 192.168.1.1, GigabitEthernet0/0
```

The Routing Table

- The **`show ip route`** and **`show ipv6 route`** commands are used to display the contents of the IPv4 and IPv6 routing tables, respectively:

```
R1# show ipv6 route
Codes: L - local, C - connected, S - static, R -
...
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#
```

Routing Table Entries

IPv4

```
D 201.165.224.0/24 [90/7680] via 192.168.1.1, 00:00:01, GigabitEthernet0/0
```

IPv6

```
O 2001:DB8:ACAD:4::/64 [110/50] via FE80::2:C, Serial0/1/1
```

Routing table entries contain the following essential information about each known network

- **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.
- **Metric** - This identifies the value assigned to reach the remote network.
- **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.

IP Routing Table

Next Hop and Exit Interfaces

IPv4

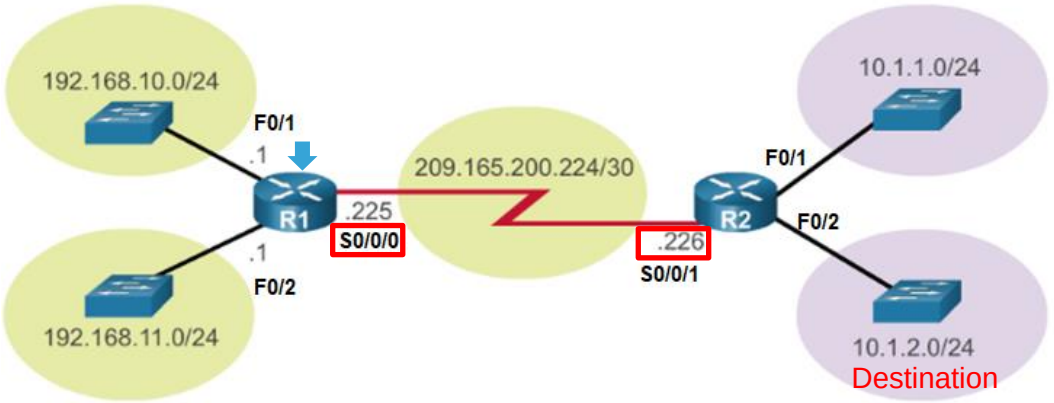
```
D 201.165.224.0/24 [90/7680] via 192.168.1.1, 00:00:01, GigabitEthernet0/0
```

IPv6

```
O 2001:DB8:ACAD:4::/64 [110/50] via FE80::2:C, Serial0/1/1
```

- The next hop and exit interfaces provide the router with the information needed to correctly forward a packet in the direction towards its final destination network
  - **Next-hop** identifies the **IP address of the next router** to which the packet would be forwarded to reach remote networks.
  - **Exit interface** identifies **this router's egress interface** to use to reach the destination network or the next router that can forward the packet

For **R1** to reach network 10.1.2.0/24:
Next Hop: **209.165.200.226**
Exit Interface: **S0/0/0**



Route Sources

IPv4
```
D 201.165.224.0/24 [90/7680] via 192.168.1.1, 00:00:01, GigabitEthernet0/0
```

IPv6
```
O 2001:DB8:ACAD:4::/64 [110/50] via FE80::2:C, Serial0/1/1
```

A routing table obtains its routes to known networks from the following:

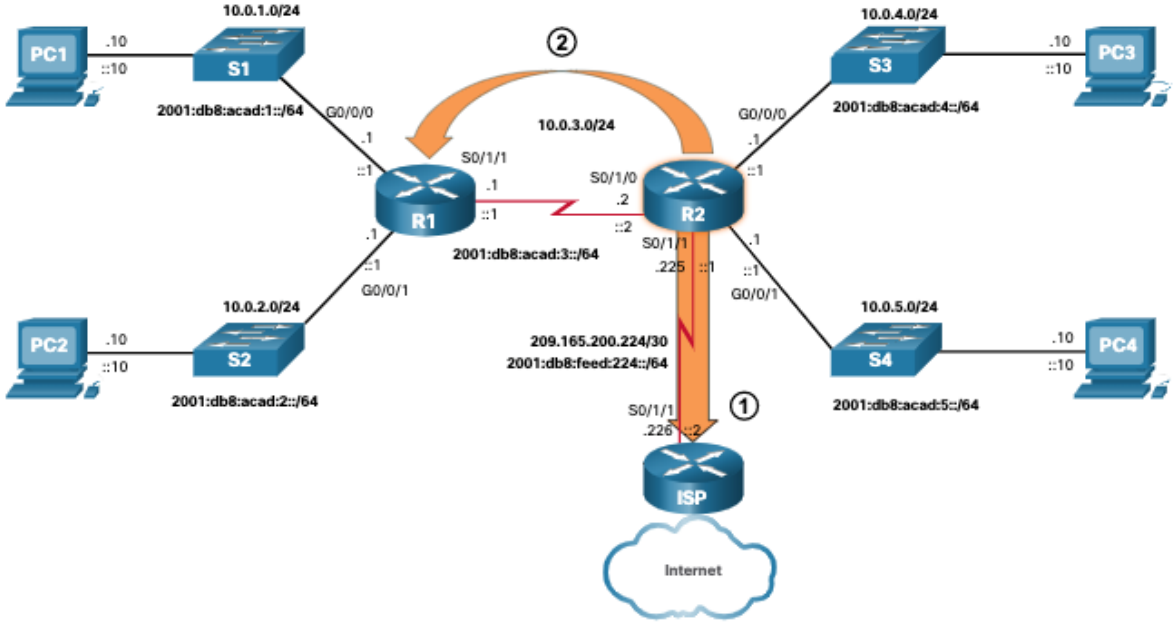
- From its own interfaces for directly connected networks
- From static routes and dynamic routing protocols for remote networks

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

- **L** - Identifies a local route which represents an address assigned to a router interface (automatically learned).
- **C** - Identifies a directly connected network (automatically learned).
- **S** - Identifies a route that is manually created to reach a specific remote network.
- **O/R/D, etc** - Identifies a dynamically learned network from another router
- ***** - This route is a candidate for a default route.

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.
- Can be either a static route or learned automatically from a dynamic routing protocol.

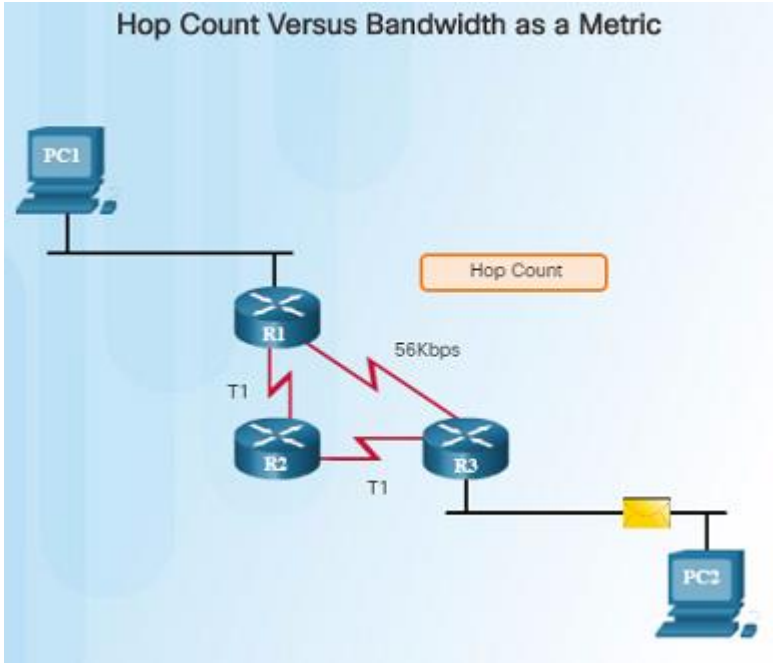


- Uses a status code with an asterisk symbol '*' and has an IPv4 route entry of 0.0.0.0/0 or an IPv6 route entry of ::/0.

```
RTR-Main>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
...
D       192.168.3.64/27 [90/30720] via 192.168.1.13, 00:00:01, GigabitEthernet0/0
S*    0.0.0.0/0 [1/0] via 192.168.1.1, GigabitEthernet0/0
```

Route Metric

- If a router has multiple paths to the same destination network, it must choose the best one to place in its routing table
- Dynamic routes are assigned a **metric**, a quantitative representation of its distance to the destination network automatically calculated by the router based on the rules of the routing protocol it uses
- The path with the lowest calculated metric is considered the best path




```
RTR-Main>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
...
192.168.3.0/26 is variably subnetted, 2 subnets, 2 masks
D       192.168.3.0/26 [90/30720] via 192.168.1.13, 00:00:01, GigabitEthernet0/0
```

Administrative Distance

- It is possible that the routing table learns about the same destination network address from more than one routing source.
- In such cases, the metric cannot be used to directly compare the routes and the **administrative distance (AD)** is used to determine route to install into the IP routing table.
  - Represents the "trustworthiness" of the route source.
  - Lower AD = more trustworthy route source.

```
RTR-Main>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
...
     192.168.2.0/25 is subnetted, 2 subnets
 192.168.2.0/25 is subnetted, 2 subnets
S       192.168.2.0/25 [1/0] via 192.168.1.2, GigabitEthernet0/1.10
S       192.168.2.128/25 [1/0] via 192.168.1.2, GigabitEthernet0/1.10
     192.168.3.0/26 is variably subnetted, 2 subnets, 2 masks
D       192.168.3.0/26 [90/30720] via 192.168.1.13, 00:00:01, GigabitEthernet0/0
```

Metric vs AD

- When choosing among several route options to a destination, a router prioritizes the lowest AD followed by the lowest metric
- Example: Assume routes A to F below can all be used to reach 192.168.1.0/24

Route	Source	Administrative Distance	Metric	Next Hop
A	OSPF	110	200	10.10.1.1
B	OSPF	110	125	10.10.1.2
C	EIGRP	90	206247	10.10.1.2
D	EIGRP	90	30013	10.10.1.1
E	RIP	120	3	10.10.1.1
F	RIP	120	2	10.10.1.2

This route is placed in the routing table

Lowest AD

Lowest metric among lowest AD routes

Routing Table Principles

There are three principles governing routing tables:

Principle 1: “Every router makes its decision alone, based on the information it has in its own routing table.”

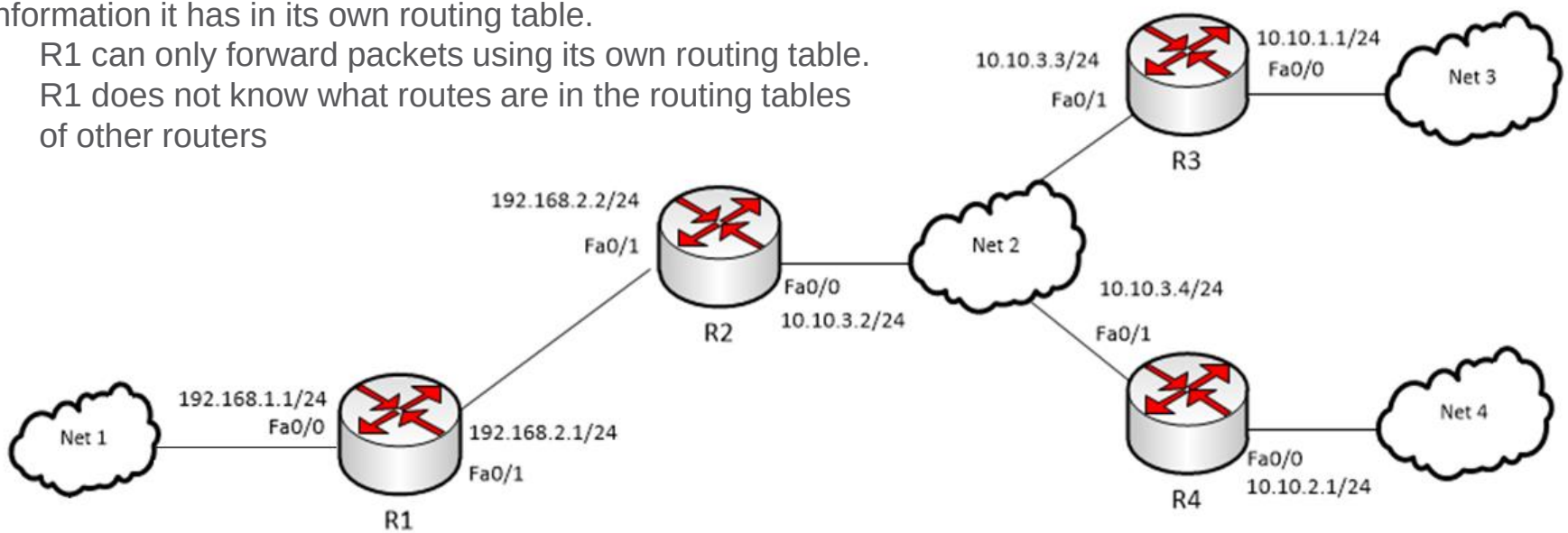
Principle 2: “The fact that one router has certain information in its routing table does not mean that other routers have the same information.”

Principle 3: “Routing information about a path from one network to another does not provide routing information about the reverse or return path.”

Routing Table Principle 1

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

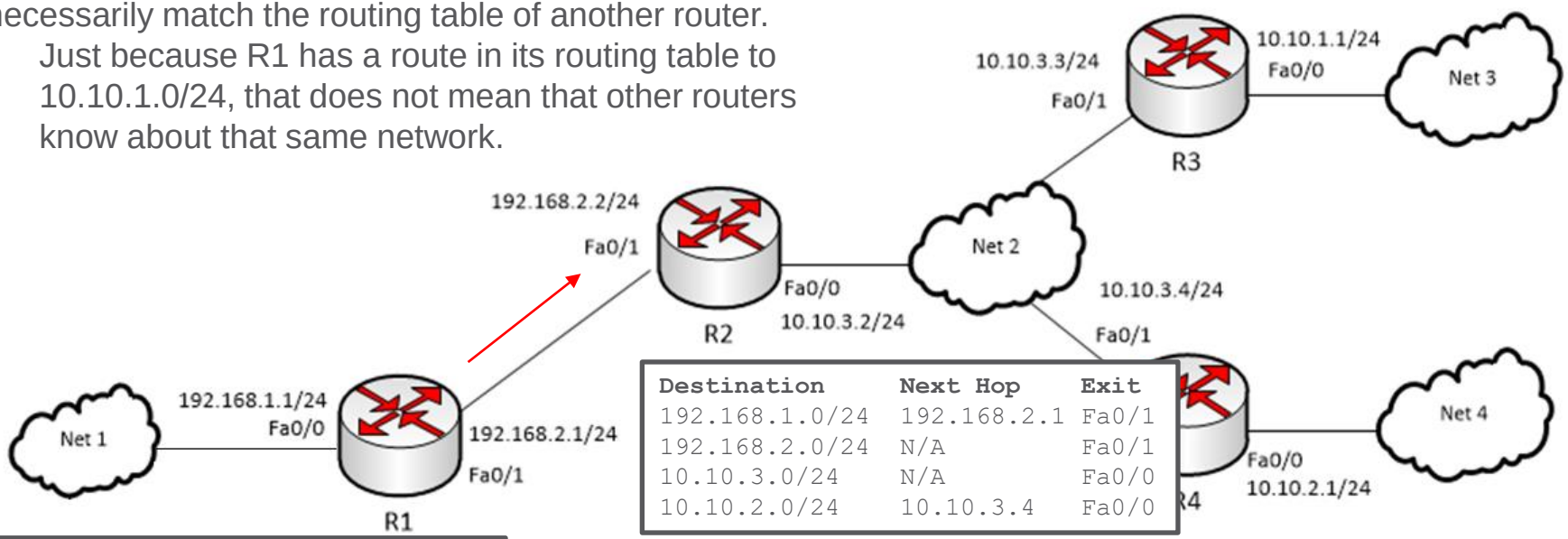


Destination	Next Hop	Exit
192.168.1.0/24	N/A	Fa0/0
192.168.2.0/24	N/A	Fa0/1
10.10.1.0/24	192.168.2.2	Fa0/1
10.10.2.0/24	192.168.2.2	Fa0/1
10.10.3.0/24	192.168.2.2	Fa0/1

Routing Table Principle 2

The information in a routing table of one router does not necessarily match the routing table of another router.

- Just because R1 has a route in its routing table to 10.10.1.0/24, that does not mean that other routers know about that same network.



Destination	Next Hop	Exit
192.168.1.0/24	192.168.2.1	Fa0/1
192.168.2.0/24	N/A	Fa0/1
10.10.3.0/24	N/A	Fa0/0
10.10.2.0/24	10.10.3.4	Fa0/0

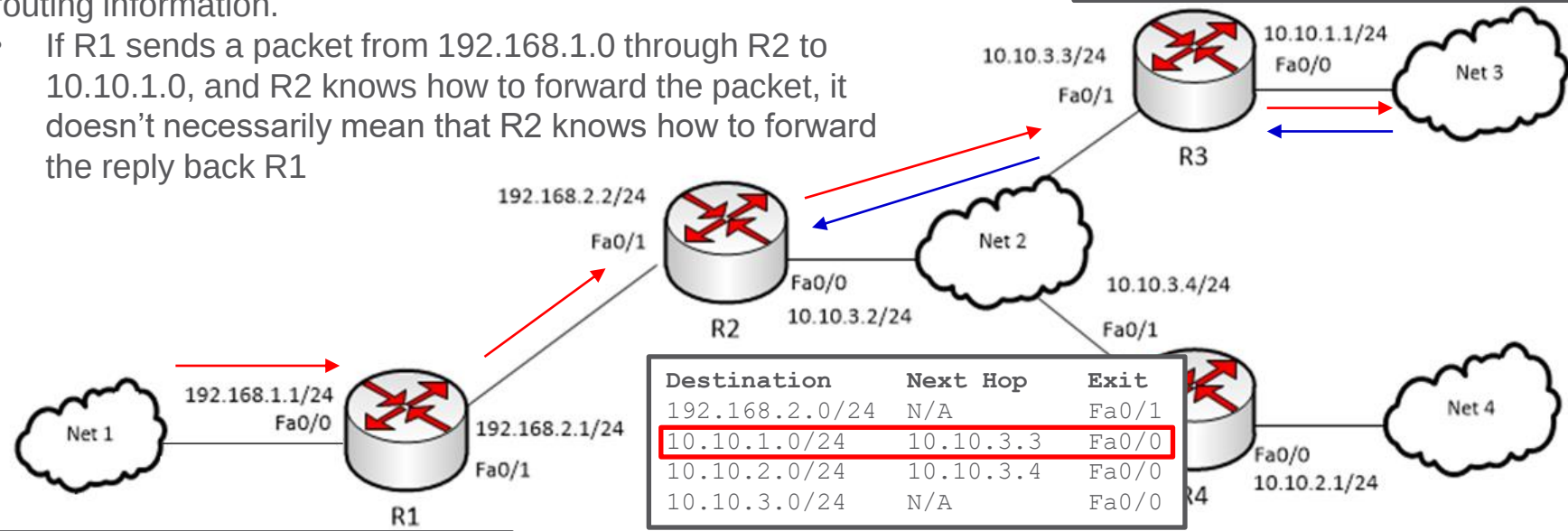
Destination	Next Hop	Exit
192.168.1.0/24	N/A	Fa0/0
192.168.2.0/24	N/A	Fa0/1
10.10.1.0/24	192.168.2.2	Fa0/1
10.10.2.0/24	192.168.2.2	Fa0/1
10.10.3.0/24	192.168.2.2	Fa0/1

No route to 10.10.1.0, still can't reach the destination network

Routing Table Principle 3

Routing information about a path does not provide return routing information.

- If R1 sends a packet from 192.168.1.0 through R2 to 10.10.1.0, and R2 knows how to forward the packet, it doesn't necessarily mean that R2 knows how to forward the reply back R1



Destination	Next Hop	Exit
192.168.1.0/24	10.10.3.2	Fa0/1
192.168.2.0/24	10.10.3.2	Fa0/1
10.10.1.0/24	N/A	Fa0/0
10.10.2.0/24	10.10.3.4	Fa0/1
10.10.3.0/24	N/A	Fa0/1

Destination	Next Hop	Exit
192.168.2.0/24	N/A	Fa0/1
10.10.1.0/24	10.10.3.3	Fa0/0
10.10.2.0/24	10.10.3.4	Fa0/0
10.10.3.0/24	N/A	Fa0/0

Destination	Next Hop	Exit
192.168.1.0/24	N/A	Fa0/0
192.168.2.0/24	N/A	Fa0/1
10.10.1.0/24	192.168.2.2	Fa0/1
10.10.2.0/24	192.168.2.2	Fa0/1
10.10.3.0/24	192.168.2.2	Fa0/1

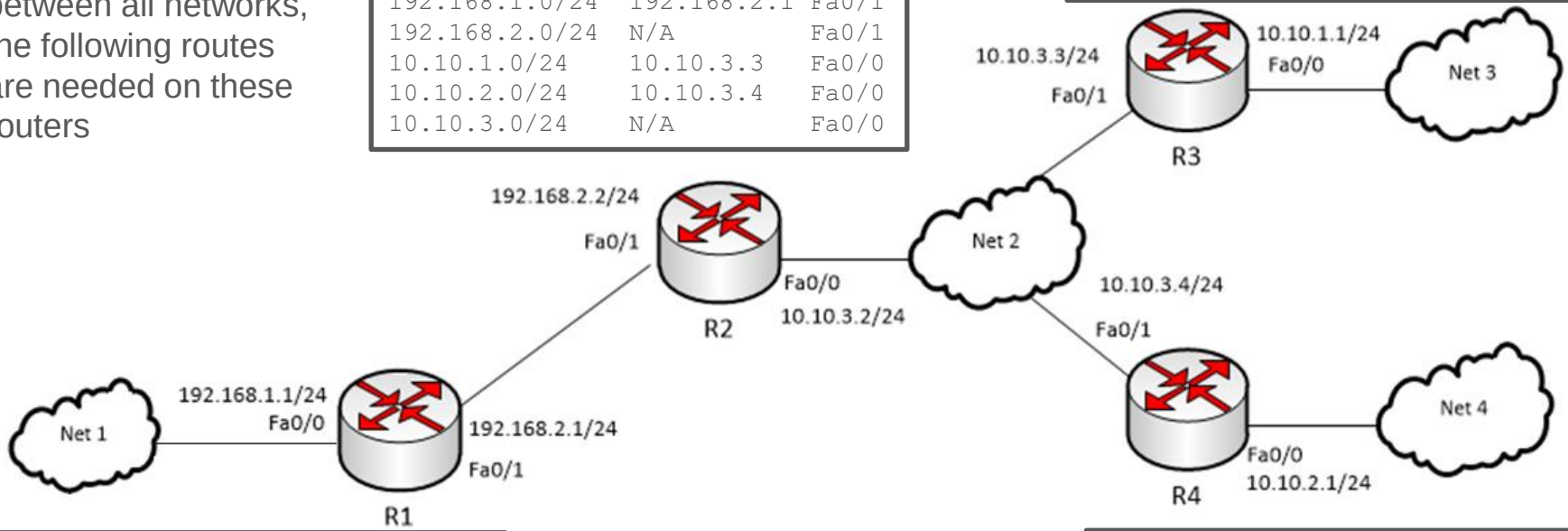
No route back to 192.168.1.0.
Reply fails

Routing Table Principles

For full connectivity between all networks, the following routes are needed on these routers

Destination	Next Hop	Exit
192.168.1.0/24	192.168.2.1	Fa0/1
192.168.2.0/24	N/A	Fa0/1
10.10.1.0/24	10.10.3.3	Fa0/0
10.10.2.0/24	10.10.3.4	Fa0/0
10.10.3.0/24	N/A	Fa0/0

Destination	Next Hop	Exit
192.168.1.0/24	10.10.3.2	Fa0/1
192.168.2.0/24	10.10.3.2	Fa0/1
10.10.1.0/24	N/A	Fa0/0
10.10.2.0/24	10.10.3.4	Fa0/1
10.10.3.0/24	N/A	Fa0/1



Destination	Next Hop	Exit
192.168.1.0/24	N/A	Fa0/0
192.168.2.0/24	N/A	Fa0/1
10.10.1.0/24	192.168.2.2	Fa0/1
10.10.2.0/24	192.168.2.2	Fa0/1
10.10.3.0/24	192.168.2.2	Fa0/1

Destination	Next Hop	Exit
192.168.1.0/24	10.10.3.2	Fa0/1
192.168.2.0/24	10.10.3.2	Fa0/1
10.10.1.0/24	10.10.3.3	Fa0/1
10.10.2.0/24	N/A	Fa0/0
10.10.3.0/24	N/A	Fa0/1

Matching Packets to Routes

- Recall: A route destination is represented by a prefix (network address), and prefix length (subnet mask)
- To determine if a route is suitable for forwarding, a packet destination must match the route prefix by a number of far-left bits that is equal to or more than the prefix length
- Example:

Must match at least 20 far-left bits to use this route

Route Prefix = 172.16.16.0/20	10101100.00010000.0001**0**000.00000000	
Packet A Dest = 172.16.25.93	10101100.00010000.0001**1**001.01011100	✓ Match
Packet B Dest = 172.16.18.3	10101100.00010000.000100**1**0.00000011	✓ Match
Packet C Dest = 172.16.42.250	10101100.00010000.00**1**01010.11111010	X No Match

Longest Match

When the routing table contains several routes that fulfill the prefix match requirement for a packet, the preferred route is the one with the longest matched prefix to the packet destination

Example:

Destination IPv4 Address		**Address in Binary**
172.16.25.93		**10101100.00010000.00011001.01011100**
Route Entry	Prefix/Prefix Length	Address in Binary
1	172.16.0.0**/16**	**10101100.00010000**.00000000.00000000
2	172.16.25.0**/24**	**10101100.00010000.00011001**.00000000
3	172.16.25.64**/26**	**10101100.00010000.00011001.01**000000

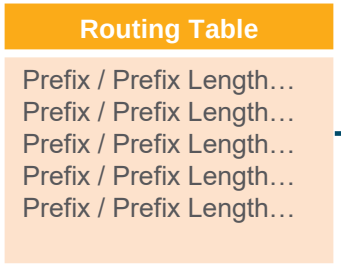
✓ Longest Match

Packet Forwarding Decision Process

1. A data frame with an encapsulated IP packet arrives through the ingress interface.

2. The router examines the destination IP address consults its routing table

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



4a. If no match is found, packet is discarded

4b. If a match is found, router encapsulates packet with appropriate header for egress interface

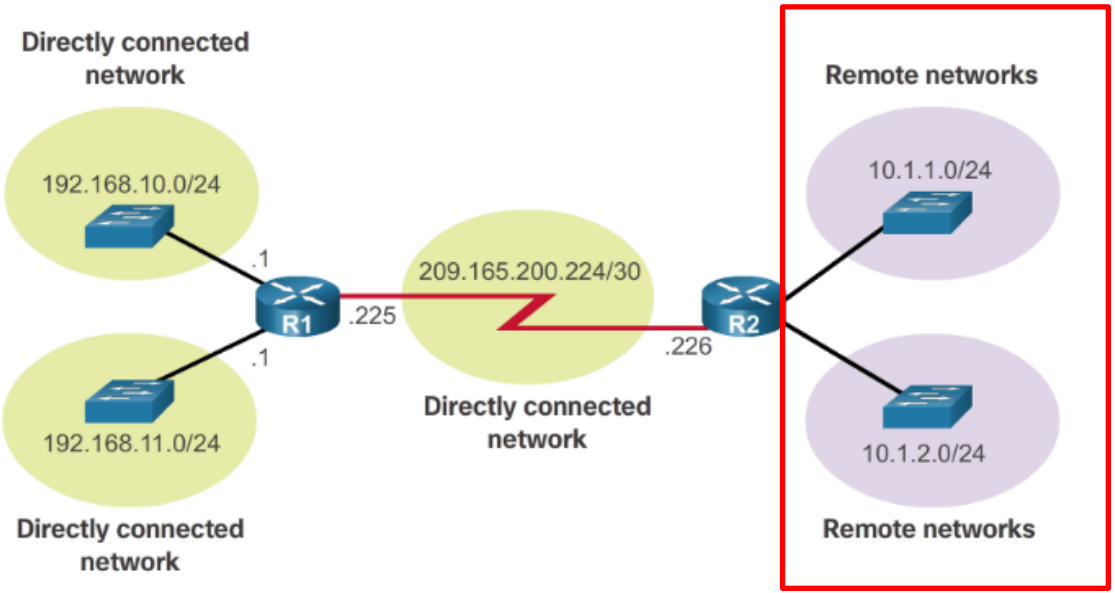
5a. Packet is for a directly connected network

5b. Packet is for a remote network

0.2 Static and Dynamic Routing

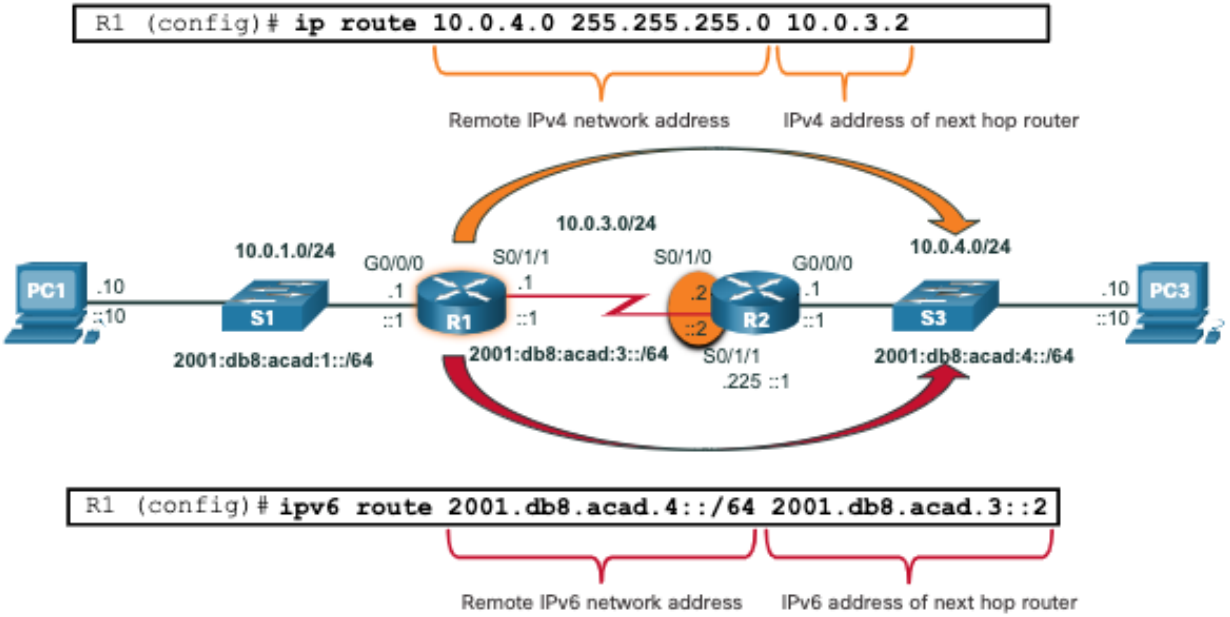
Reaching Remote Networks

- **Recall**: To reach remote networks, routers must use remote routes. These are either:
  - Statically configured routes or
  - Dynamic routes learned using a routing protocol



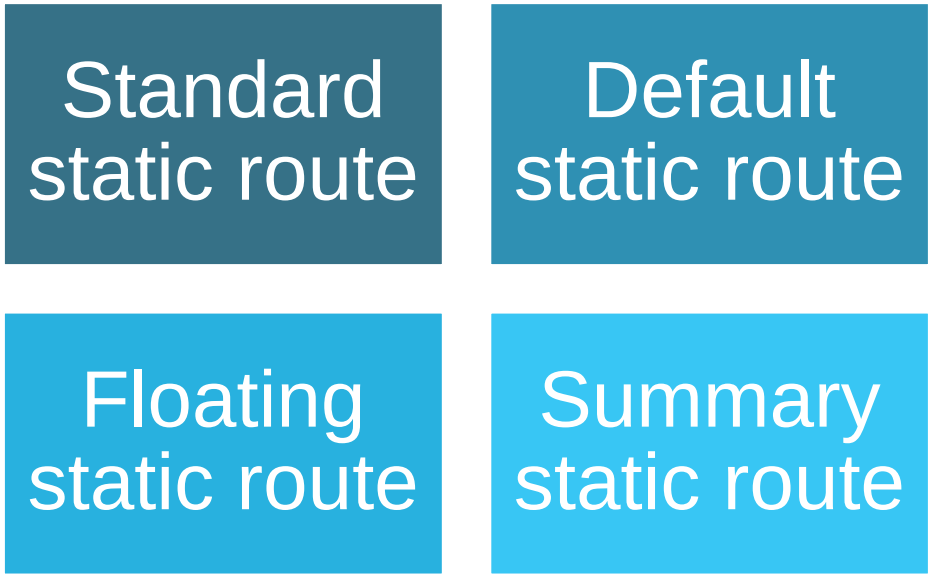
Static Routing

- Static routes are manually configured by a network administrator to define an explicit path between two networking devices.
- Are not automatically updated and must be manually reconfigured if the network topology changes.



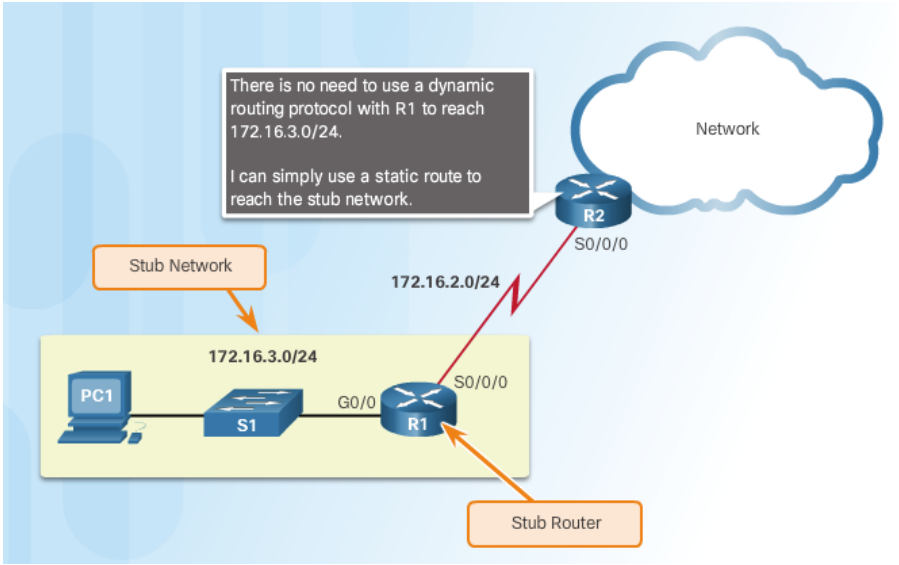
Types of Static Routes

- Static routes can be configured for IPv4 and IPv6. Both protocols support the following types of static routes:



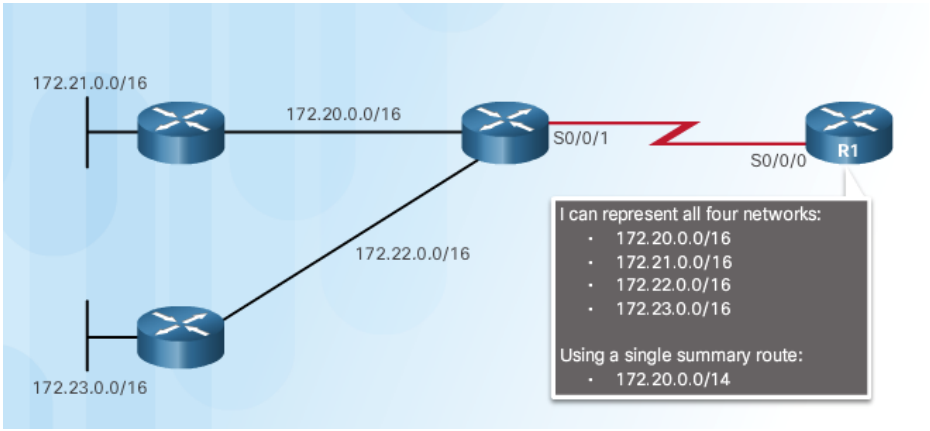
Standard Static Route

- A standard static route is one where the route prefix identifies a specific destination network
- Commonly used on routers serving as neighbors of a stub network



Summary Static Route

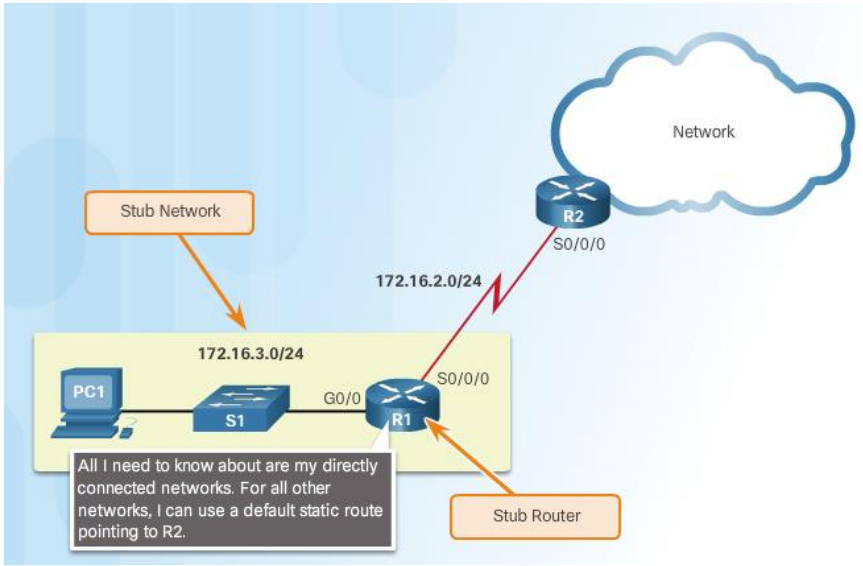
- A summary / aggregate route represents multiple routes as a single large network
- Often used in order to reduce the number of routes that need to be maintained in the routing table thereby consuming less RAM and making route lookup faster



Types of Static Routes

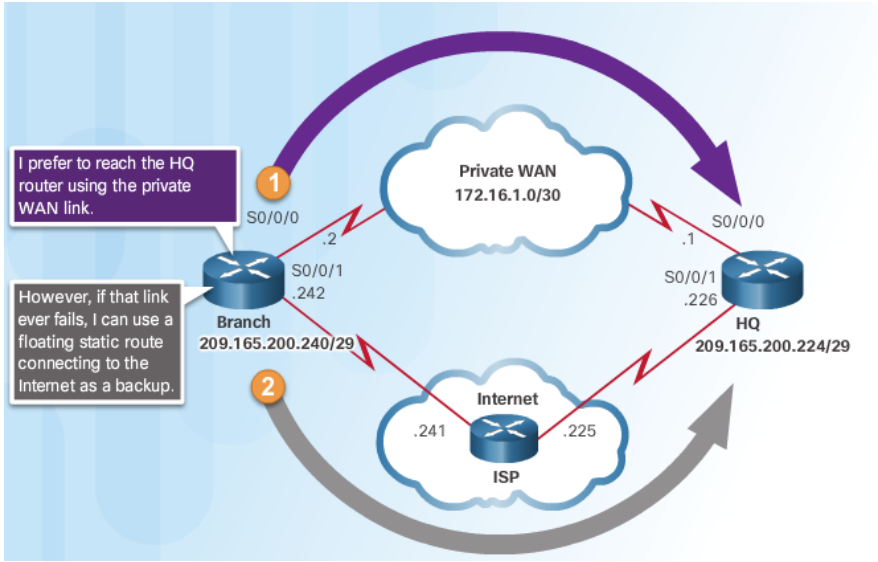
Default Static Route

- Default route is used to match and route all packets that do not match a more specific route in the routing table
- Commonly use on stub routers or edge routers connected to the ISP network



Floating Static Route

- Floating static routes are used to provide a backup path that a router will use when a primary route is not available
- Commonly configured by assigning a higher administrative distance than the main route



IP Route Command

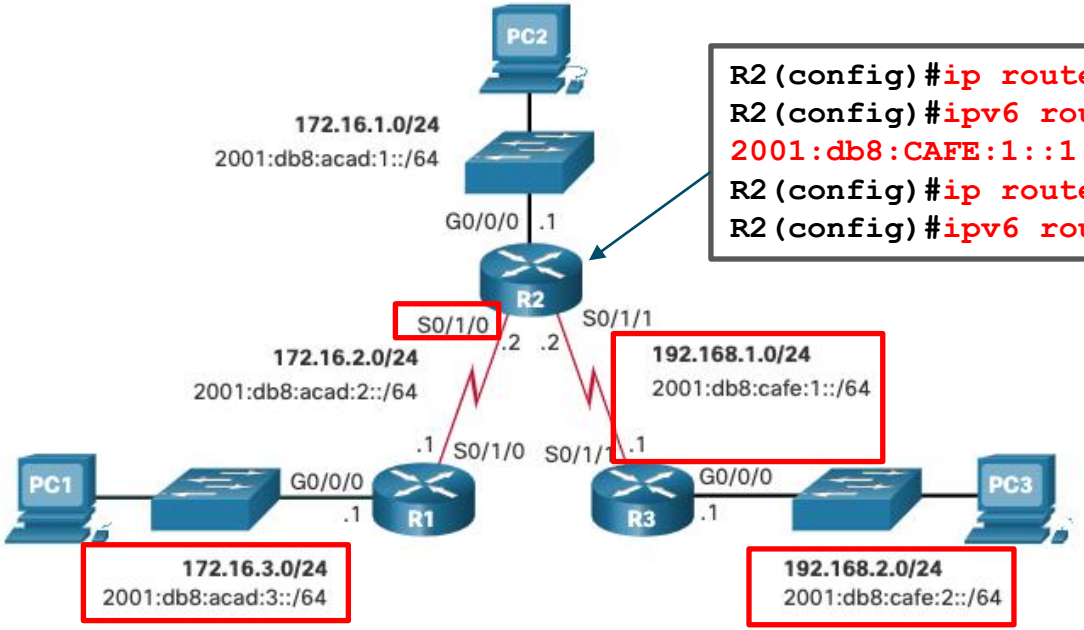
- Static routes are configured using the **ip route** and **ipv6 route** global configuration commands
  - For IPv4: **Router(config)# ip route** *network-address subnet-mask* {*next_hop* | *exit_int* [*next_hop*]} [*admin_dist*]
  - For IPv6: **Router(config)# ipv6 route** *ipv6-prefix/prefix-length* {*next_hop* | *exit_int* [*next_hop*]} [*admin_dist*]

Parameter	Description
network-address subnet mask ipv6-prefix/prefix length	Network address of destination e.g. 192.168.1.0 255.255.255.0 2001:db9:acad:1/64
next_hop	IP/IPv6 address of next hop router to reach the destination
exit_int	Egress interface of this router to reach the destination
admin_dist (optional)	Administrative distance assigned to route. AD = 1 if not explicitly specified

Static Route Configuration Sample

When configuring a static route, the destination can be configured using 3 format options:

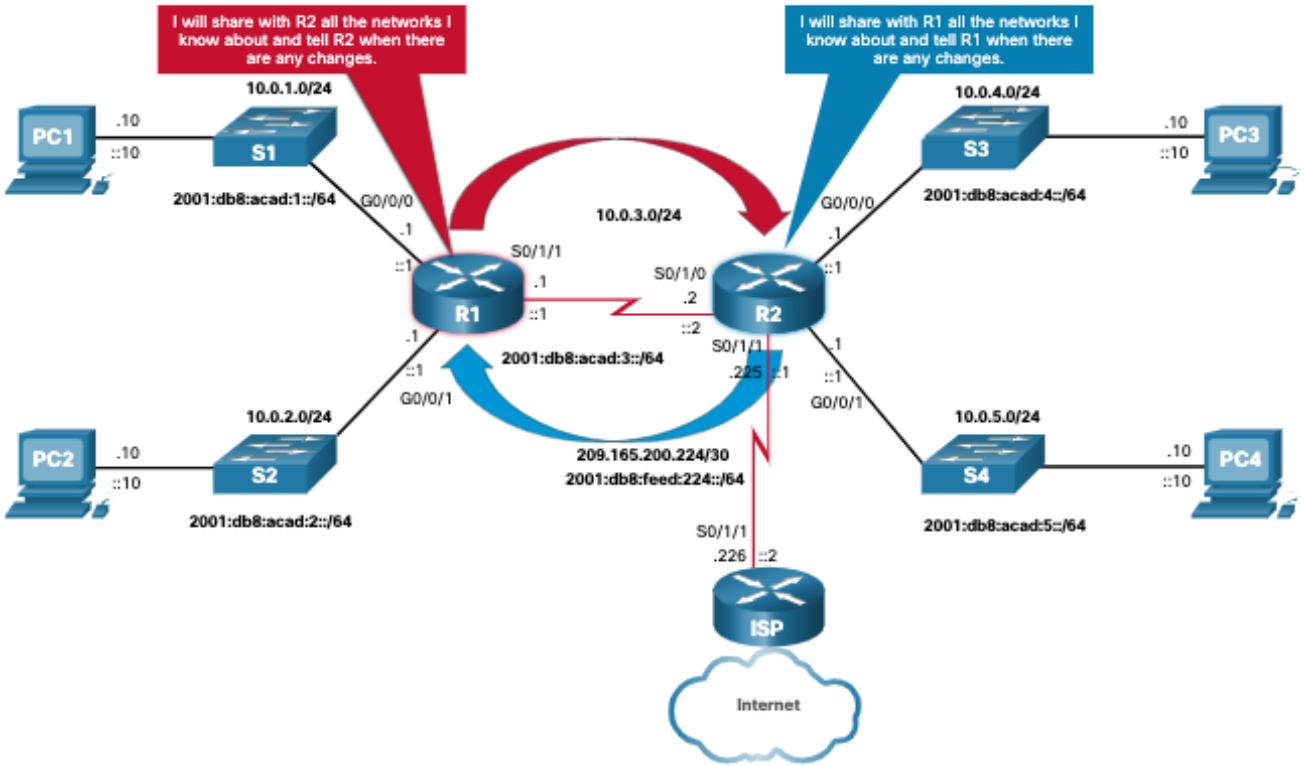
- with next hop (recursive format)
- with exit interface (directly connected format) – usable for serial interfaces only
- with next hop and exit interface (fully specified format)




```
R2(config)#ip route 192.168.2.0 255.255.255.0  192.168.1.1
R2(config)#ipv6 route 2001:db8:CAFE:2::/64
2001:db8:CAFE:1::1
R2(config)#ip route 172.16.3.0 255.255.255.0  S0/1/0
R2(config)#ipv6 route 2001:db8:ACAD:3::/64 S0/1/0
```

Dynamic Routing

Dynamic routing uses routing protocols so that routers automatically share information among themselves about the reachability and status of remote networks.



Dynamic Routing Protocol

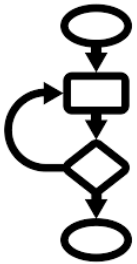
- A **routing protocol** is used exchange routing information and populate the routing table with the choice of best paths.
- The purpose of dynamic routing protocols includes the following:
  - Discovery of remote networks
  - Maintaining up-to-date routing information
  - Choosing the best path to destination networks
  - Ability to find a new best path if the current path is no longer available

Dynamic Routing Protocol Components

Main components of dynamic routing protocols include:

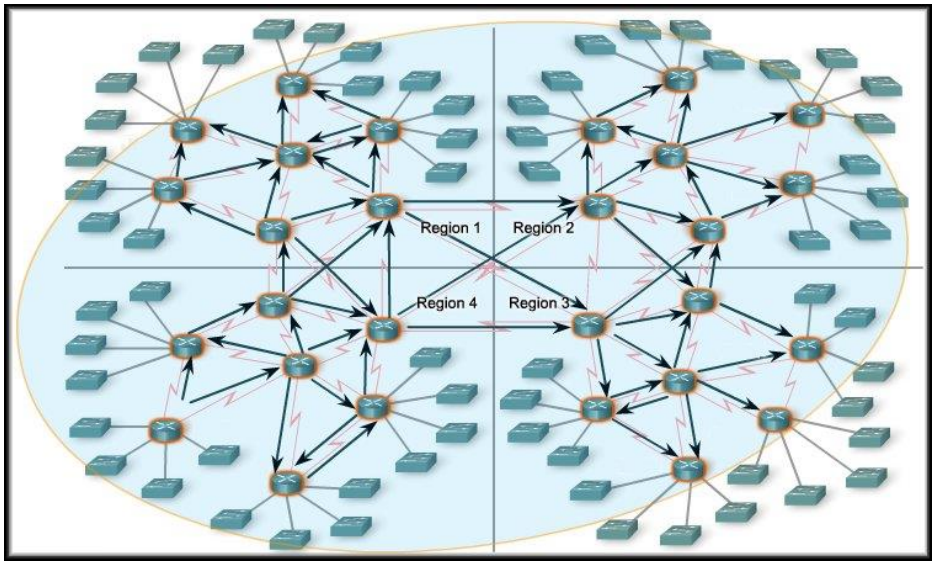
- **Data structures -** Routing protocols typically use tables or databases for its operations. This information is kept in RAM.
- **Routing protocol messages -** Routing protocols use various types of messages to discover neighboring routers, exchange routing information, and other tasks to learn and maintain accurate information about the network
- **Algorithm -** Routing protocols use algorithms for facilitating exchange of routing information and calculating the best path

Net 1	…	…
Net 2	…	…



Achieving Convergence

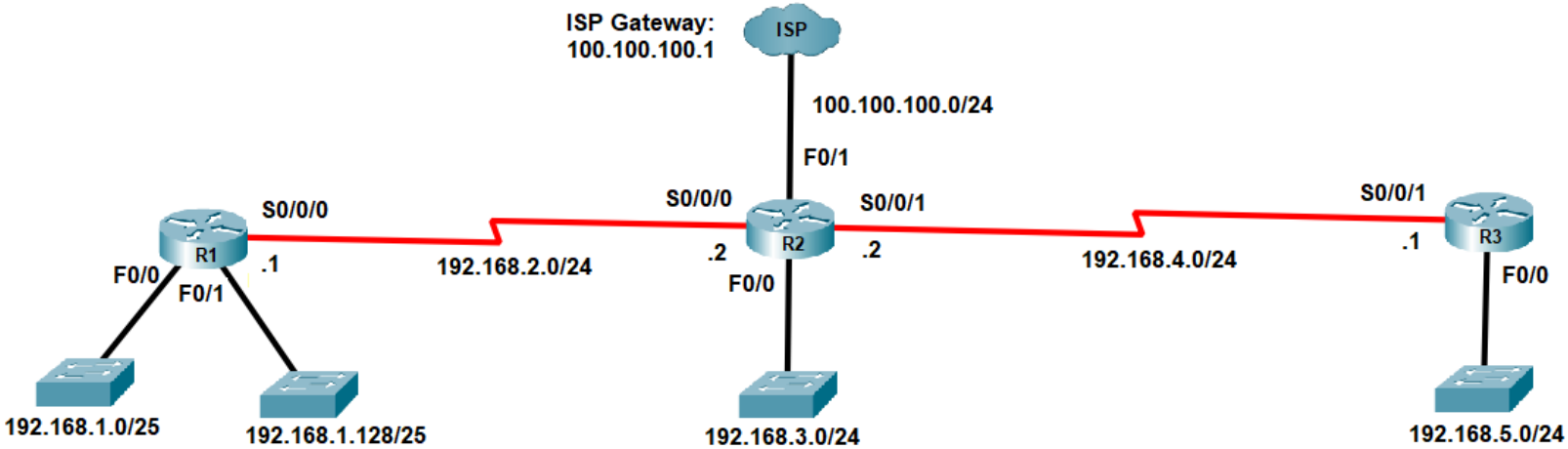
- The network has *converged* when all routers have complete and accurate information about the network.
- The speed of convergence is an important characteristic of a network because it affects how quickly routers adjust to topology changes.
  - Affected by the size of the network
  - A network is not completely operable until it has converged.
  - Routing protocols with shorter convergence times are preferred.



Typical Routing Protocol Configuration Procedure (RIP)

Task	IOS Command
1. Enter routing configuration mode	**Router(config)# router rip**
2. Identify directly connected networks to advertise and participate in routing updates	**Router(config-router)# network** *net_address*
3. Select passive interfaces (optional but recommended)	**Router(config-router)# passive-interface** *interface_id*
4. Advertise a static default route (case-to-case basis)	**Router(config-router)# default-information originate**

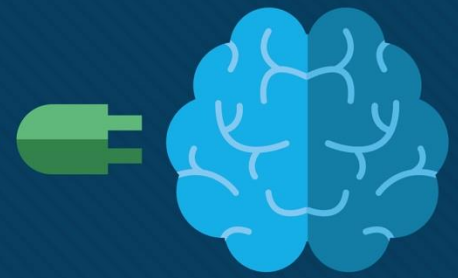
RIP Configuration Sample




```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 192.168.1.0
R1(config-router)#network 192.168.2.0
R1(config-router)#passive-interface f0/0
R1(config-router)#passive-interface f0/1
```

```
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 192.168.2.0
R2(config-router)#network 192.168.3.0
R2(config-router)#network 192.168.4.0
R2(config-router)#passive-interface f0/0
R2(config-router)#default-information
  originate
R2(config-router)#exit
R2(config)#ip route 0.0.0.0 0.0.0.0
  100.100.100.1
```

```
R3(config)#router rip
R3(config-router)#version 2
R3(config-router)#network 192.168.4.0
R3(config-router)#network 192.168.5.0
R3(config-router)#passive-interface f0/0
```



Module 2
Open Shortest Path First

ITNET04

WAN Connectivity

Module Objectives

Module Title: Open Shortest Path First

Module Objectives:

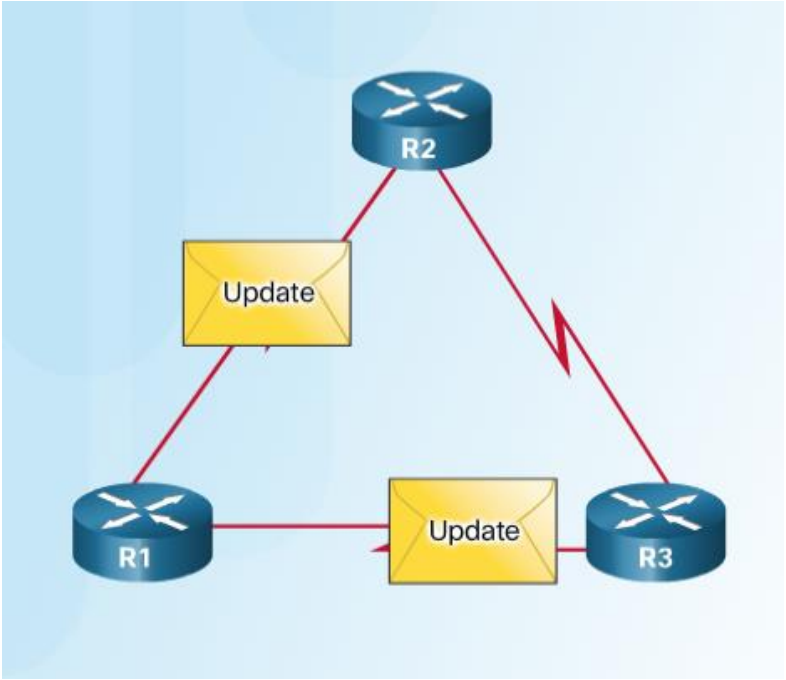
- Review basic concepts of dynamic routing protocols
- Be familiar with basic concepts and characteristics of the Open Shortest Path First (OSPF) routing protocol
- Narrate the operation of OSPF
- Configure single area OSPF for IPv4 networks
- Perform fine tuning on OSPF operations

References: CCNA ENSA Modules 1 and 2

2.1 Review of Routing Protocol Concepts

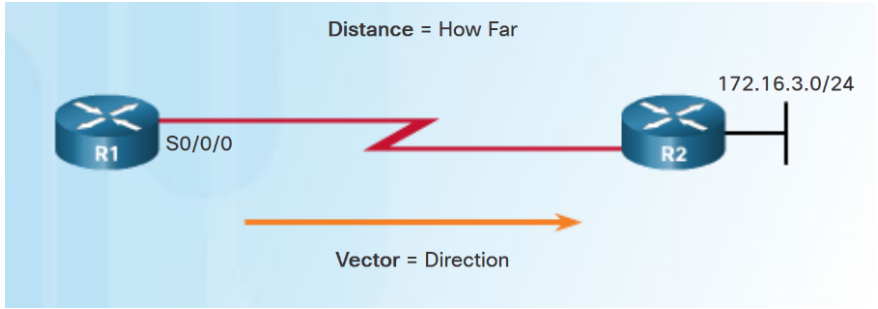
Dynamic Routing Protocols

- Dynamic routing protocols are used to facilitate the sharing of information about the reachability and status of remote networks between routers.
- The operations of dynamic routing protocols include:
  - Discovery of remote networks
  - Maintaining up-to-date routing information
  - Choosing the best path to destination networks
  - Ability to find a new best path if the current path is no longer available

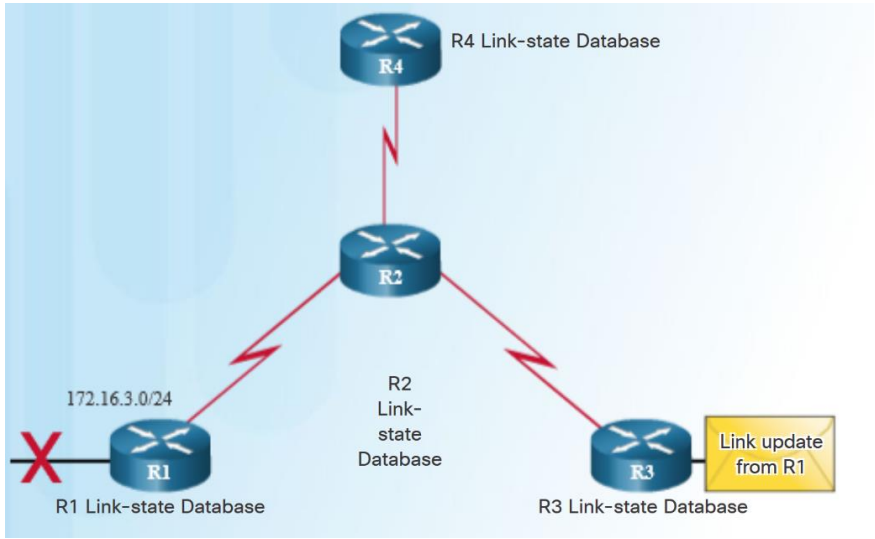


Distance Vector vs Link State Routing Protocols

- Distance vector protocols are aware of reachable networks only by their distance and direction and do not know the complete path that packets take to their destination:
- Examples: RIP and EIGRP



- Link state routing protocols learn about reachable networks by having a full view of the entire topology
- Examples: OSPF and IS-IS



Operating Fundamentals

Main components of dynamic routing protocols include:

- **Data structures -** Tables or databases in RAM used to keep track of information
- **Routing protocol messages -** Messages used for discovering neighboring routers, exchange routing information, and other tasks related to protocol operations
- **Algorithm –** Sequence of steps used exchange of routing information and calculating the best paths to known destinations

Routing protocols use a **metric** to represent the distance to reach a network.

- Each protocol has its own basis for metric calculation e.g. hop count, cost, etc)
- Lower metric = better route

2.2 Introduction to Open Shortest Path First (OSPF)

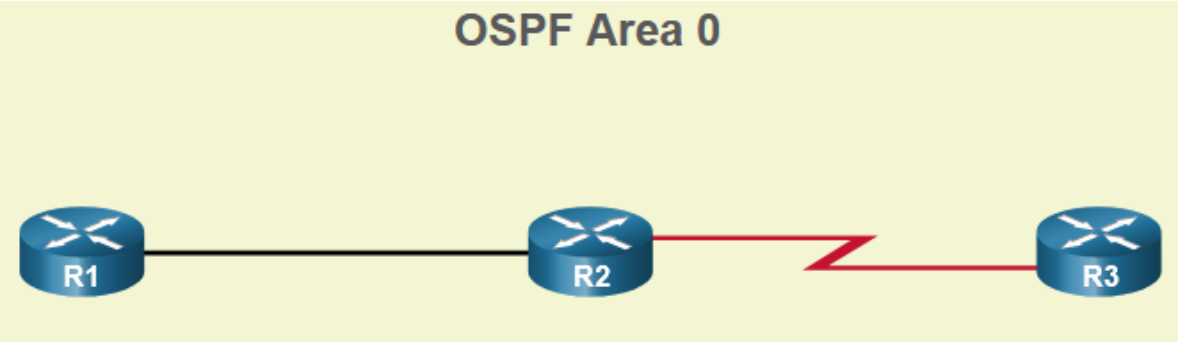
Introduction to OSPF

- **Open Shortest Path First (OSPF)** is a **link-state** routing protocol that was developed as an alternative for the distance vector Routing Information Protocol (RIP).
  - A **link** is an interface on a router, a network segment that connects two routers, or a stub network that is connected to a single router.
  - Information about a link is known as a **link-state**. All link-state information includes the network prefix, prefix length, and cost.
- Most widely used interior gateway protocol for enterprise networks
- Faster convergence and scales to much larger networks compared to RIP.
- Uses the concept of areas which allows a network administrator to divide the routing domain into distinct areas that help control routing update traffic.
- Versions:

OSPFv1	OSPFv2	OSPFv3
Experimental version – not supported on current routers	Current standard version used for IPv4 networks	Current standard version used for IPv6 networks

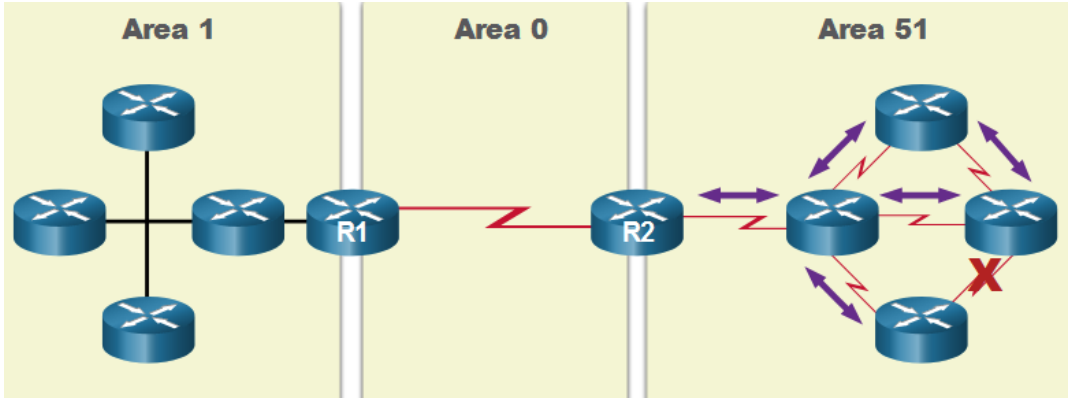
Single-Area OSPF

- For more efficiency and scalability, OSPF supports hierarchical routing using areas. An OSPF area is a group of routers that share the same link-state information in their link state databases.
- OSPF can be implemented in one of two ways:
  - **Single-Area OSPF** - All routers are in one area and share identical Link State Databases (topology map). For best practice, this single area is designated as ‘Area 0’



Multiarea OSPF

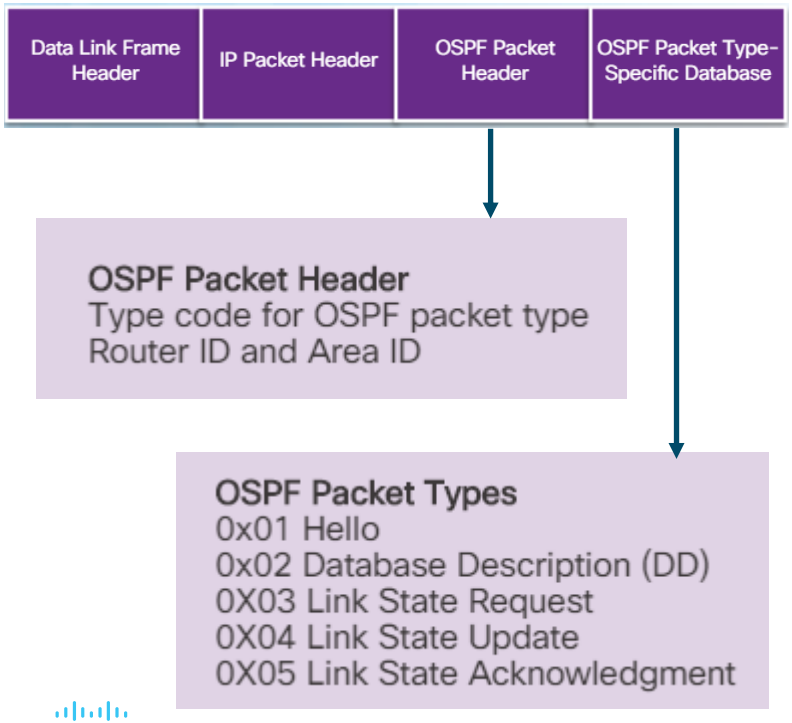
- **Multiarea OSPF** - OSPF is implemented in a hierarchical fashion for larger networks.
- Routers interconnecting the areas are referred to as Area Border Routers (ABRs) and can perform route summarization for their respective areas.



- The hierarchical-topology design can offer the following advantages:
  - **Smaller routing tables** - Fewer routing table entries if summarization is implemented
  - **Reduced link-state update overhead** - Minimized processing and memory requirements for updates.
  - **Reduced frequency of route calculations** -–Localized impact of a topology change within an area.

OSPF Messages

Routers running OSPF exchange messages to convey routing information using five types of packets:



Type	Packet Name	Description
1	Hello	Discovers neighbors and builds adjacencies between them
2	Database Description (DBD)	Checks for link state database synchronization between routers
3	Link-State Request (LSR)	Requests specific link-state records from router to router
4	Link-State Update (LSU)	Sends specifically requested link-state records
5	Link-State Acknowledgment (LSAck)	Acknowledges the other packet types

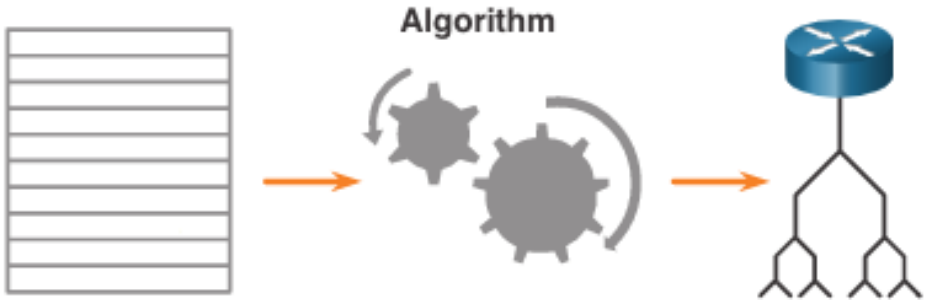
OSPF Data Structures

OSPF messages and its algorithm are used to create and maintain three OSPF databases:

Database	A.K.A.	Description
Adjacency Database	Neighbor Table	•List of all neighbor routers to which a router has established bi-directional communication. •This table is unique for each router.
Link-state Database (LSDB)	Topology Table	•Lists information about all other routers in the network. •The database represents the network LSDB. •All routers within an area have identical LSDB.
Forwarding Database	Routing Table	•List of routes generated when the algorithm is run on the link-state database. •Each router's routing table is unique and contains information on how and where to send packets to other routers.

Shortest Path First Algorithm

- The router builds the topology table using results of calculations based on the **Dijkstra shortest-path first (SPF) algorithm**. The SPF algorithm is based on the cumulative cost to reach a destination.
- The SPF algorithm creates an SPF tree by placing each router at the root of the tree and calculating the shortest path to each node. The SPF tree is then used to calculate the best routes.
- OSPF places the best routes into the forwarding database, which is used to make the routing table.



2.3 OSPF Operation

Link-State Routing Process

To maintain routing information, OSPF routers complete a generic link-state routing process to reach a state of convergence. The following are the link-state routing steps that are completed by a router and their corresponding OSPF operational states:

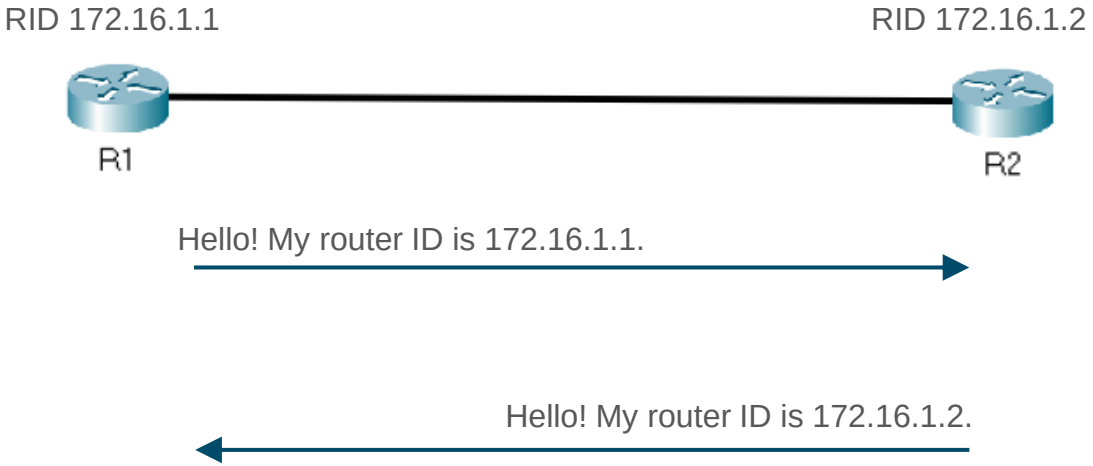
Step	OSPF State
Establish Neighbor Adjacencies	Down
	Init
	Two-Way
	Ex-Start
Exchange Link-State Advertisements	Exchange
Build the Link State Database	
Execute the SPF Algorithm	Loading
Choose the Best Route	
	Full

Establish Neighbor Adjacencies

- Routers running OSPF are assigned a **Router ID**, a 32-bit number that identifies them within the routing domain.
- To begin operations, a router must first discover neighbor routers (router connected to the same network link) using Hello messages.

1. **Down State**
   Router begins sending Hello packets but has not received any Hello packets yet

2. **Init State**
   Router has received a Hello from a neighbor and knows the neighbor router ID



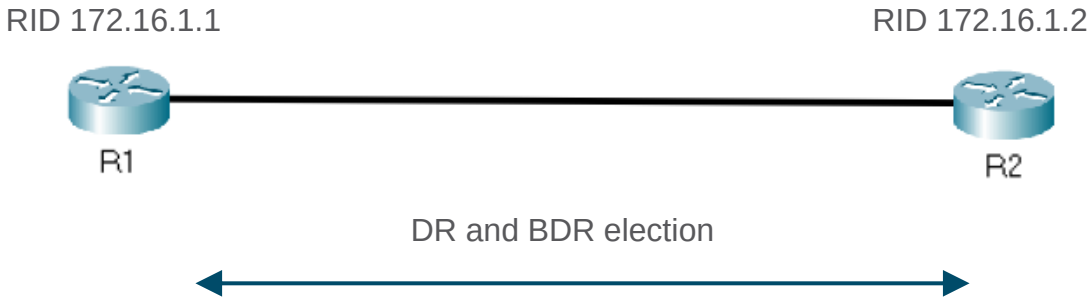
Establish Neighbor Adjacencies

- Once two neighboring routers know each other's router IDs, they will have established bidirectional communications.
- If a link uses multiaccess network type such as Ethernet, the connected routers must elect a Designated router (DR) and Backup Designated Router (BDR).

3

Two-Way
Routers achieve bidirectional communication.

On multiaccess links (e.g. Ethernet), the routers elect a DR and a BDR.



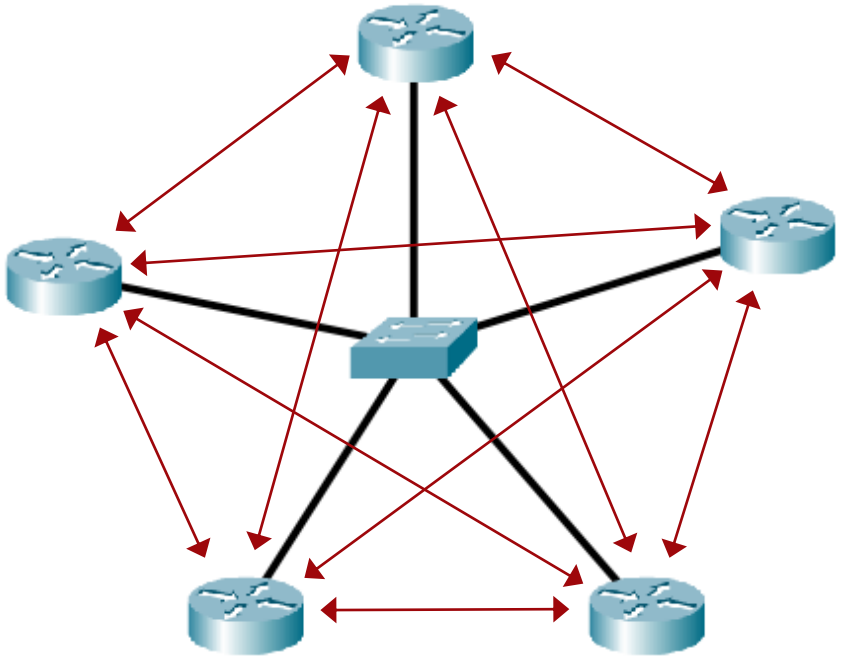
OSPF DR and BDR

- Why have a DR/BDR election?
- In a multiaccess network, adjacencies exponentially increase as the number of routers increase

$$\text{Adjacencies} = \frac{n(n-1)}{2}$$

where n = number of routers on link

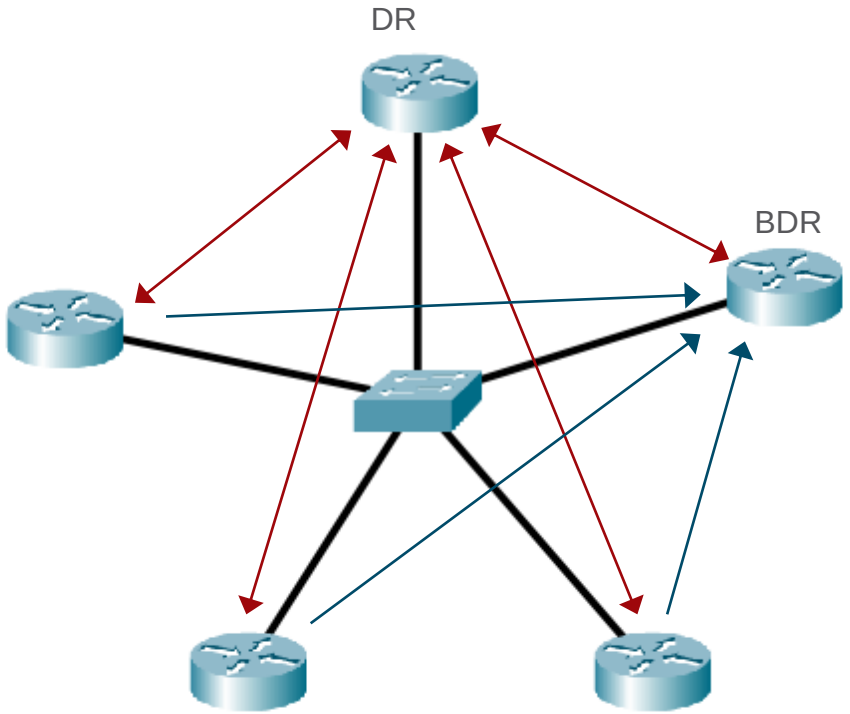
- Routers exchange updates with all neighbors that they have established adjacency with, thus potentially leading to extensive flooding of updates if too many adjacencies are created



Routers	Potential Adjacencies
5	10
10	45
20	190
100	4950

OSPF DR and BDR

- Why have a DR/BDR election?
- Solution: Elect a DR and a BDR per multiaccess link, and establish adjacencies only with these 2 routers
- Reduce the number of LSUs sent:
  - Routers send updates only to the DR and BDR
  - DR will be responsible for distributing updates to the rest of the routers on the link
  - BDR takes over in case DR fails

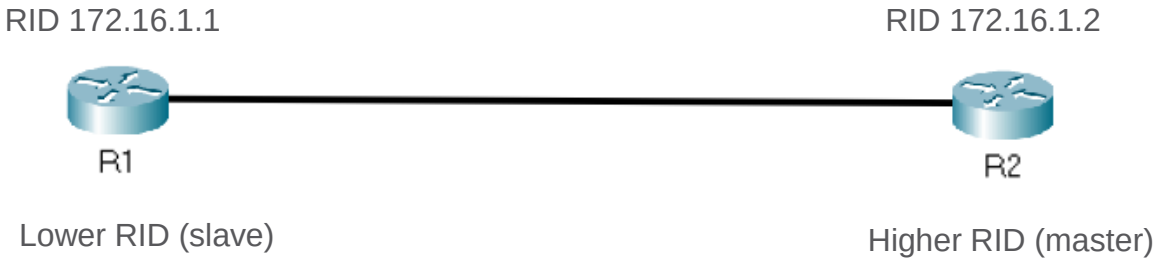


Establish Neighbor Adjacencies

- Routers who will establish an adjacency with each other will take master and slave roles
  - Master – router with higher router ID, will initiate the link information exchange
  - Slave – router with lower router ID
- Routers will complete establishment of their adjacencies at the end of this stage

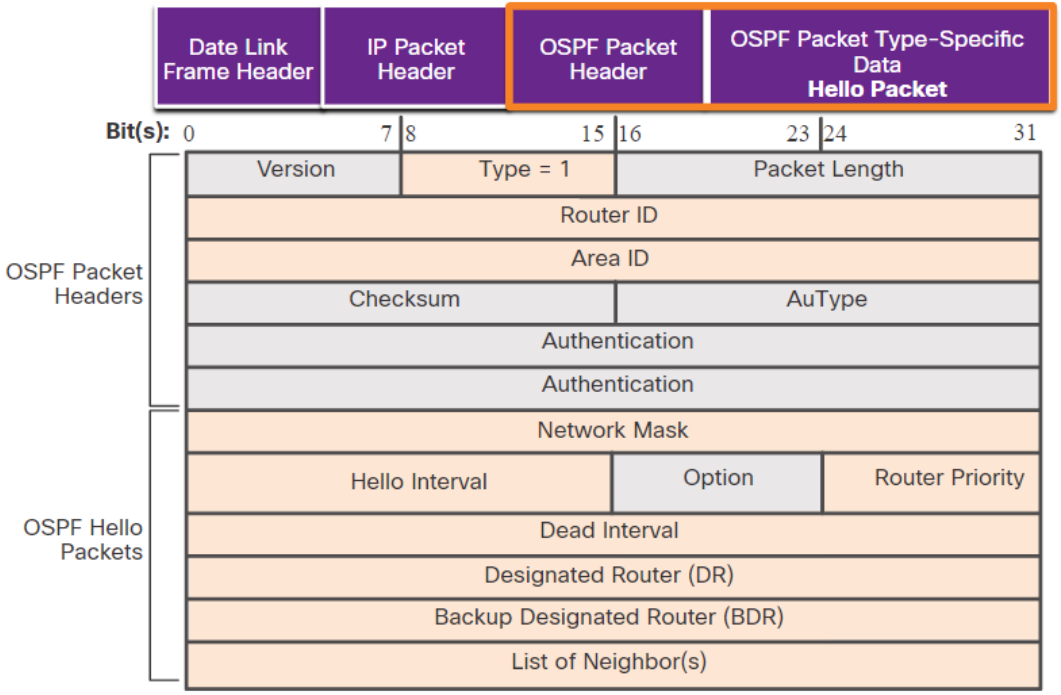
4

ExStart
Routers establish a master-slave relationship and choose the initial sequence number for adjacency formation



Hello Packet

- Hello packets have a crucial purpose in the establishing neighbor adjacencies:
  - Discover OSPF neighbors
  - Advertise parameters on which two routers must agree to become neighbors.
  - Elect the DR and BDR on multiaccess networks
- Transmitted periodically as a multicast on each link
  - 224.0.0.5 (IPv4)
  - FF02::5 (IPv6)

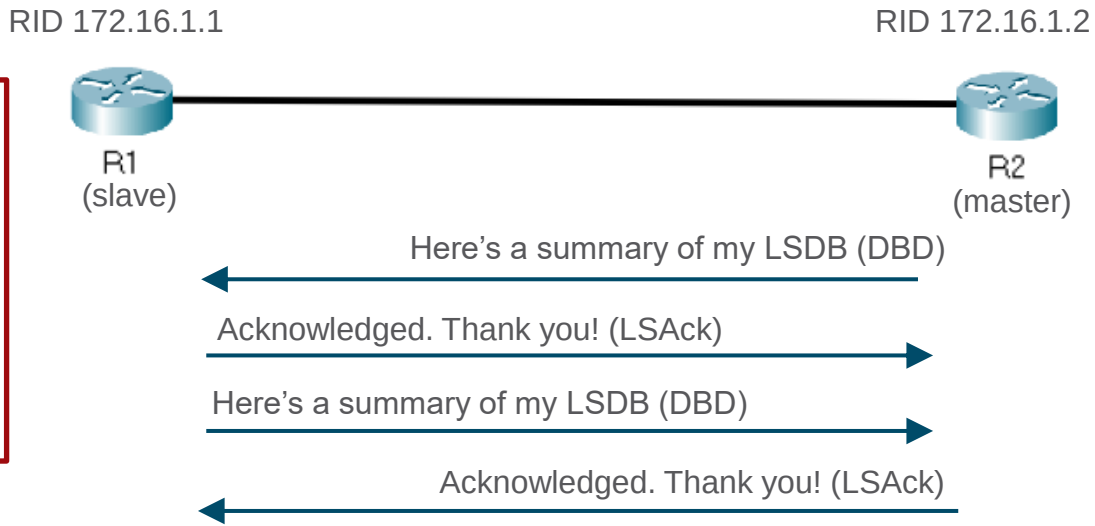


Synchronizing OSPF Databases

- After the Two-Way state, routers begin to synchronize their link state databases by transitioning to the Exchange state and using the other four types of OSPF packets to exchange information.

5

Exchange
Neighbors with adjacencies exchange the summaries of their LSDBs using Database Description (DBD) packets and acknowledge these using LS Acknowledge (LSAck) packets



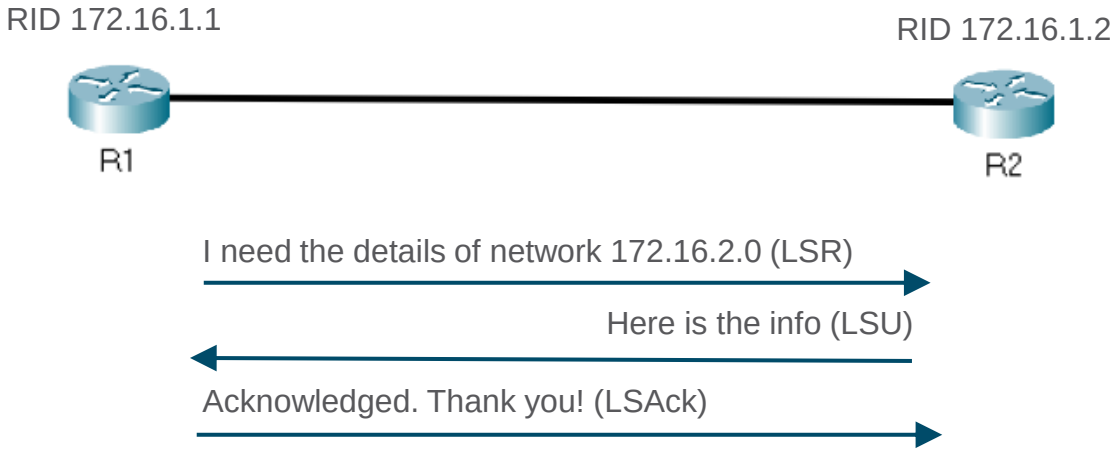
Synchronizing OSPF Databases

- When receiving a DBD, a router compares the content with its LSDB. If the DBD has updated link information, the router requests for details of the missing or updated link
- After all LSR/LSUs have been exchanged and satisfied, the routers are considered synchronized

6 **Loading**
Link State Request (LSR) and Link State Updates (LSU) are used to gain additional route information.

Routes are processed using the SPF algorithm.

7 **Full**
Databases are fully synchronized

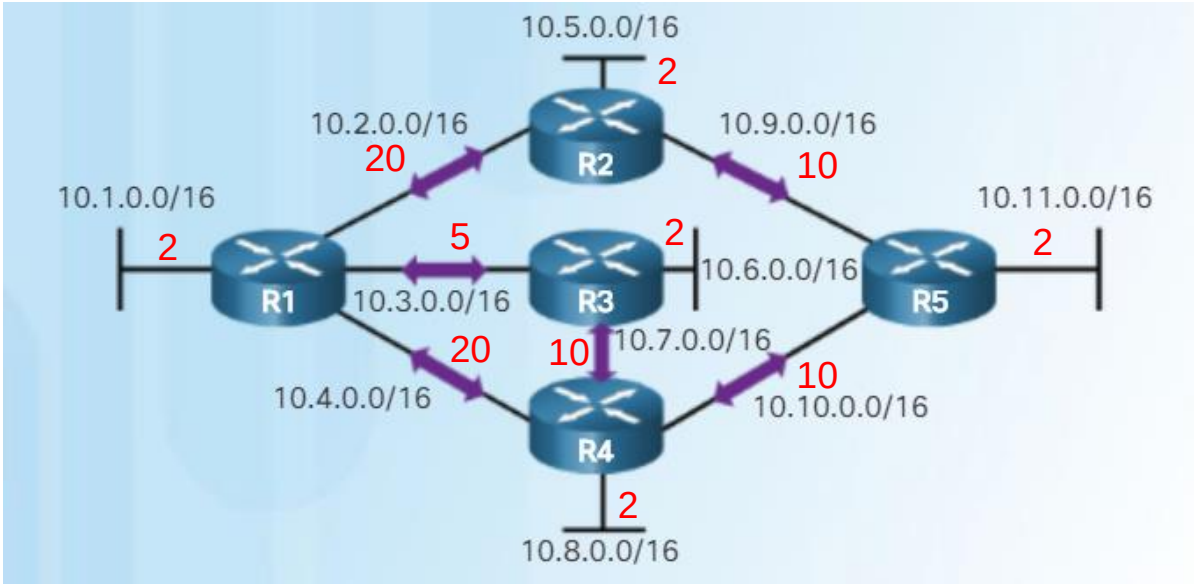


Link-State Updates

- Link State Updates (LSUs) are used to send Link State Advertisements (LSAs) which contain detailed information about each link connected to the router
- Each LSA contains:
  - ID of the source router
  - Router ID of a neighbor on the link (if present)
  - Address and mask of link network or address of router interface connected to the link
  - Metric of the link
- LSUs are sent
  - Every 30 minutes
  - Whenever a topology change occurs

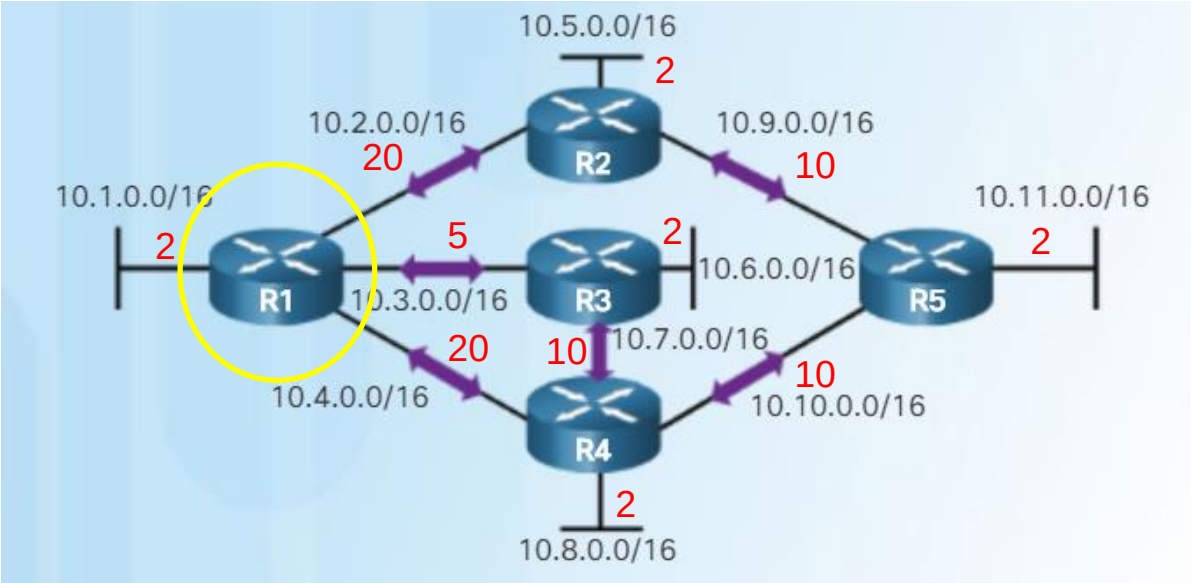
Path Calculation

- Each router uses the LSAs it received to build a graph representing the network topology (routers = nodes, links = edges)
- A cost value (usually based on link bandwidth) is associated with each link according to information contained in the LSA



Path Calculation

- To calculate the best path to a destination network, a router uses the Dijkstra algorithm to find the path with the least total cost of links to the destination



Destination	Shortest Path	Cost
10.5.0.0/16	R1→R2	22
10.6.0.0/16	R1→R3	7
10.7.0.0/16	R1→R3	15
10.8.0.0/16	R1→R3→R4	17
10.9.0.0/16	R1→R2	30
10.10.0.0/16	R1→R3→R4	25
10.11.0.0/16	R1→R3→R4→R5	27
10.5.0.0/16	R1→R2	22

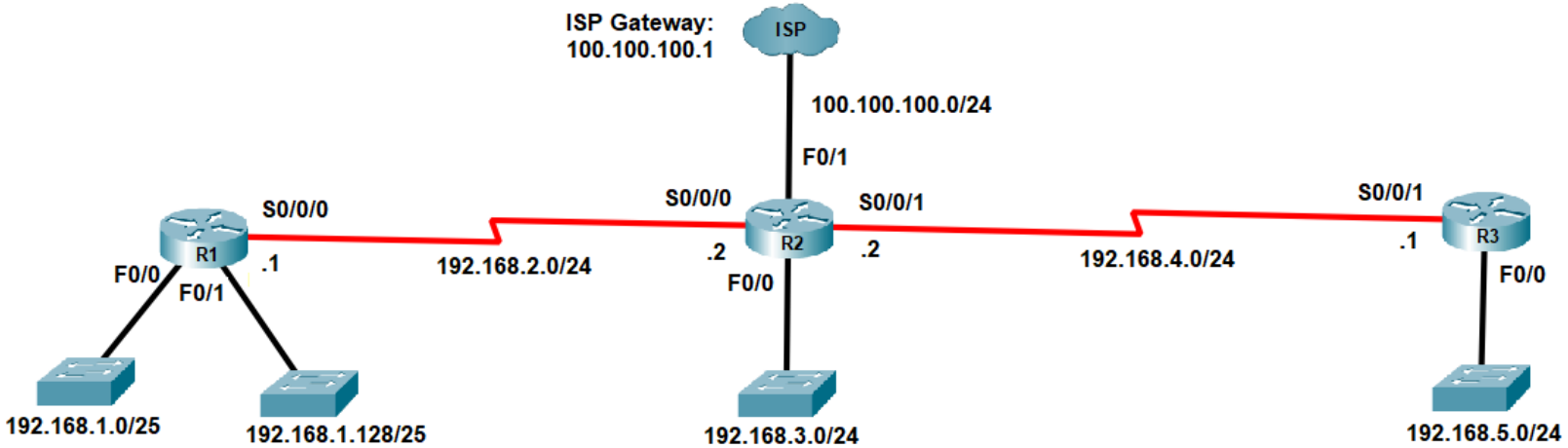
2.4 Single Area OSPF Configuration

OSPF Basic Configuration Procedure

Task	IOS Command
1. Enter OSPF configuration mode	**Router(config)# router ospf** *proc_id*
2. Set router ID (optional but recommended)	**Router(config-router)# router-id** *address*
3. Identify directly connected networks to advertise and participate in routing updates	**Router(config-router)# network** *net_address wildcard* ***area*** *area_num*
4. Select passive interfaces (optional but recommended)	**Router(config-router)# passive-interface** *interface_id*
5. Advertise a static default route (case-to-case basis)	**Router(config-router)# default-information originate**

OSPF Configuration Mode

- OSPFv2 is enabled using the **router ospf** *process-id* global configuration mode command.
- The *process-id* is an administrator-assigned number between 1 and 65,535 It is locally significant only, but it is good practice to use the same value on all OSPF routers.



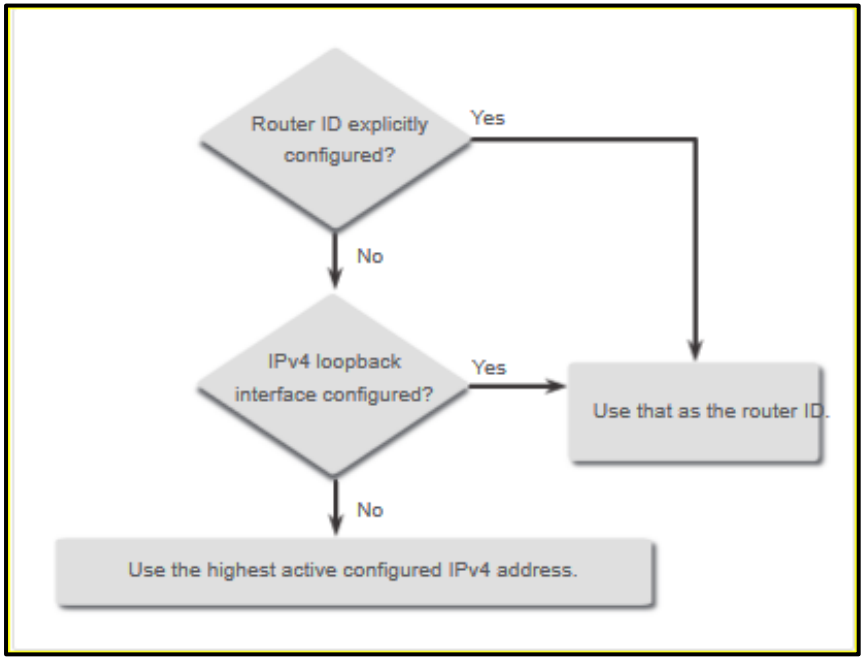

```
R1(config)#router ospf 10
```

```
R2(config)#router ospf 10
```

```
R3(config)#router ospf 10
```

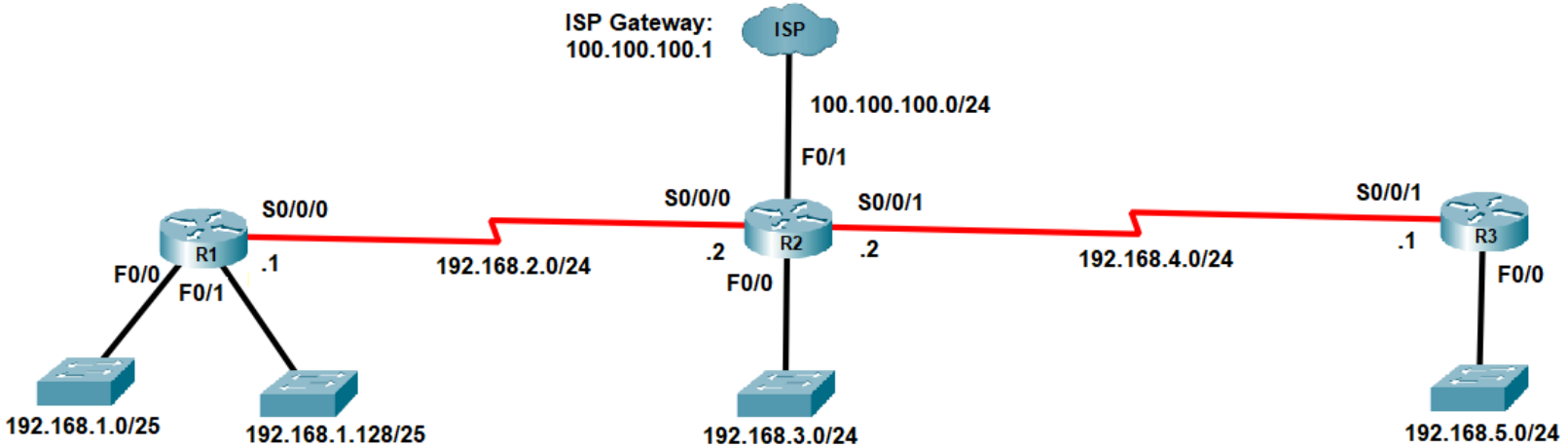
OSPF Router ID

- The router ID is a 32-bit value, represented as an IPv4 address, used to uniquely identify an OSPF router
- Recall: The router ID is used for the following:
  - Determine order of DBD sending during the Exchange state
  - Election of the DR and BDR on multiaccess network links
- Cisco routers obtain the router ID in the following preferential order:
  1. The router ID is explicitly configured (Recommended)
  2. Highest IPv4 address of any of its configured loopback interfaces.
  3. Highest active IPv4 address of any of its physical interfaces.



OSPF Router ID

- The router ID is explicitly configured using the OSPF **router-id** command and must be unique per router in the routing domain.
- The ID is formatted as an IPv4 address but need not be an actual address in the network




```
R1(config)#router ospf 10
R1(config-router)#router-id
  1.1.1.1
```

```
R2(config)#router ospf 10
R2(config-router)#router-id
  2.2.2.2
```

```
R3(config)#router ospf 10
R3(config-router)#router-id
  3.3.3.3
```

Configure a Loopback Interface as the Router ID

- Alternatively, a loopback interface can be configured as an automatic source of the OSPF router ID. Typically, the IPv4 address for this type of loopback interface should be configured using a 32-bit subnet mask (255.255.255.255).

```
R1(config)#interface Loopback 1
R1(config-if)#ip address 1.1.1.1 255.255.255.255
R1(config-if)#end
```

- Note: After a router selects a router ID, changing the router ID does not take effect until the router is reloaded or the OSPF process is reset. Clearing the OSPF process is done using the ***clear ip ospf process*** Privileged EXEC command

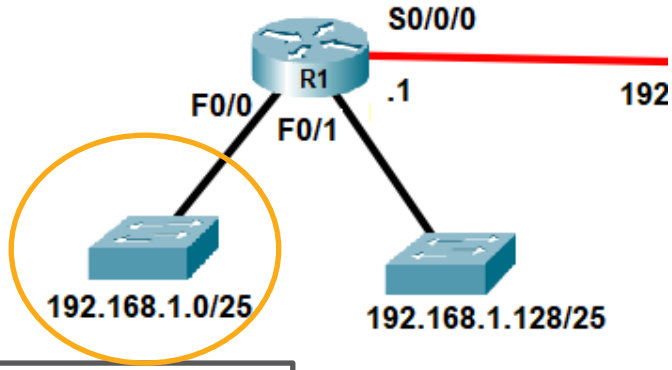
```
R1(config)# router ospf 10
R1(config-router)# router-id 100.100.100.100
% OSPF: Reload or use "clear ip ospf process" command, for this to take effect
R1(config-router)# end
R1# clear ip ospf process
Reset ALL OSPF processes? [no]: y
```

Advertising Networks

- The network command serves 2 purposes:
  - Specifies a directly connected network that the router will include in link state updates
  - Sets the router interface belonging to the specified network to send and receive OSPF messages
- The basic syntax for the **network** command is as follows:

```
Router(config-router)# network address wildcard-mask area area-id
```

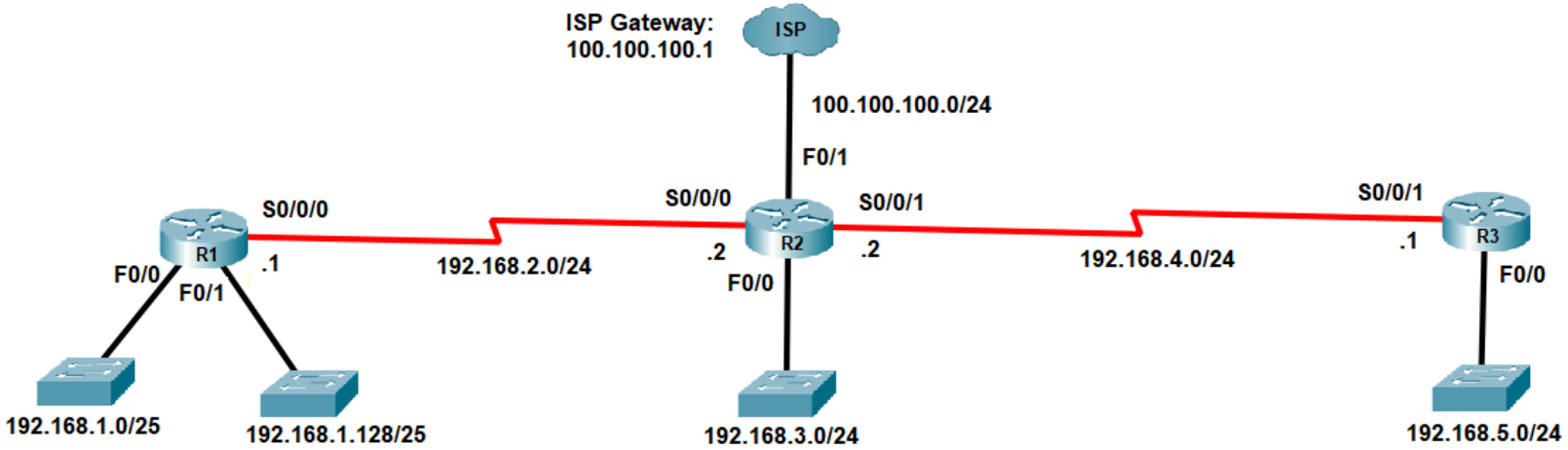
- ***address*** – address of the directly connected network/subnet
- ***wildcard-mask*** - inverse of the network subnet mask
- ***area-id*** - refers to the OSPF area (0- 255). For single-area OSPF, this must be the same value for all networks on all routers in the routing domain and is commonly set to 0



- Example:

```
R1(config-router)# network 192.168.1.0 0.0.0.127 area 0
```

Advertising Networks




```
R1(config)#router ospf 10
R1(config-router)#router-id
  1.1.1.1
R1(config-router)#network
  192.168.1.0 0.0.0.127 area 0
R1(config-router)#network
  192.168.1.128 0.0.0.127 area 0
R1(config-router)#network
  192.168.2.0 0.0.0.255 area 0
```

```
R2(config)#router ospf 10
R2(config-router)#router-id
  2.2.2.2
R2(config-router)#network
  192.168.2.0 0.0.0.255 area 0
R2(config-router)#network
  192.168.3.0 0.0.0.255 area 0
R2(config-router)#network
  192.168.4.0 0.0.0.255 area 0
```

```
R3(config)#router ospf 10
R3(config-router)#router-id
  3.3.3.3
R3(config-router)#network
  192.168.4.0 0.0.0.255 area 0
R3(config-router)#network
  192.168.5.0 0.0.0.255 area 0
```

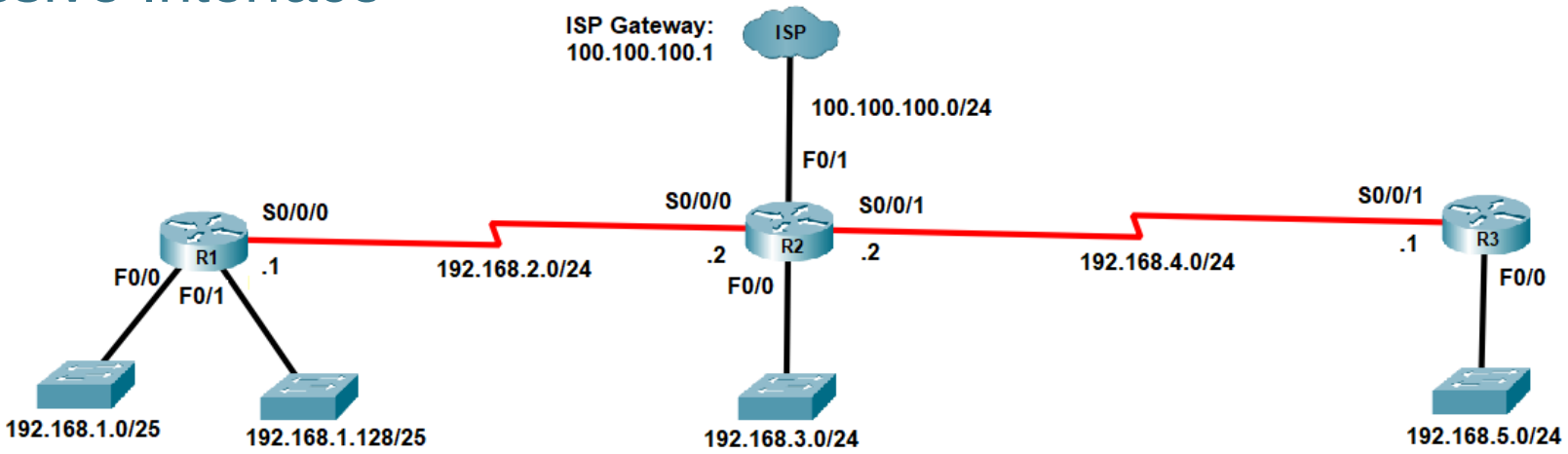
Passive Interfaces

By default, OSPF messages are forwarded out all OSPF-enabled interfaces. However, these messages only need to be sent out interfaces that are connecting to other OSPF-enabled routers.

Sending out unneeded messages on a LAN affects the network in three ways:

- **Inefficient Use of Bandwidth** - Available bandwidth is consumed transporting unnecessary messages.
- **Inefficient Use of Resources** - All devices on the LAN must process and eventually discard the message.
- **Increased Security Risk** - Without additional OSPF security configurations, OSPF messages can be intercepted with packet sniffing software. Routing updates can be modified and sent back to the router, corrupting the routing table with false metrics that misdirect traffic.

Passive Interface



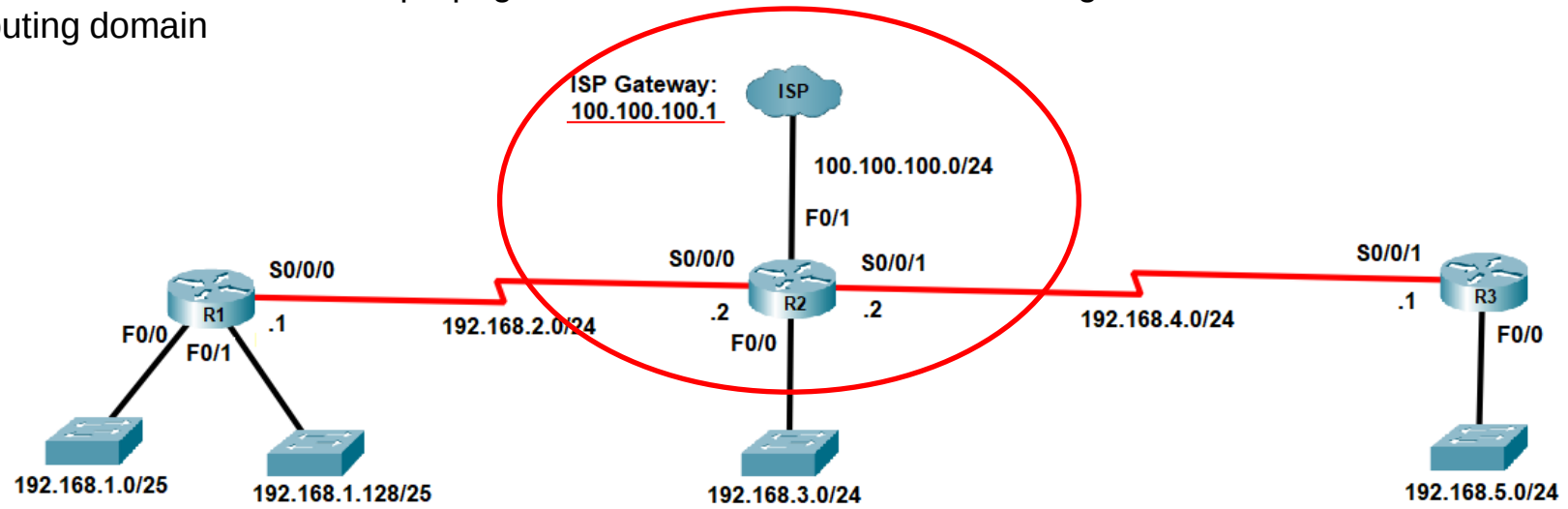

```
R1(config)#router ospf 10
R1(config-router)#router-id 1.1.1.1
R1(config-router)#network 192.168.1.0
   0.0.0.127 area 0
R1(config-router)#network 192.168.1.128
   0.0.0.127 area 0
R1(config-router)#network 192.168.2.0
   0.0.0.255 area 0
R1(config-router)#passive-interface f0/0
R1(config-router)#passive-interface f0/1
```

```
R2(config)#router ospf 10
R2(config-router)#router-id 2.2.2.2
R2(config-router)#network 192.168.2.0
   0.0.0.255 area 0
R2(config-router)#network 192.168.3.0
   0.0.0.255 area 0
R2(config-router)#network 192.168.4.0
   0.0.0.255 area 0
R2(config-router)#passive-interface f0/0
```

```
R3(config)#router ospf 10
R3(config-router)#router-id 3.3.3.3
R3(config-router)#network 192.168.4.0
   0.0.0.255 area 0
R3(config-router)#network 192.168.5.0
   0.0.0.255 area 0
R3(config-router)#passive-interface f0/0
```

Propagating a Default Route

- OSPF can also be used to propagate a static default route from an edge router to other routers within the routing domain




```
R2(config)#router ospf 10
R2(config-router)#router-id 2.2.2.2
R2(config-router)#network 192.168.2.0 0.0.0.255 area 0
R2(config-router)#network 192.168.3.0 0.0.0.255 area 0
R2(config-router)#network 192.168.4.0 0.0.0.255 area 0
R2(config-router)#passive-interface f0/0
R2(config-router)#default-information originate
R2(config-router)#exit
R2(config)#ip route 0.0.0.0 0.0.0.0 100.100.100.1
```

Verifying OSPF

- show ip protocols – displays the current status of OSPF, advertised networks, passive interfaces and list of other OSPF routers where LSUs were received

```
R1#show ip protocols

Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.127 area 0
    192.168.1.128 0.0.0.127 area 0
    192.168.2.0 0.0.0.255 area 0
  Passive Interface(s):
    FastEthernet0/0
    FastEthernet0/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:04:15
    2.2.2.2              110      00:02:38
    3.3.3.3              110      00:02:38
Distance: (default is 110)
```

Verifying OSPF

- show ip ospf interface *int-id* – displays the current status of OSPF on an interface, cost of the connected link and any neighbors on the link

```
R1# show ip ospf interface S0/0/0
Serial0/0/0 is up, line protocol is up
  Internet address is 192.168.2.2/24, Area 0
  Process ID 10, Router ID 1.1.1.1, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.2.2
  Suppress hello for 0 neighbor(s)
```

Verifying OSPF

- show ip ospf neighbor– displays the Adjacency Database (AKA neighbor table) of an OSPF-enabled router. This contains the list of recognized OSPF neighbors and the current adjacency status of the router with each

```
R2#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           0   FULL/  -        00:00:36    192.168.2.2     Serial0/0/0
3.3.3.3           0   FULL/  -        00:00:39    192.168.4.2     Serial0/0/1
```

- .A connected router must be present on the local router's neighbor table before LSUs can be exchanged with it

Verifying OSPF

- show ip ospf database– displays the Link State Database (AKA Topology table) of an OSPF-enabled router. This contains the summary list of IDs of routers in the routing domain from which LSUs were received and the number of LSAs received from each

```
R2#show ip ospf database
            OSPF Router with ID (2.2.2.2) (Process ID 10)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
1.1.1.1         1.1.1.1         773         0x80000006 0x00ef70 4
2.2.2.2         2.2.2.2         676         0x80000008 0x00e3e9 5
3.3.3.3         3.3.3.3         676         0x80000003 0x00f750 3

                Type-5 AS External Link States
Link ID         ADV Router      Age         Seq#       Checksum Tag
0.0.0.0         2.2.2.2         778         0x80000001 0x00e0e9 1
```

Verifying OSPF

- show ip route– displays the Forwarding Database (AKA Routing table) of an OSPF-enabled router. This contains the list of calculated best paths for each destination network and the corresponding total cost.

```
R1#show ip route
...

Gateway of last resort is 192.168.2.1 to network 0.0.0.0

     192.168.1.0/25 is subnetted, 2 subnets
C       192.168.1.0 is directly connected, FastEthernet0/0
C       192.168.1.128 is directly connected, FastEthernet0/1
C    192.168.2.0/24 is directly connected, Serial0/0/0
O    192.168.3.0/24 [110/65] via 192.168.2.1, 00:20:26, Serial0/0/0
O    192.168.4.0/24 [110/128] via 192.168.2.1, 00:19:03, Serial0/0/0
O    192.168.5.0/24 [110/129] via 192.168.2.1, 00:18:43, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 192.168.2.1, 00:20:26, Serial0/0/0
```

- OSPF routes use a source indicator of ‘O’. Propagated default routes have an additional ‘E2’ to indicate an external route
- OSPF routes are assigned an administrative distance of 110

2.5 Fine Tuning OSPF

OSPF Fine Tuning

- OSPF operation can be further fine-tuned by configuring the following:
  - Adjusting link cost calculation
  - Influencing DR and BDR election on multiaccess links
  - Setting link type
  - Adjusting OSPF Hello Intervals

OSPF Cost Metric

- On Cisco routers, the OSPF cost of a link is inversely proportional to the bandwidth of the interface (higher bandwidth = lower cost).
- Formula to calculate the OSPF cost is (rounded up to nearest whole number):

$$\textbf{Cost} = \frac{reference\ bandwidth}{interface\ bandwidth}$$

Where default reference bandwidth = 100,000,000 bps

Interface Type	Reference Bandwidth in bps		Default Bandwidth in bps	Cost
10 Gbps Ethernet	100,000,000	÷	10,000,000,000	1
1 Gbps Ethernet	100,000,000	÷	1,000,000,000	1
100 Mbps Ethernet	100,000,000	÷	100,000,000	1
10 Mbps Ethernet	100,000,000	÷	10,000,000	10
1.544 Mbps Serial	100,000,000	÷	1,544,000	64
128 kbps Serial	100,000,000	÷	128,000	781
64 kbps Serial	100,000,000	÷	64,000	1562

- Issue: The default reference bandwidth causes OSPF to assume the same cost for Gigabit Ethernet links and Fast Ethernet links → Not good because Gigabit should be faster!

OSPF Fine Tuning

Adjusting the Link Cost

- To fix the issue, the reference bandwidth can be adjusted using the **auto-cost reference-bandwidth** *Mbps* router configuration command (recommended to do this on ALL routers).
- Example: To set a reference bandwidth of 10 Gbps:

```
R1(config)# router ospf 10
R1(config-router)# auto-cost reference bandwidth 10000
R1(config-router)# end
```

Interface Type	Reference Bandwidth in bps		Default Bandwidth in bps	Cost
10 Gbps Ethernet	100,000,000	÷	10,000,000,000	1
1 Gbps Ethernet	100,000,000	÷	1,000,000,000	1
100 Mbps Ethernet	100,000,000	÷	100,000,000	1
10 Mbps Ethernet	100,000,000	÷	10,000,000	10
1.544 Mbps Serial	100,000,000	÷	1,544,000	64
128 kbps Serial	100,000,000	÷	128,000	781
64 kbps Serial	100,000,000	÷	64,000	1562

Interface Type	Reference Bandwidth in bps		Default Bandwidth in bps	Cost
10 Gbps Ethernet	10,000,000,000	÷	10,000,000,000	1
1 Gbps Ethernet	10,000,000,000	÷	1,000,000,000	10
100 Mbps Ethernet	10,000,000,000	÷	100,000,000	100
10 Mbps Ethernet	10,000,000,000	÷	10,000,000	1000
1.544 Mbps Serial	110,000,000,000	÷	1,544,000	6477
128 kbps Serial	10,000,000,000	÷	128,000	78126
64 kbps Serial	10,000,000,000	÷	64,000	156250

Adjusting the Link Cost

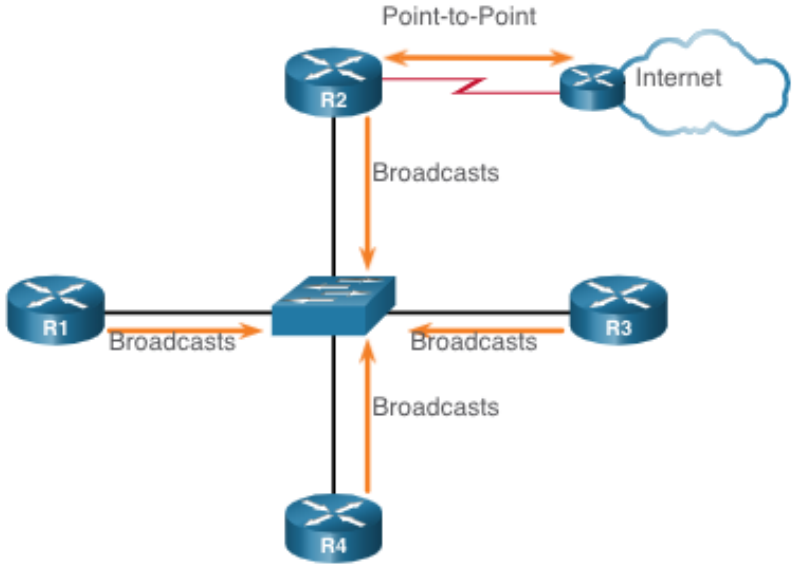
- Interface cost may also be manually assigned
- Reasons to manually set the cost value include:
  - The Administrator may want to influence path selection within OSPF, causing different paths to be selected than what normally would given default costs and cost accumulation.
  - Connections to equipment from other vendors who use a different formula to calculate OSPF cost.
- To change the cost value reported by the local OSPF router to other OSPF routers, use the interface configuration command **ip ospf cost** *value*.
- Example:

```
R1(config)# interface g0/0/1
R1(config-if)# ip ospf cost 30
R1(config-if)# end
R1#
```

DR and BDR Election

Recall: In multiaccess network links, OSPF controls the distribution of LSAs by assigning roles to routers using an election process.

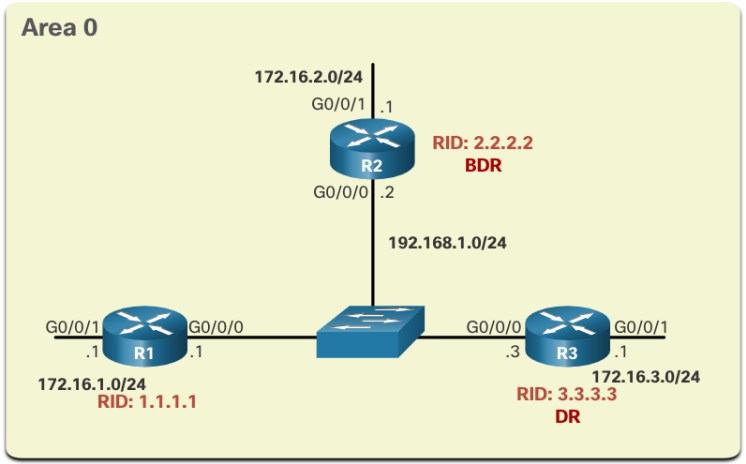
- The **Designate Router (DR)** collects LSAs distributing these from and to routers on the same link by multicasting to 224.0.0.5
- The **Backup Designated Router (BDR)** listens passively and maintains a relationship with all the routers. If the DR stops producing Hello packets, the BDR promotes itself and assumes the role of DR.
- All other routers become a **DROTHER** and use the multiaccess address 224.0.0.6 to send OSPF packets to the DR and BDR only



DR and BDR Election

The OSPF DR and BDR election is based on the following criteria, in sequential order:

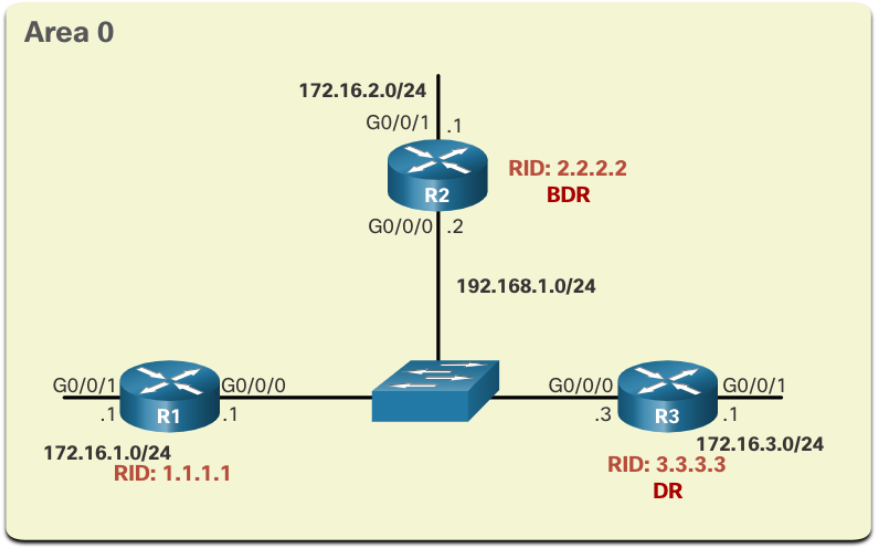
1. The routers in the network elect the router with the highest OSPF interface priority as the DR. The router with the second highest interface priority is becomes the BDR.
2. If the interface priorities are equal, then the router with the highest router ID is elected the DR. The router with the second highest router ID is the BDR.



- The election process takes place when the first router with an OSPF-enabled interface is active on the network. If all routers on the network have not finished booting, it is possible that a router with a lower priority / router ID becomes the DR.
- The addition of a new router does not initiate a new election process.

DR and BDR Election

To verify the role of the OSPFv2 router, use the **show ip ospf interface**




```
R1# show ip ospf interface GigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet Address 192.168.1.1/24, Area 0, Attached via Interface Enable
  Process ID 10, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
  (output omitted)
  Transmit Delay is 1 sec, State DROTHER, Priority 1
  Designated Router (ID) 3.3.3.3, Interface address 192.168.1.3
  Backup Designated router (ID) 2.2.2.2, Interface address 192.168.1.2
  (output omitted)
  Neighbor Count is 2, Adjacent neighbor count is 2
  Adjacent with neighbor 2.2.2.2 (Backup Designated Router)
  Adjacent with neighbor 3.3.3.3 (Designated Router)
  Suppress hello for 0 neighbor(s)
R1#
```

DR and BDR Election

- Use **show ip ospf neighbor** to verify roles of all neighbor routers on the link

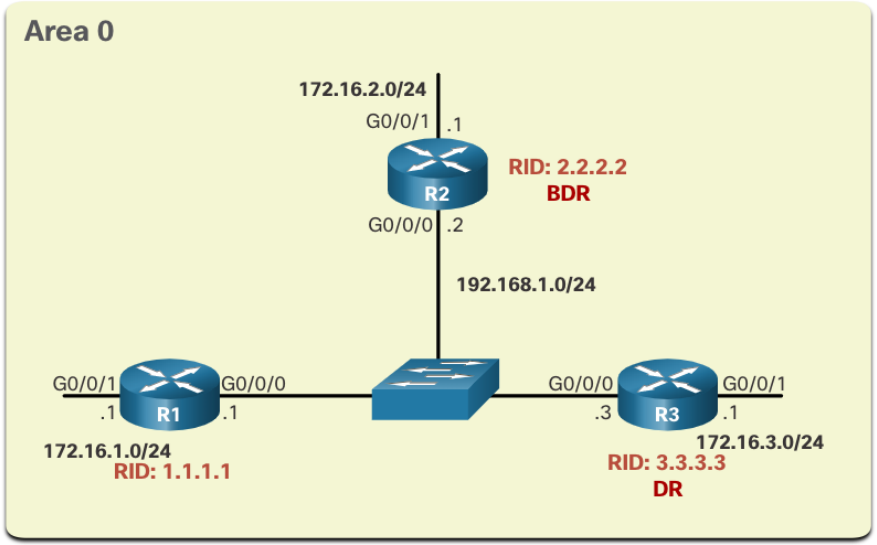
```
R2# show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time       Address         Interface
1.1.1.1         1     FULL/DROTHER 00:00:31    192.168.1.1     GigabitEthernet0/0/0
3.3.3.3         1     FULL/DR         00:00:34  192.168.1.3     GigabitEthernet0/0/0
```

- The state of neighbors in multiaccess networks can be as follows:
  - **FULL/DROTHER** – The local router is a DR or BDR that is fully adjacent with a DROTHER router
  - **FULL/DR** - The local router is fully adjacent with the indicated DR neighbor
  - **FULL/BDR** - The local router is fully adjacent with the indicated BDR neighbor.
  - **2-WAY/DROTHER** - The local router is a DROTHER and has a neighbor relationship with another DROTHER router. These two neighbors exchange Hello packets only.
- Note: The normal state for an OSPF router is usually FULL or 2-WAY (in multiaccess links). If it is stuck in another state, it is an indication that there are problems in forming adjacencies.

DR and BDR Election

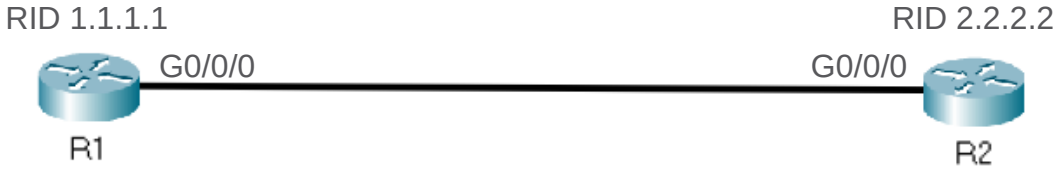
- Instead of relying on the router ID, it is better to control the election by setting interface priorities. This allows an administrator to choose a router with better resources to handle DR tasks
- To set the priority of an interface, use the command **ip ospf priority** *value*, where value is 0 to 255.
- Example: To set R1 as DR using priority

```
R1(config)# interface GigabitEthernet 0/0/0
R1(config-if)# ip ospf priority 255
R1(config-if)# end
R1# clear ip ospf process
Reset ALL OSPF processes? [no]: y
R1# *Jun 5 03:47:41.563: %OSPF-5-ADJCHG:
Process 10, Nbr 2.2.2.2 on
GigabitEthernet0/0/0 from FULL to DOWN,
Neighbor Down: Interface down or detached
```



Setting Link Type

- By default, a DR and BDR are elected on Ethernet interfaces even if the link directly connects 2 routers only

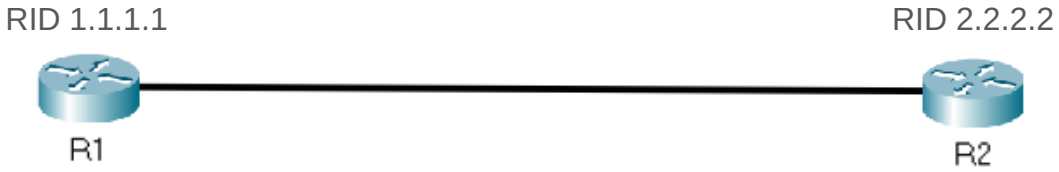



```
R1# show ip ospf interface GigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet Address 10.1.1.5/30, Area 0, Attached via Interface Enable
  Process ID 10, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown    Topology Name
        0           1        no           no          Base
  Enabled by interface config, including secondary ip addresses
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 2.2.2.2, Interface address 10.1.1.6
  Backup Designated router (ID) 1.1.1.1, Interface address 10.1.1.5
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
```

OSPF Fine Tuning

Setting Link Type

- DR/BDR election is unnecessary for the link since it is actually a point-to-point connection
- Election can be disabled to speed up adjacency establishment by specifying the link type of the interface using the **ip ospf network point-to-point** command




```
R1(config)# interface GigabitEthernet 0/0/0
R1(config-if)# ip ospf network point-to-point
*Jun 6 00:44:05.208: %OSPF-5-ADJCHG: Process 10, Nbr 2.2.2.2 on GigabitEthernet0/0/0 from
FULL to DOWN, Neighbor Down: Interface down or detached
*Jun 6 00:44:05.211: %OSPF-5-ADJCHG: Process 10, Nbr 2.2.2.2 on GigabitEthernet0/0/0 from
LOADING to FULL, Loading Done
R1(config-if)# end
R1# show ip ospf interface GigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet Address 10.1.1.5/30, Area 0, Attached via Interface Enable
  Process ID 10, Router ID 1.1.1.1, Network Type POINT_TO_POINT, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown    Topology Name
```

Hello Packet Intervals

- OSPFv2 Hello packets are transmitted to multicast address 224.0.0.5 (all OSPF routers) every 10 seconds by default on multiaccess and point-to-point networks.
- The Dead interval is the period that the router waits to receive a Hello packet before declaring the neighbor down.
  - If the Dead interval expires before a router receives a Hello packet, OSPF removes that neighbor from its link-state database (LSDB) and initiates the flooding of LSUs to update all routers
  - By default, it is 4 times the Hello interval - 40 seconds on multiaccess and point-to-point networks.

```
R1# show ip ospf interface S0/0/0
Serial0/0/0 is up, line protocol is up
  Internet address is 192.168.2.2/24, Area 0
  Process ID 10, Router ID 1.1.1.1, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.2.2
  Suppress hello for 0 neighbor(s)
```

Hello Packet Intervals

- OSPF timers can be adjusted so that routers detect network failures in less time. Doing this increases traffic, but results in faster convergence
  - The OSPF Hello and Dead intervals are configurable on a per-interface basis.
  - Intervals must match between neighbors otherwise an adjacency does not occur.

```
Router(config-if)# ip ospf hello-interval seconds
Router(config-if)# ip ospf dead-interval seconds
```

- Example:

```
R1(config)# interface S0/0/0
R1(config-if)# ip ospf hello-interval 5
R1(config-if)# ip ospf dead-interval 20
R1(config-if)# end

R1# show ip ospf interface S0/0/0
Serial0/0/0 is up, line protocol is up
  Internet address is 192.168.2.2/24, Area 0
  Process ID 10, Router ID 1.1.1.1, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 5, Dead 20, Wait 20, Retransmit 5
    Hello due in 00:00:02
```

Module Summary

What did you learn in this module?

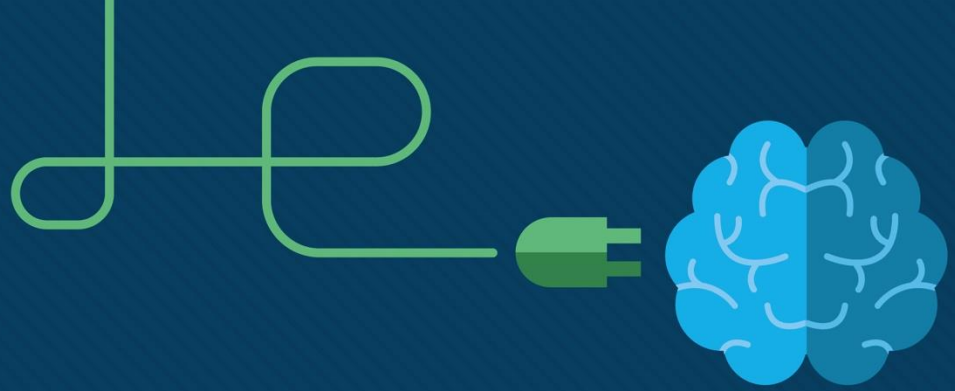
- Open Shortest Path First (OSPF) is a link-state routing protocol
  - A link is an interface on a router and is also a network segment
  - All link-state information includes the network prefix, prefix length, and cost.
- OSPF messages are used to create and maintain three OSPF databases: the adjacency database creates the neighbor table, the link-state database (LSDB) creates the topology table, and the forwarding database creates the routing table.
- An OSPF router topology table uses results of calculations based on the Dijkstra SPF (shortest-path first) algorithm which uses the cumulative cost to choose the best route to reach a destination.
- OSPF routers complete a generic link-state routing process to reach a state of convergence: Establish Neighbor Adjacencies, Exchange Link-State Advertisements, Build the Link State Database, Execute the SPF Algorithm, Choose the Best Route
- The states that OSPF progresses through to do reach convergence are down state, init state, two-way state, ExStart state, Exchange state, loading state, and full state.

What did you learn in this module?

- Routers running OSPF exchange 5 types of messages to convey routing information : Hello packet, Database Description, Link-state Request, Link-state Update, and Link-state Acknowledgment.
  - Hello packets are used to discover neighbor routers and establish adjacencies and are sent as multicasts.
  - Database Description packets are used to send a summary of a router's link states
  - Link State Requests and Link State Updates are used to exchanged detailed link state information
  - Link State Acknowledge packets are used to acknowledge DBD, LSRs and LSUs
- Routers connected to multiaccess networks elect a Designated router and Backup Designated router to avoid creation of multiple adjacencies and extensive flooding of LSAs. The DR serves as distribution point of link state advertisements
- To run OSPF on a router, the following are needed:
  - A process ID to OSPF
  - A unique router ID (manually assigned or automatically derived from loopback or physical interface IPv4 address)
  - Network address and wildcard mask of links to advertise

What did you learn in this module?

- To assign a cost to a link, the router divides a reference bandwidth with the link interface bandwidth. The default reference bandwidth is 100 Mbps and must be adjusted to differentiate among link types in networks with high-bandwidth Ethernet links
- Link cost may also be manually set, and is usually done to manipulate preferred routes or when interfacing with routers from other manufacturers that do not use the same cost computation
- The DR / BDR election is based on
  - Interface priority (highest = DR, 2nd highest = BDR); or
  - Router ID (highest = DR, 2nd highest = BDR)
- Routers maintain full adjacency and send LSUs only to the DR and BDR on a multiaccess link
- Ethernet links may be set to ‘point-to-point’ type to skip the DR/BDR election if only 2 routers are connected using the link
- Hello (default 10 secs) and Dead (default 40 secs) intervals control the frequency of Hello packet transmission and the amount of time before a neighbor router is declared to be unreachable. Values may be set on a per-interface basis to adjust convergence time



Module 2
Network Security Concepts

ITNET04

WAN Connectivity

Module Objectives

Module Title: Network Security Concepts

Module Objectives:

- Describe the current state of cybersecurity, attack vectors, threat actors and consequences of data loss
- Describe network attack types
- Describe the vulnerabilities of the TCP/IP stack and the attacks that exploit them
- Describe network security best practices and solutions
- Describe common cryptographic processes used to protect data in transit.

References: CCNA ENSA Module 3

3.1 Current State of Cybersecurity

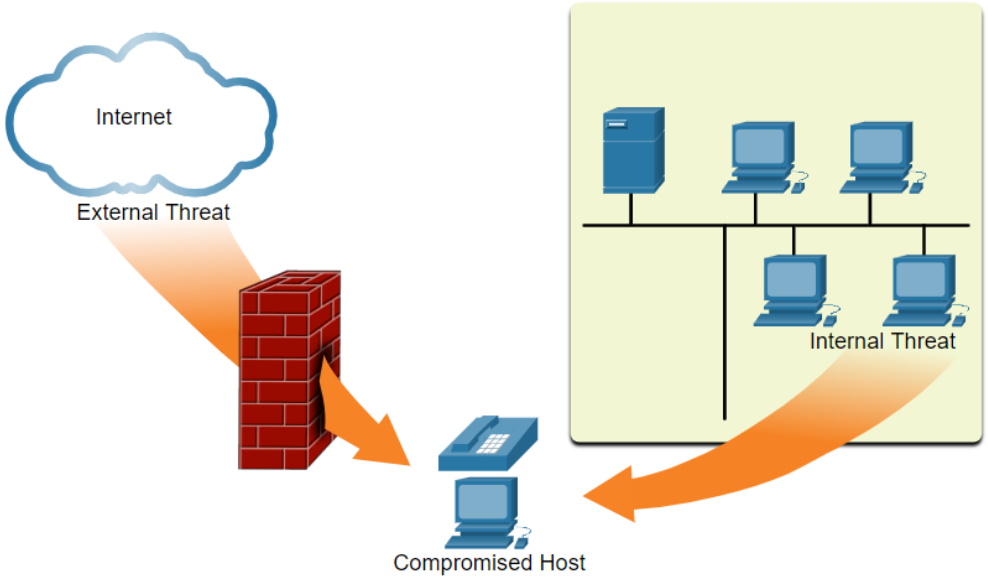
Current State of Affairs

- Cyber criminals continue to develop the expertise and tools necessary to take down critical infrastructure and systems. Maintaining a secure network ensures the safety of network users and protects commercial interests.
- Identify the terms described in the table:

Security Terms	Description
Asset	Anything of value to the organization. It includes people, equipment, resources, and data.
Vulnerability	A weakness in a system, or its design, that could be exploited by a threat.
Threat	A potential danger to a company's resources, data, or network functionality.
Exploit	A mechanism that takes advantage of a weakness.
Control	A counter-measure that reduces the likelihood or severity of a potential security incident
Risk	Likelihood of an occurrence and degree of negative impact of a security incident affecting an organization

Vectors of Network Attacks

- An attack vector is a path by which a threat actor can gain access to a server, host, or network.
- Can originate from inside or outside the corporate network
- Internal threats have the potential to cause greater damage than external threats because internal users have direct access to the building and its infrastructure devices.



Threat Actors

A **threat actor** is any person who has the potential to impact the security of an organization.

Threat Actor	Description
Script Kiddies	These are teenagers or inexperienced hackers running existing scripts, tools, and exploits, to cause harm, but typically not for profit.
Vulnerability Broker	These are usually gray hat hackers who attempt to discover exploits and report them to vendors, sometimes for prizes or rewards.
Hacktivists	These are gray hat hackers who publicly protest organizations or governments by posting articles, videos, leaking sensitive information, and performing network attacks.
Cyber criminals	These are black hat hackers who are either self-employed or working for large cybercrime organizations who steal for financial gain.
State-Sponsored	These are either white hat or black hat hackers who steal government secrets, gather intelligence, and sabotage networks. Their targets are foreign governments, terrorist groups, and corporations.
Insiders	These are people who infiltrate an organization and work from within to get around he organization's cybersecurity framework for profit or for revenge
Internal Users	Members or employees of an organization who are not malicious but may unintentionally cause security incidents.

Data Loss

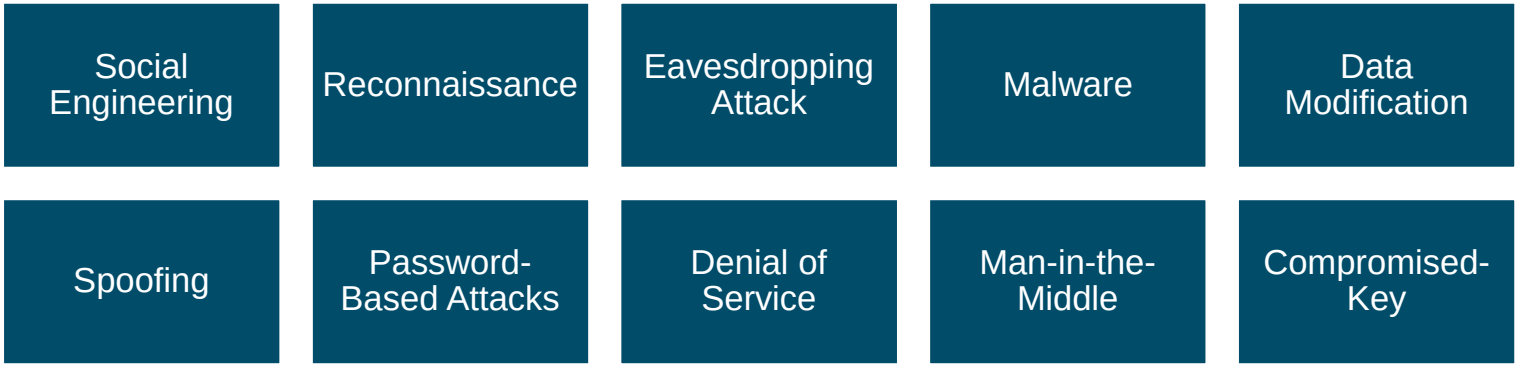
- Data loss or data exfiltration is when data is intentionally or unintentionally lost, stolen, or leaked to the outside world.

- The data loss can result in:
  - Brand damage and loss of reputation
  - Loss of competitive advantage
  - Loss of customers
  - Loss of revenue
  - Litigation/legal action resulting in fines and civil penalties
  - Significant cost and effort to notify affected parties and recover from the breach
- Network security professionals must protect the organization's data using various Data Loss Prevention (DLP) controls which combine strategic, operational and tactical measures.

3.2 Network Attacks

Attack Types

- To exploit a vulnerability, a threat actor must have an attack technique or tool.
- Over the years, attacks have become more sophisticated, highly automated and easier to implement even with minimal technical knowledge.



Attack Types

Social Engineering

- Social engineering is an attack that attempts to manipulate people into performing actions or divulging confidential information by rely on people's weakness or willingness to help

Social Engineering Attack	Description
Pretexting	A threat actor pretends to need personal or financial data to confirm the identity of the recipient.
Phishing	A threat actor sends fraudulent email which is disguised as being from a legitimate, trusted source to trick the recipient into installing malware on their device, or to share personal or financial information.
Spam	Also known as junk mail, this is unsolicited email which often contains harmful links, malware, or deceptive content.
Something for Something	Sometimes called "Quid pro quo", this is when a threat actor requests personal information from a party in exchange for something such as a gift.
Baiting	A threat actor leaves a malware infected flash drive in a public location. A victim finds the drive and unsuspectingly inserts it into their laptop, unintentionally installing malware.
Impersonation	This type of attack is where a threat actor pretends to be someone they are not to gain the trust of a victim.
Tailgating	This is where a threat actor quickly follows an authorized person into a secure location to gain access to a secure area.
Shoulder surfing	This is where a threat actor inconspicuously looks over someone's shoulder to steal their passwords or other information.
Dumpster diving	This is where a threat actor rummages through trash bins to discover confidential documents

Attack Types

Social Engineering

- The Social Engineering Toolkit (SET) was designed to help white hat hackers and security professionals to create social engineering attacks to test their own networks.
- Enterprises must educate their users about the risks of social engineering, and develop strategies to validate identities over the phone, via email, or in person.

Attack Types
Malware

- Malware are any programs that perform any unwanted or harmful behavior on a computer.
- End devices are particularly prone to malware attacks and threat actors rely on users to install malware to help exploit the security gaps.
- Types:

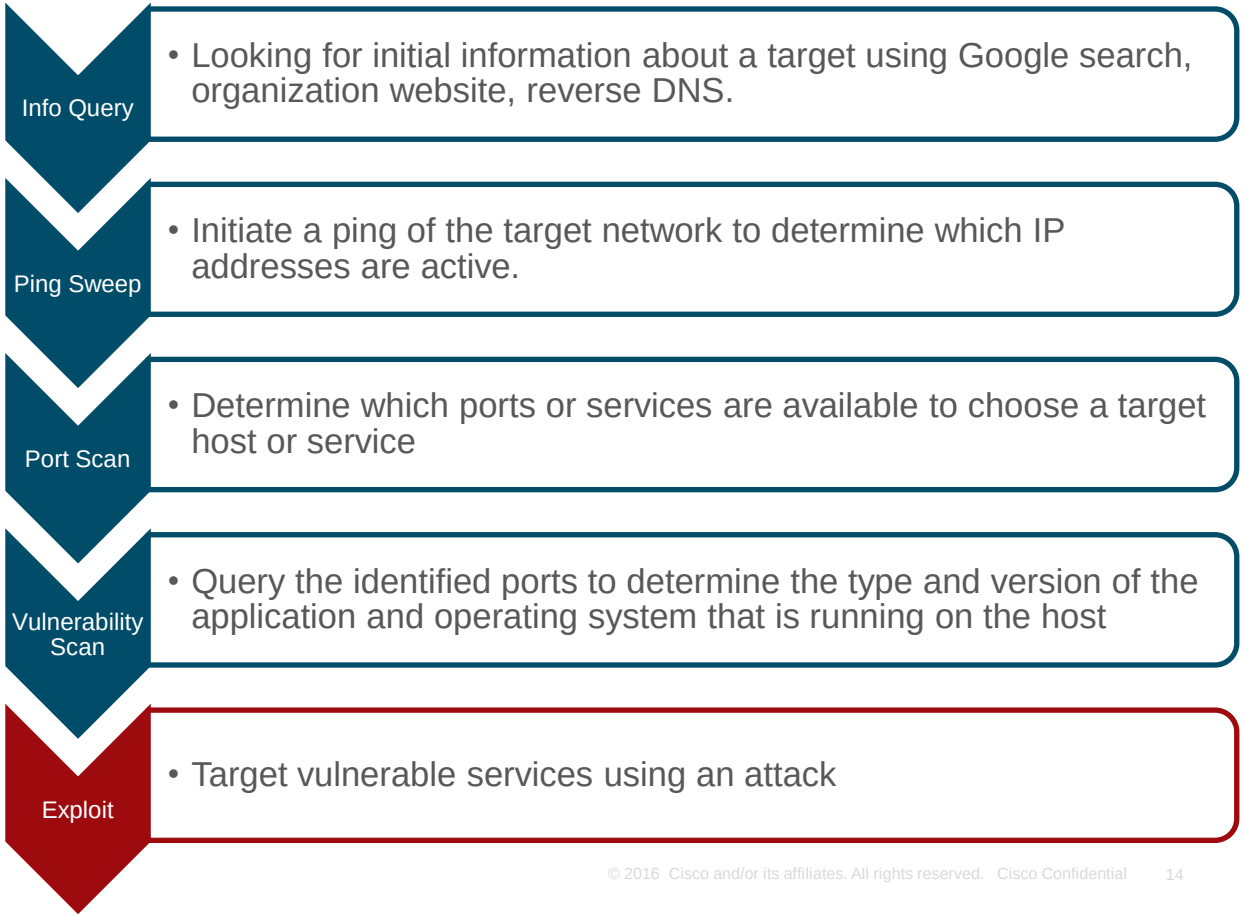
Virus	Programs that hide by attaching itself to computer code, software, or documents on the computer and require human action to propagate and infect other computers.
Trojan	Programs that look useful but also carry malicious code. Commonly distributed through freeware or ‘cracked’ software
Worm	A self-replicating program that propagates automatically through the network without user actions by exploiting vulnerabilities in legitimate software.
Ransomware	Program that denies a user access to their data by encrypting files and then demanding a ransom for the decryption key
Adware	Display unsolicited pop-up web browser windows, new toolbars, or unexpectedly redirect a webpage to a different website.

Common Network Attacks

- When malware is delivered and installed, the payload can be used to cause a variety of network related attacks.
- Network attacks exploit vulnerabilities of the TCP/IP protocol stack and network application services
- Networks are susceptible to the following types of attacks:
  - Reconnaissance Attacks
  - Access Attacks
  - DoS Attacks

Reconnaissance Attacks

- Reconnaissance refer to information gathering used to perform unauthorized discovery and mapping of systems, services, or vulnerabilities.
- Normally precede access attacks or DoS attacks.



Access Attacks

- Access attacks exploit known vulnerabilities in authentication services, FTP services, and web services. The purpose of these types of attacks is to gain entry to web accounts, confidential databases, and other sensitive information.
- **Password Attacks:** Threat actor attempts to discover critical system passwords using various methods. Password attacks are very common and can be launched using a variety of password cracking tools.
- **Spoofing Attacks:** Threat actor device attempts to pose as another device by falsifying data commonly through spoofing methods
- Other Access attacks include:
  - Trust exploitations
  - Port redirections
  - Man-in-the-middle attacks
  - Buffer overflow attacks

DoS and DDoS Attacks

- A Denial of Service (DoS) attacks interrupt of network services to users, devices, or applications to cause significant loss of time and money.
- There are two major approaches to DoS attacks:
  - **Overwhelming Quantity of Traffic** - The threat actor sends an enormous quantity of data at a rate that the network, host, or application cannot handle to slow down or crash a service
  - **Maliciously Formatted Packets** - The threat actor sends wrongly formatted packet to a host or application that the receiver is not designed to handle, causing it to run slowly or crash.
- A Distributed DoS Attack (DDoS) is similar to a DoS attack, but it originates from multiple, coordinated sources.

3.3 Protocol Vulnerabilities and Threats

IPv4 and IPv6

- IP is a connectionless protocol which does not validate packet sources nor perform matching between request and response packets
- Some of the more common IP related attacks:

ICMP Attacks

Amplification and Reflection Attacks

Address Spoofing

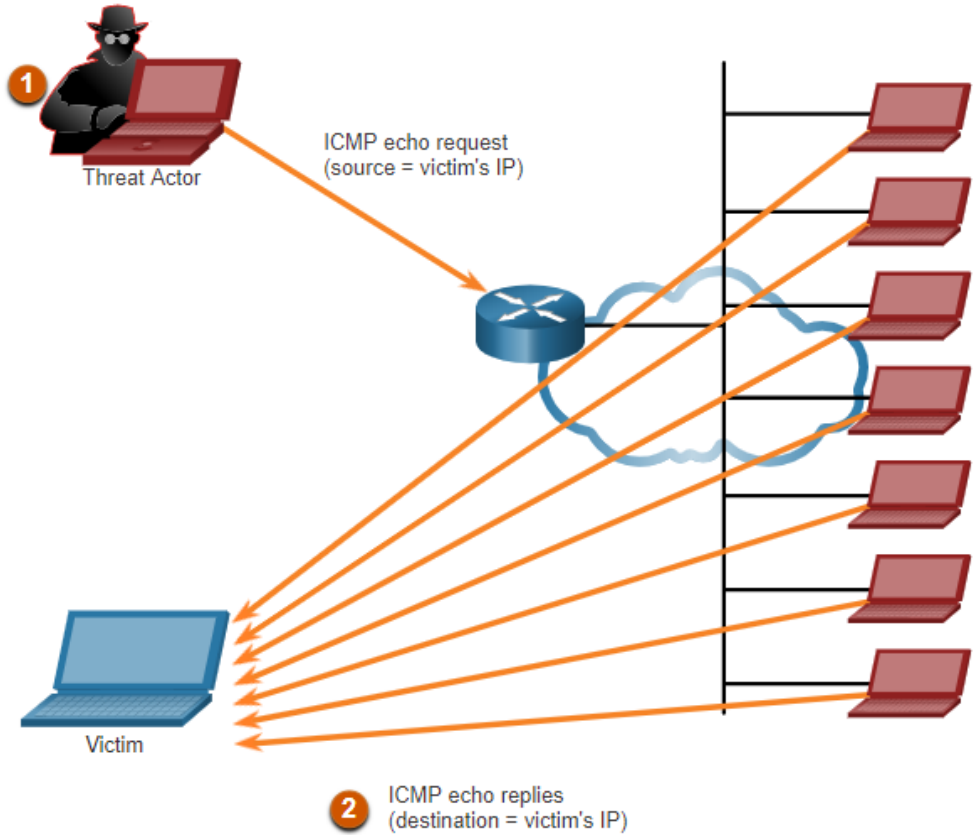
ICMP Attacks

- ICMP is commonly used for reconnaissance to map out a network topology, discover which hosts are active (reachable), identify the host operating system (OS fingerprinting), and determine the state of a firewall.
- Threat actors also use ICMP for DoS attacks.
- Common ICMP messages used in attacks are:

ICMP Messages used by Hackers	Description
ICMP echo request and echo reply	This is used to perform host verification and DoS attacks.
ICMP unreachable	This is used to perform network reconnaissance and scanning attacks.
ICMP mask reply	This is used to map an internal IP network.
ICMP redirects	This is used to lure a target host into sending all traffic through a compromised device and create a Man in the Middle attack.
ICMP router discovery	This is used to inject bogus route entries into the routing table of a target host.

Amplification and Reflection Attacks

- Threat actors often use amplification and reflection techniques (e.g. broadcasting a request using a fake source) to create DoS attacks.
- Threat actors also use resource exhaustion attacks to either to crash a target host or to consume the resources of a network.



Address Spoofing Attacks

- IP address spoofing attacks occur when a threat actor creates packets with false source IP address information to either hide the identity of the sender, or to pose as another legitimate user.
- Usually combined with another exploit to create an attack (e.g. Smurf DoS)
- Spoofing attacks can be non-blind or blind:
  - **Non-blind spoofing** - The threat actor can see the traffic that is being sent between the host and the target. Non-blind spoofing determines the state of a firewall and sequence-number prediction. It can also hijack an authorized session.
  - **Blind spoofing** - The threat actor cannot see the traffic that is being sent between the host and the target. Blind spoofing is used in DoS attacks.

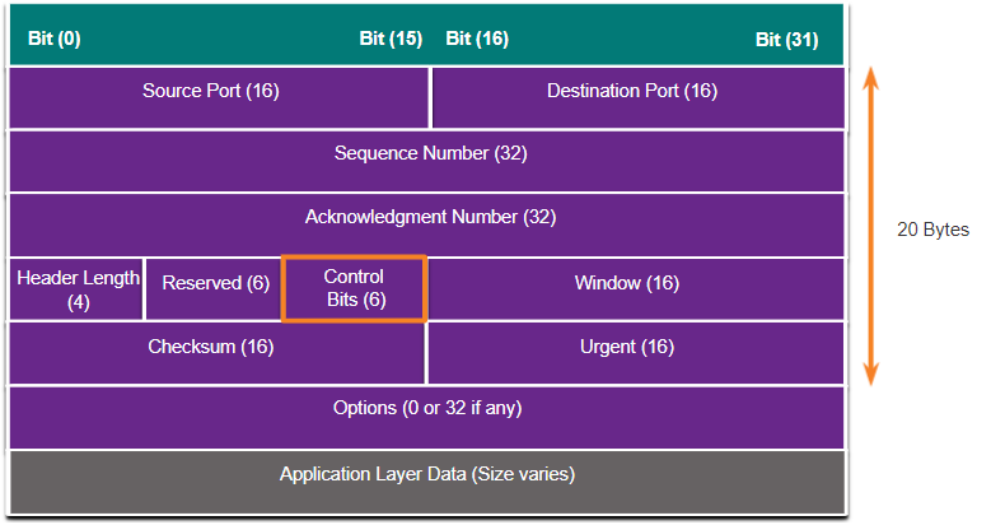
TCP Services

TCP provides these services:

- **Reliable delivery** - TCP incorporates acknowledgments to guarantee delivery. If a timely acknowledgment is not received, the sender retransmits the data.
- **Flow control** - TCP implements adjust the speed at which data is sent according to recipient capabilities by acknowledging data as multiple segments.
- **Stateful communication** - TCP ensures that a connection is established before exchanging data.

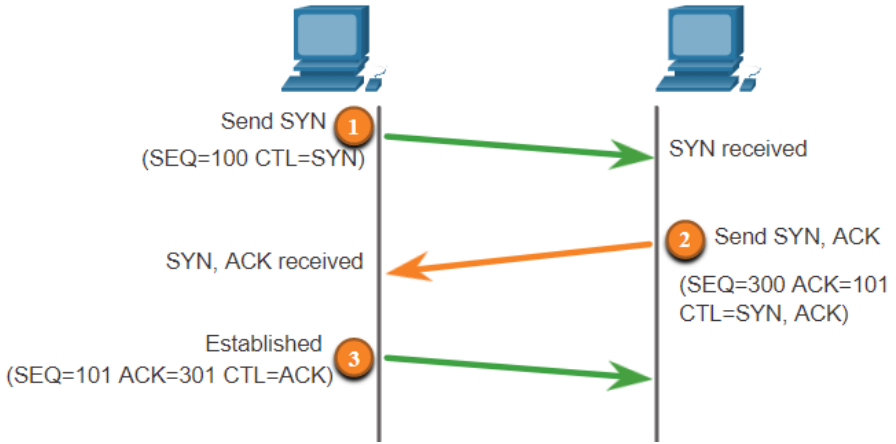
TCP segment information appears after the IP header. The following are the six control bits of the TCP segment:

- **URG** - Urgent pointer field significant
- **ACK** - Acknowledgment field significant
- **PSH** - Push function
- **RST**- Reset the connection
- **SYN** - Synchronize sequence numbers
- **FIN** - No more data from sender

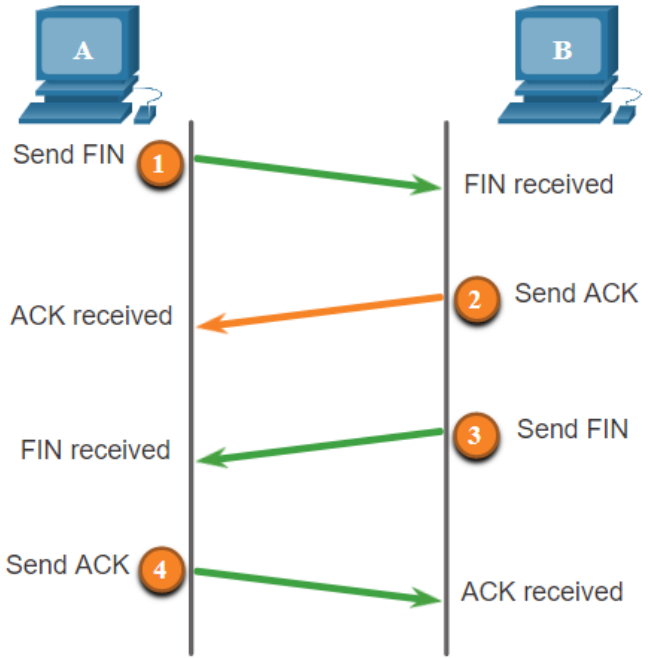


TCP Services (Cont.)

A TCP connection is established in three steps:

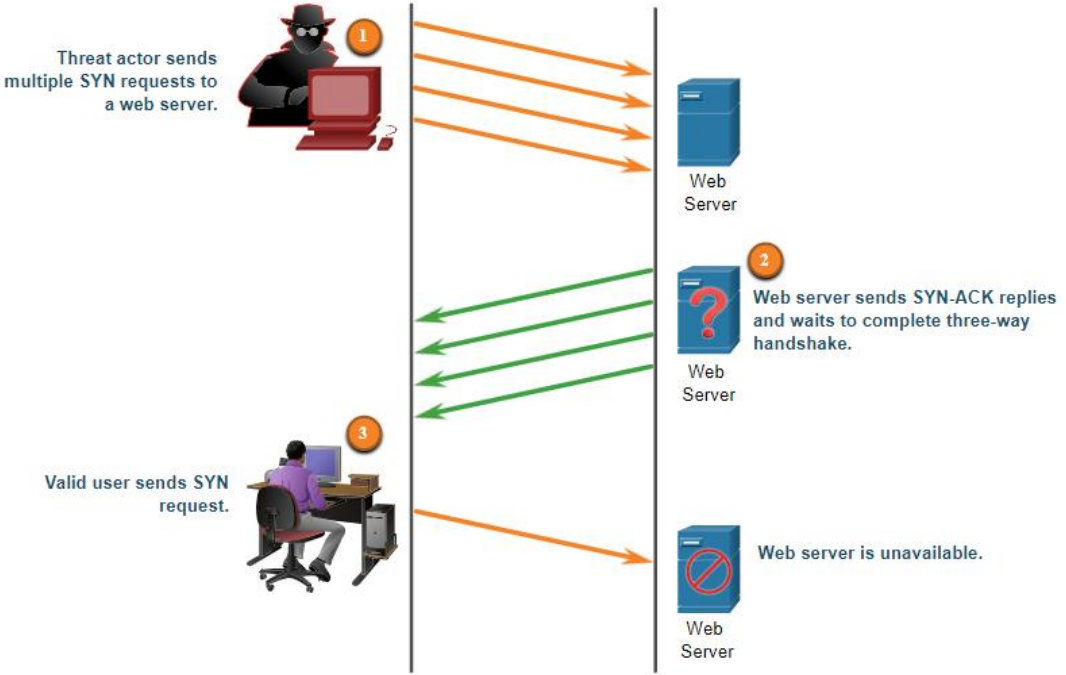


Terminating a TCP session uses the following four-way exchange process:



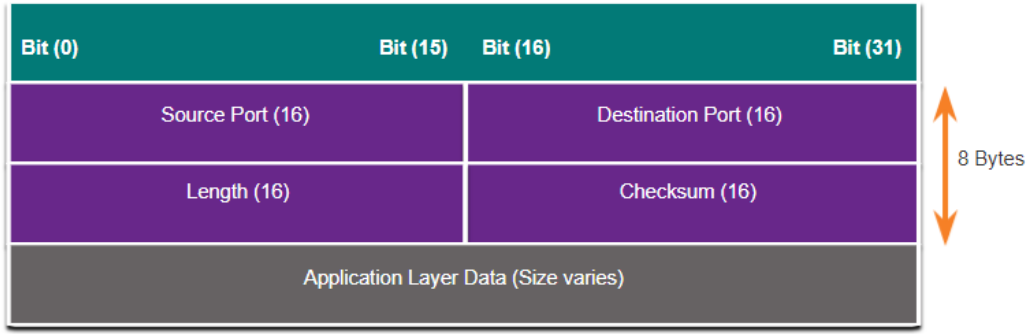
TCP Attacks

- **TCP SYN Flood Attack -** The threat actor sends multiple SYN requests to a webserver without acknowledging SYN-ACKs to tie up server resources and cause it to be unable to serve legitimate users
- **TCP Reset Attack** – A threat actor spoofs the IP address of a victim and sends a TCP RST packet to the host it is communicating with, which forces the connection between the hosts to be closed
- **TCP Session Hijack – A** threat actor takes over an connected host as it communicates with the target. The threat actor must spoof the IP address of one host and predict the next sequence number to insert itself in the connection



UDP Segment Header and Operation

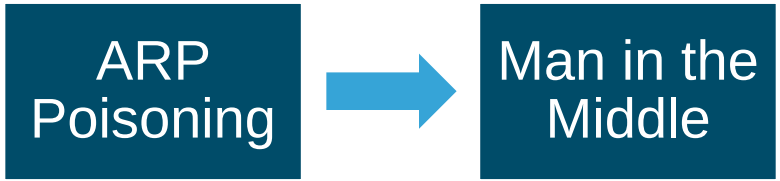
- UDP is a connectionless transport layer protocol commonly used by application protocols that make simple request and reply transactions (e.g. DNS, TFTP, NFS, SNMP, real time apps and media streaming)
- Much lower overhead than TCP because and does not offer the sophisticated retransmission, sequencing, and flow control mechanisms that provide reliability.



- **UDP Flood Attacks:** The threat actor uses a tool to send a flood of UDP packets, often from a spoofed host, to a server to sweep through all the known ports trying to find closed ports. This will cause the server to become busy replying with ICMP port unreachable messages.

ARP Vulnerabilities

- Hosts broadcast an ARP Request to other hosts on the segment to determine the MAC address of a host with a particular IP address. The host with the matching IP address in the ARP Request sends an ARP Reply.
- Recall: Any client can send an unsolicited ARP Reply called a “gratuitous ARP” which cause other network hosts to update their ARP tables.
- This feature of ARP makes it possible for any host can claim to be the owner of any IP or MAC address and perform the following attacks:



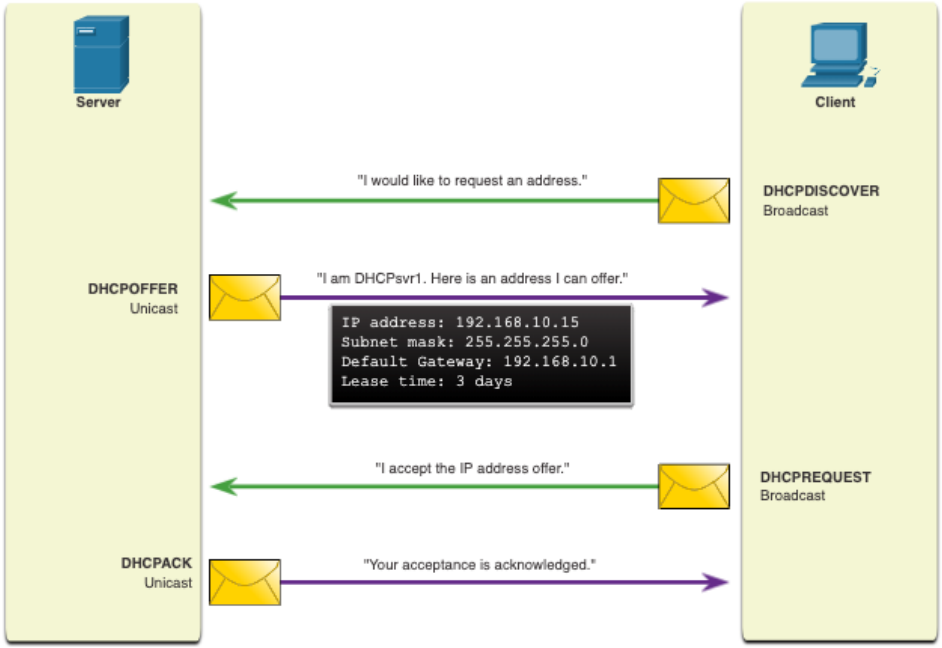
- Prevented by using Dynamic ARP Inspection on switches

DHCP

- DHCP servers dynamically provide IP configuration information to clients.
- Recall: DHCP servers and client are not capable of authenticating if requests or offers come from legitimate sources.
- DHCP attacks:

  DHCP Starvation **DHCP Spoofing**

- Prevented by enabling DHCP snooping on switches



DNS Attacks

- The Domain Name Service (DNS) protocol matches resource names (e.g. www.dlsu.edu.ph) with the corresponding numeric network address
- It includes the format for queries, responses, and data and uses resource records (RR) to identify the type of DNS response.
- DNS attacks include the following:
  - DNS open resolver attacks – attacks involving public DNS servers, commonly through injection of false DNS entries, overwhelming them using a DoS, or using them for attack amplification
  - DNS stealth attacks – attacks that involve DNS to hide the identity of the attacker
  - DNS domain shadowing attacks - threat actor takes domain account credentials to create multiple sub-domains typically pointing to malicious servers to be used during the attacks
  - DNS tunneling attacks – threat actor places non-DNS traffic within DNS traffic. Common technique used to relay commands between a botnet CnC server and an infected host

DNS Attacks (Cont.)

DNS Stealth Attacks: To hide their identity, threat actors also use the DNS stealth techniques described in the table to carry out their attacks.

DNS Stealth Techniques	Description
Fast Flux	Threat actors use this technique to hide their phishing and malware delivery sites behind a quickly-changing network of compromised DNS hosts. The DNS IP addresses are continuously changed within minutes. Botnets often employ Fast Flux techniques to effectively hide malicious servers from being detected.
Double IP Flux	Threat actors use this technique to rapidly change the hostname to IP address mappings and to also change the authoritative name server. This increases the difficulty of identifying the source of the attack.
Domain Generation Algorithms	Threat actors use this technique in malware to randomly generate domain names that can then be used as rendezvous points to their command and control (C&C) servers.

3.4 Network Security Best Practices

Confidentiality, Availability, and Integrity

- Network security consists of protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.
- Recall: Organizations follow the CIA information security triad:
  - **Confidentiality** - Only authorized individuals, entities, or processes can access sensitive information. It may require using cryptographic encryption and access control
  - **Integrity** - Refers to protecting data from unauthorized alteration. It may require the use of cryptographic hashing algorithms.
  - **Availability** - Authorized users must have uninterrupted access to important resources and data. It requires implementing redundant services, gateways, and links.

The Defense-in-Depth Approach

- To ensure secure communications across both public and private networks, all devices must be secured, including routers, switches, servers, and hosts.
- Most organizations employ a defense-in-depth approach to security. It requires a combination of networking devices and services working together.
  - Virtual Private Networks
  - Firewalls
  - Intrusion Prevention Systems
  - Email Security Appliance /Web Security Appliance
  - AAA Server
- All network devices including the router and switches are hardened.
- Data is secured as it travels across various links.

Firewalls

A firewall is a system, or group of systems, that enforces an access control policy between networks.

Performs filtering on network traffic based on packet content

Allow traffic from any external address to the web server.

Allow traffic to FTP server.

Allow traffic to SMTP server.

Allow traffic to internal IMAP server.

Deny all inbound traffic with network addresses matching internal-registered IP addresses.

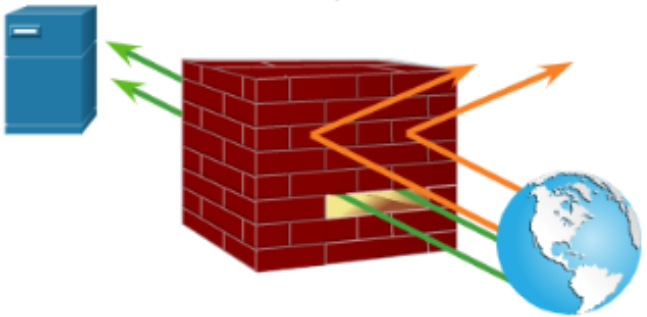
Deny all inbound traffic to server from external addresses.

Deny all inbound ICMP echo request traffic.

Deny all inbound MS Active Directory queries.

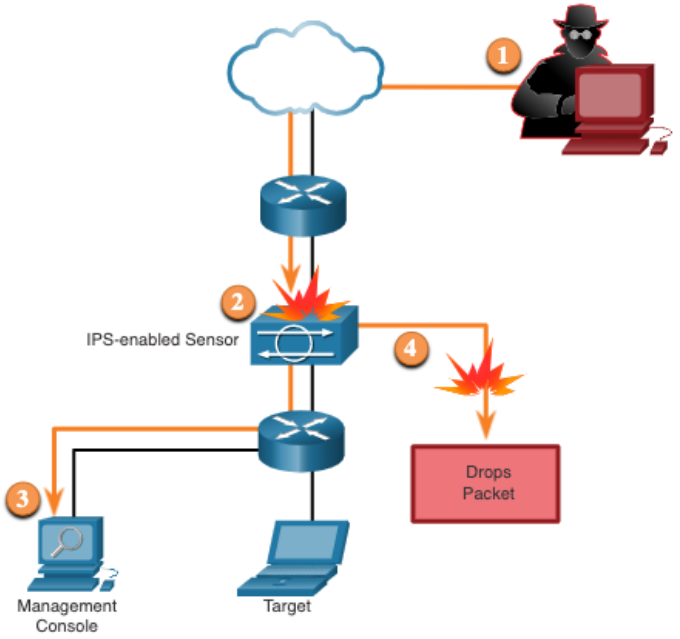
Deny all inbound traffic to MS SQL server queries.

Deny all MS Domain Local Broadcasts.



Intrusion Prevention Systems

- To defend against fast-moving and evolving attacks, IDS/IPS detect them using.
  - Signature matching - match traffic against rules used to detect malicious activity
  - Anomaly detection – measure how much a type of network traffic differs from what is normal
- IDS / IPS technologies are deployed as sensors to monitor network traffic and take the form of several different devices:
  - A router configured with IPS software
  - A device specifically designed to provide dedicated IDS or IPS services
  - A network module installed in an adaptive security appliance (ASA), switch, or router
  - IDS/IPS software installed on network hosts



Content Security Devices

Content security devices monitor threats and issues that are specific to a particular Internet application such as email or web

- **Email Security Appliances (ESA)** are designed to monitor and protect the Simple Mail Transfer Protocol (SMTP).
  - Block known email threats such as malware and suspicious file attachments
  - Discard emails with bad links
  - Block access to newly infected sites.
  - Encrypt content in outgoing email to prevent data loss.
- **Web Security Appliances (WSA)** are designed to address the challenges of securing and controlling web traffic.
  - Categorization, blacklisting and filtering of URLs
  - Malware scanning
  - Web application filtering according to organization policy
  - Encryption and decryption of web traffic

3.5 Cryptography

Securing Communications

- Organizations must provide support to secure the data as it travels across links. This may include internal traffic, but it is even more important to protect the data that travels outside of the organization.
- These are the four elements of secure communications:

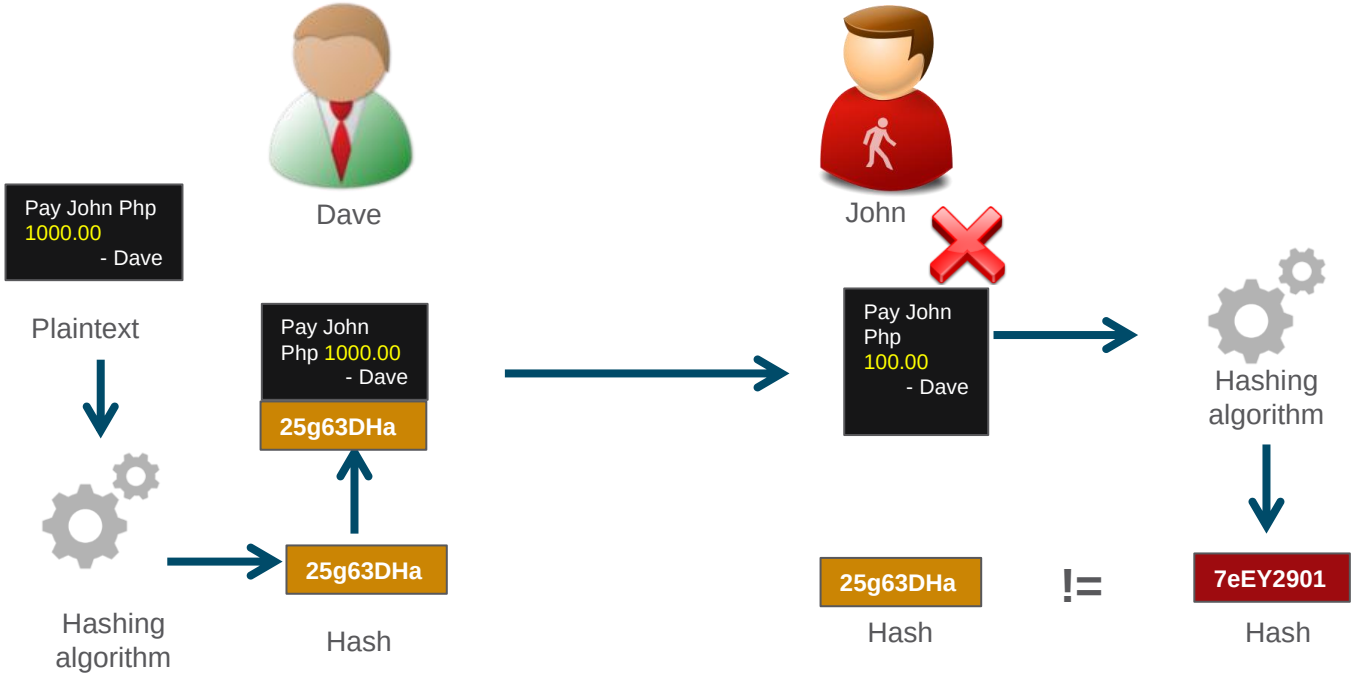
Confidentiality	• Guarantees that messages, if intercepted, cannot be deciphered
Integrity	• Guarantees that messages are accurate, complete, and not altered in transit
Authenticity	• Guarantees that the messages are not a forgery and actually come from whom it states.
Non-repudiation	• Guarantees that the sender cannot refute, the validity of a message sent

Intro to Cryptography

- The practice and the study of techniques for secure communication in the presence of third parties
- Authentication, integrity, and confidentiality are components of cryptography.
- Actions
  - Encryption : act of turning plaintext into ciphertext
  - Decryption : act of turning ciphertext into plaintext
- Encryption methods use specific algorithms (ciphers) to encrypt / decrypt messages
- The key serves as the link between the plaintext and the ciphertext

Data Integrity

- Hash functions can verify that data is not changed accidentally, such as by a communication error.

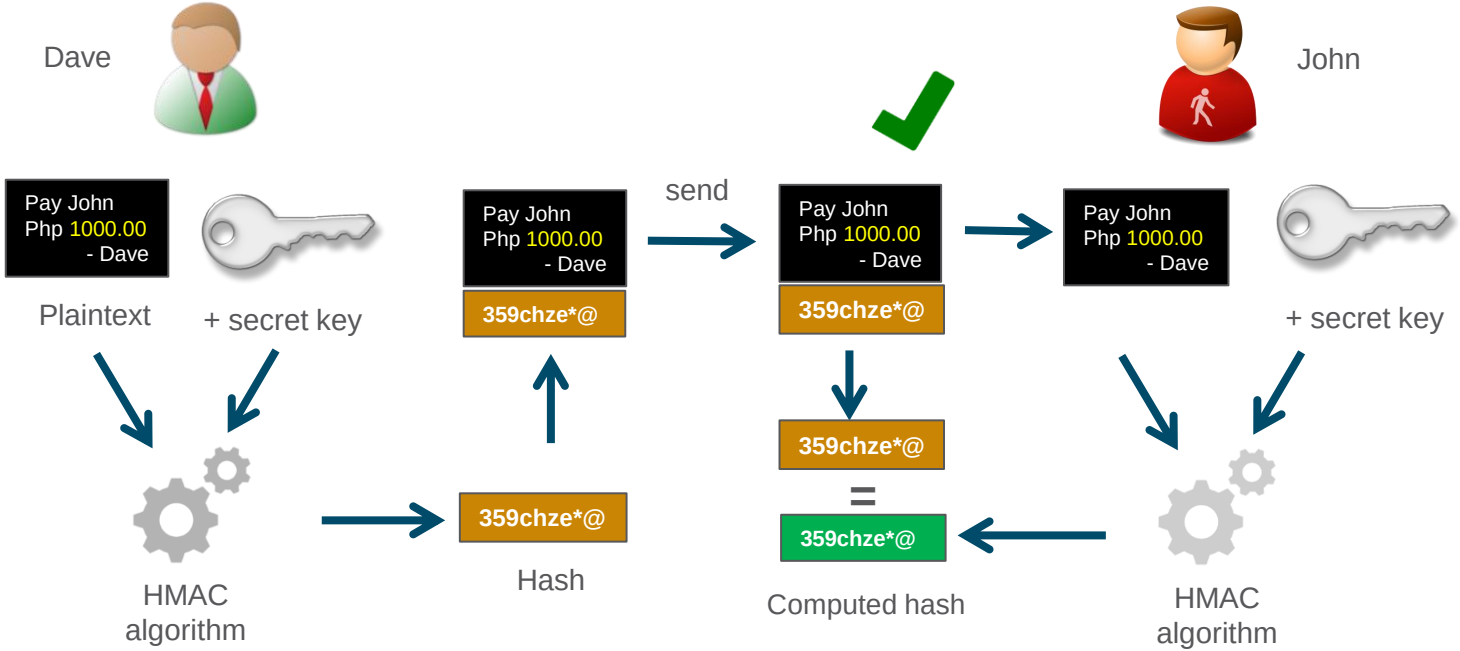


Hash Functions

- Well-known hash functions:
  - **MD5 with 128-bit Digest:** MD5 is a one-way function that produces a 128-bit hashed message. MD5 is a legacy algorithm that should only be used when no better alternatives are available. Use SHA-2 instead.
  - **SHA Hashing Algorithm:** SHA-1 is very similar to the MD5 hash functions. SHA-1 creates a 160-bit hashed message and is slightly slower than MD5. SHA-1 has known flaws and is a legacy algorithm. Use SHA-2 when possible.
  - **SHA-2:** This includes SHA-224 (224 bit), SHA-256 (256 bit), SHA-384 (384 bit), and SHA-512 (512 bit). SHA-256, SHA-384, and SHA-512 are next-generation algorithms and should be used whenever possible.
- Hash functions are limited in guarding against deliberate changes.
  - No unique identifying information from the sender in the hashing procedure
  - A message can be made to look legitimate as long as the correct hash function used is known
  - Vulnerable to man-in-the-middle attacks.

Origin Authentication

- Keyed-hash message authentication code (HMAC). is a message authentication code that is calculated using a hash function and a secret key to add authentication and non-repudiation to integrity assurance.



Data Confidentiality

- There are two classes of encryption used to provide data confidentiality. These two classes differ in how they use keys.

Symmetric Key Encryption

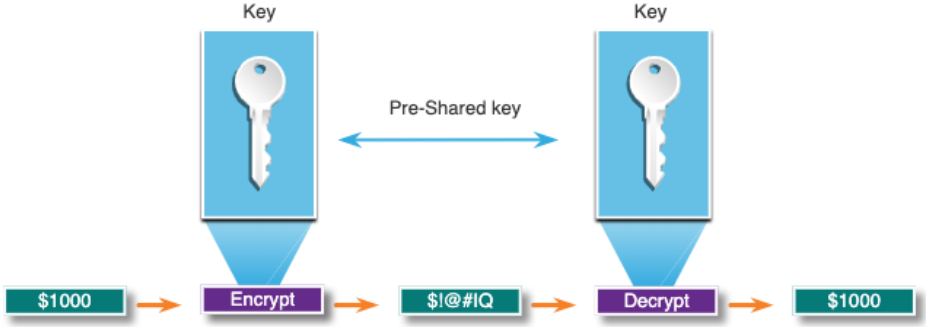
- A.K.A. shared-secret key algorithms.
- A sender and receiver must pre-share a secret key before encrypted communication begins.
- Usually fast (wire speed) because algorithms are based on simple mathematical operations.
- Key length affects the speed and strength of encryption (Shorter keys = faster execution, easier to break)

Asymmetric Key Encryption

- A.K.A public key encryption
- A pair of keys is generated where data encrypted by 1 key needs the paired key for decryption
  - Public Key - May be given freely to anyone
  - Private Key -Kept confidential by the key owner
- Slower in performance due to complex math operations but generally considered more secure than shared key encryption

Cryptography

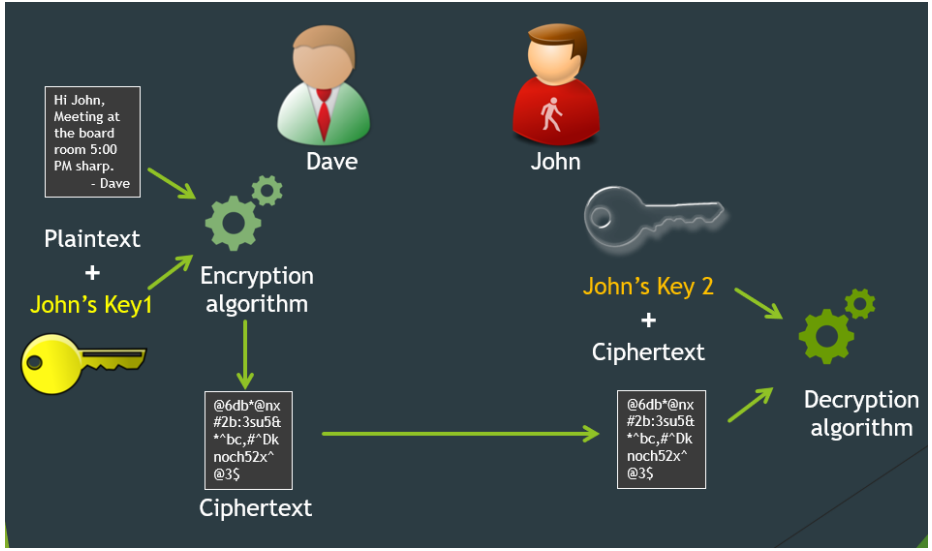
Symmetric Encryption



Algorithms	Description
Data Encryption Algorithm (DES)	A legacy symmetric encryption algorithm. It can be used in stream cipher mode but usually operates in block mode by encrypting data in 64-bit block size.
3DES (Triple DES)	This is a newer version of DES that repeats the DES algorithm process three times. It is considered very trustworthy when implemented using very short key lifetimes.
Advanced Encryption Standard (AES)	AES is a popular and recommended symmetric encryption algorithm. It offers a variable key length of 128-, 192-, or 256-bit key to encrypt 128, 192, or 256 bit data blocks .
Software-Optimized Encryption Algorithm (SEAL)	Faster alternative to DES, 3DES, and AES. It uses a 160-bit encryption key and has a lower impact on the CPU compared to other software-based algorithms.
Rivest ciphers (RC) series algorithms	This algorithm was developed by Ron Rivest. RC4 is the most prevalent version in use. RC4 is a stream cipher and is used to secure web traffic in SSL and TLS.

Asymmetric Encryption

- Asymmetric algorithms are typically used in low-volume cryptographic mechanisms, such as digital signatures and key exchange.
- Examples of protocols that use asymmetric key algorithms:
  - **Internet Key Exchange (IKE) -** This is a fundamental component of IPsec VPNs.
  - **Secure Socket Layer (SSL) -** This is now implemented as Transport Layer Security (TLS).
  - **Secure Shell (SSH) -** This protocol provides a secure remote access connection to network devices.
  - **Pretty Good Privacy (PGP) -** This computer program provides cryptographic privacy and authentication. It is often used to increase the security of email communications.



Asymmetric Encryption (con't)

Asymmetric Encryption Algorithm	Key Length	Description
Diffie-Hellman (DH)	512, 1024, 2048, 3072, 4096	The Diffie-Hellman algorithm allows two parties to agree on a key that they can use to encrypt messages they want to send to each other. The security of this algorithm depends on the assumption that it is easy to raise a number to a certain power, but difficult to compute which power was used given the number and the outcome.
Digital Signature Standard (DSS) and Digital Signature Algorithm (DSA)	512 - 1024	DSS specifies DSA as the algorithm for digital signatures. DSA is a public key algorithm based on the ElGamal signature scheme. Signature creation speed is similar to RSA but is 10 to 40 times slower for verification.
Rivest, Shamir, and Adleman encryption algorithms (RSA)	512 to 2048	RSA is for public-key cryptography that is based on the current difficulty of factoring very large numbers. It is the first algorithm known to be suitable for signing as well as encryption. It is widely used in electronic commerce protocols and is believed to be secure given sufficiently long keys and the use of up-to-date implementations.
ElGamal	512 - 1024	An asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie-Hellman key agreement. A disadvantage of the ElGamal system is that the encrypted message becomes very big, about twice the size of the original message and for this reason it is only used for small messages such as secret keys.
Elliptical curve techniques	160	Elliptic curve cryptography can be used to adapt many cryptographic algorithms, such as Diffie-Hellman or ElGamal. The main advantage of elliptic curve cryptography is that the keys can be much smaller.

Module Summary

What did you learn in this module?

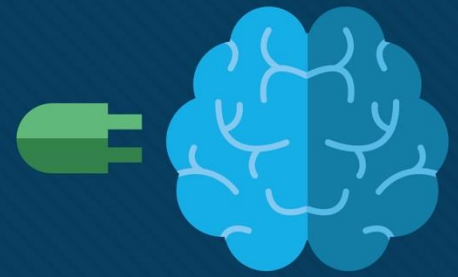
- Network security breaches can disrupt e-commerce, cause the loss of business data, threaten people's privacy, and compromise the integrity of information.
  - An attack vector is a path by which a threat actor can gain access to a server, host, or network. Attack vectors originate from inside or outside the corporate network.
  - The term 'threat actor' includes hackers and any device, person, group, or nation state that is, intentionally or unintentionally, the source of an attack.
  - Attack tools have become more sophisticated and highly automated. These new tools require less technical knowledge to implement.
- The three most common types of malware are worms, viruses, and Trojan horses.
- Social engineering attacks used human-based approaches to compromise security
- Networks are susceptible to the following types of attacks: reconnaissance, access, and DoS.
  - Reconnaissance – information gathering on a target (ping sweeps, port scans, vulnerability scans)
  - Access attacks – breaking into a system (password attacks, spoofing, trust exploitation, man in the middle)
  - DoS – rendering a system unusable to legitimate users (flooding and malformed data)

What Did I Learn In This Module?

- Network attacks target vulnerabilities in the TCP/IP protocol stack and network services
  - IP attacks include: address spoofing, ICMP-based reconnaissance, amplification and reflection type DoS
  - TCP attacks include: TCP SYN Flood attack, TCP reset attack, and TCP Session hijacking.
  - UDP attacks include: UDP Flood DoS
  - ARP attacks include: ARP poisoning and MITM using gratuitous ARP
  - DNS attacks include: open resolver attacks, stealth attacks, domain shadowing attacks, and tunneling attacks.
  - DHCP attacks include: DHCP spoofing and DHCP starvation
- Most organizations follow the CIA information security triad: confidentiality, integrity, and availability.
- To ensure secure communications across both public and private networks, you employ the defense-in-depth approach
  - A firewall is a system, or group of systems, that enforces an access control policy between networks.
  - IDS/IPS detect and guard against fast-moving network attacks
  - Content security devices monitor threats and issues that are specific to a particular Internet application

What Did I Learn In This Module?

- The four elements of secure communications are data integrity, origin authentication, data confidentiality, and data non-repudiation and are addresses using cryptographic approaches.
  - Hash functions guarantee that message data has not changed accidentally or intentionally.
  - Keyed-hash message authentication code (HMAC) adds authentication to integrity assurance, by combining a cryptographic hash function with a secret key.
  - Symmetric encryption algorithms use an identical pre-shared key between 2 parties to encrypt messages for confidentiality and are suited for bulk data transfers
  - Asymmetric encryption algorithms use a paired private and public key to encrypt messages between 2 parties are suitable for low volume data transfers



Module 3
Advanced Packet Filtering

ITNET04

WAN Connectivity

Module Objectives

Module Title: Advanced Packet Filtering

Module Objectives:

- Review the concepts of packet filtering and principles of access control list formulation
- Implement extended access control lists to control traffic flow in a network
- Perform troubleshooting for extended ACLs

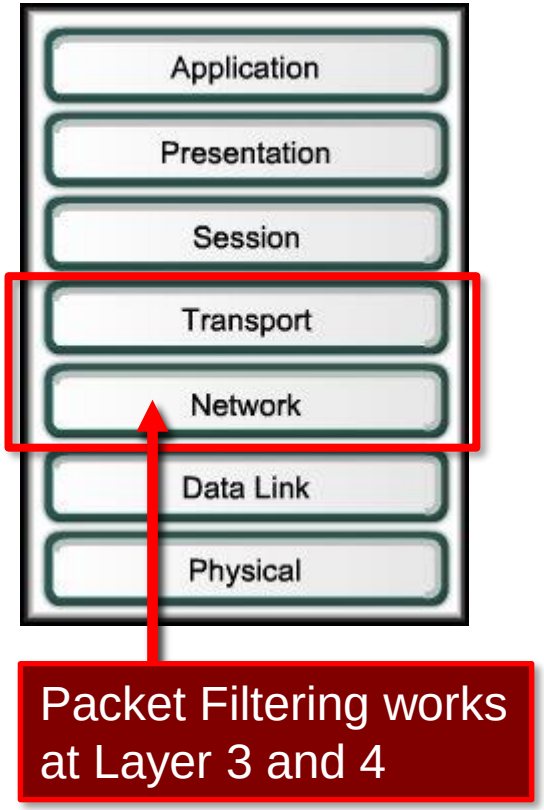
Module References:

- CCNAv7 ENSA– Module 4, 5.4 - 5.5

3.1 ACL Operation and Configuration Review

Recall: Packet Filtering

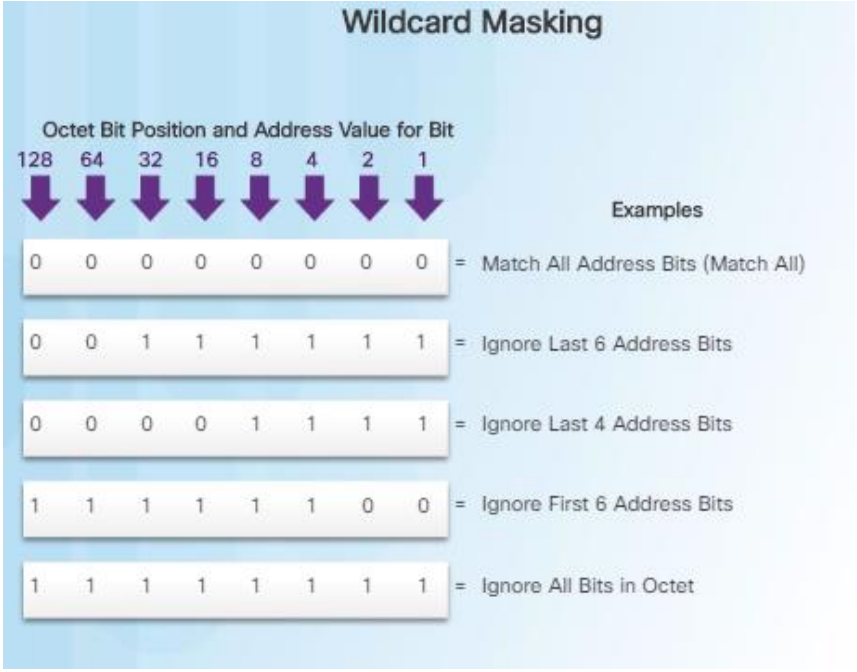
- Packet Filtering is the process of controlling access to a network by analyzing the incoming and outgoing packets and passing or halting them based on certain criteria.
- Used as a method to manage network traffic or enforce network security policies to user groups
- Often performed by a network router or firewall which forwards or drops data packets according to filtering rules
- Can occur at
  - Layer 3: filtering by address
  - Layer 4: filtering by protocol or host connection status



Recall: Access Control Lists

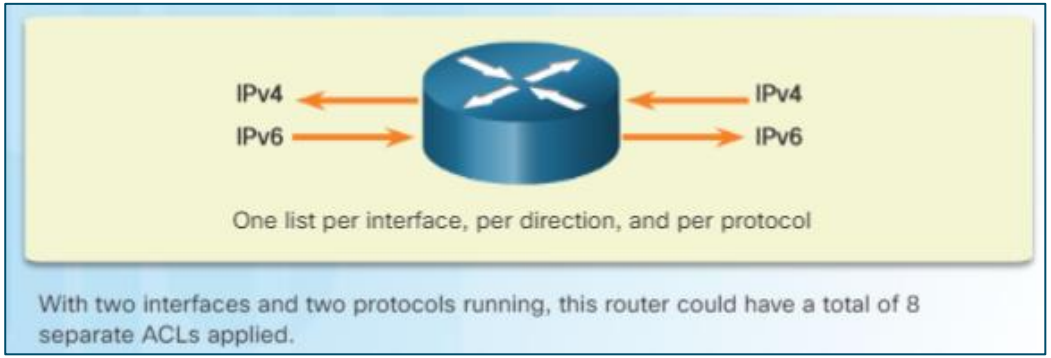
- An Access Control List (ACL) is a sequential list list of **permit** or **deny** statements, known as access control entries which perform packet filtering on a network

- IPv4 ACEs include the use of wildcard masks which are a string of 32 binary digits used by the router to determine which bits of the address to examine for a match.
  - Wildcard mask bit 0 - The corresponding bit value in the IP Address to be tested must match the bit value in the address specified in the ACL.
  - Wildcard mask bit 1 - Ignore the corresponding bit value.



ACL Operation Overview

- You can configure:
  - **One ACL per protocol** - To control traffic flow on an interface, an ACL must be defined for each protocol enabled on the interface.
  - **One ACL per direction** - ACLs control traffic in one direction at a time on an interface. Two separate ACLs must be created to control inbound and outbound traffic.
  - **One ACL per interface** - ACLs control traffic for an interface, for example, GigabitEthernet 0/0.



ACL Operation Overview

- By default, a router does not have any ACLs.
- As each packet comes through an interface with an associated ACL:
  - The ACL is checked from top to bottom one line at a time.
  - Matches the pattern defined in the ACL statement to the specified area of the incoming packet.
  - Stops checking when it finds a matching statement then takes the defined action (permit or deny).
  - If no match is present, the default is to deny the packet.
- An ACL does not filter traffic originating from the router where it is applied.

Similar to your chained if-else code…

```
If (pattern 1)
{    permit / deny;
}
Else if (pattern 2)
{    permit / deny;
}
Else if (pattern 3)
{    permit / deny;
}
…
Else deny;
```

ACL Operation Overview

- A packet is tested against ACLs that it encounters as it flows through router interfaces
- When a packet arrives at a router interface:
  - The router checks to see whether the destination Layer 2 address matches its interface Layer 2 address.
  - If the frame is accepted, the router checks for an ACL on the inbound interface.
  - If an ACL exists, the packet is tested against the ACEs and the packet is either permitted or denied.
  - If the packet is permitted, it is then checked against routing table to determine the destination interface.
  - If a routing table entry exists for the destination, the packet is then switched to the outgoing interface.
- Next, the router checks whether the outgoing interface has an ACL.
  - If an ACL exists, the packet is tested against the ACEs.
  - If the packet matches an ACE, it is either permitted or denied.
  - If there is no ACL or the packet is permitted, the packet is encapsulated in the new Layer 2 protocol and forwarded out the interface to the next device.

Types of IPv4 ACLs

	Numbered ACL	Named ACL
Standard ACL	Numbered standard	Named standard
Extended ACL	Numbered extended	Named extended

On Cisco routers, there are two types of IPv4 ACLs based on granularity of criteria:

- **Standard ACLs** - These permit or deny packets based only on the source IPv4 address.
- **Extended ACLs** - These permit or deny packets based on the source and destination IPv4 address, protocol type, source and destination TCP or UDP ports and more.

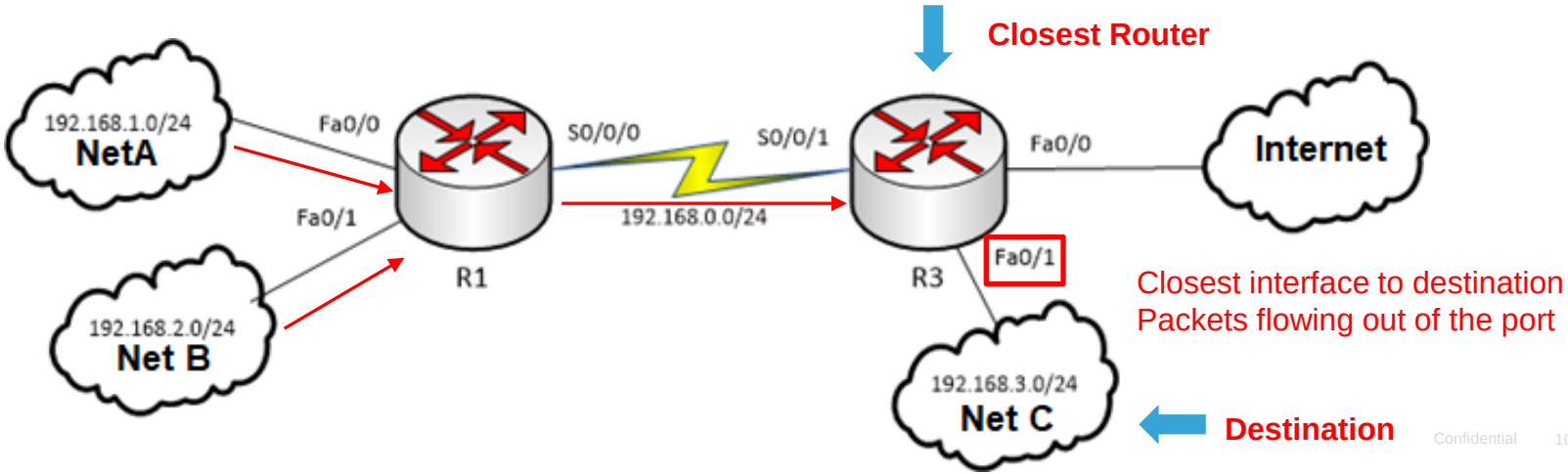
For each, there are two further types of ACLs based on identification method:

- **Numbered ACLs** - These ACLs are identified using a numerical ID 1 - 99, 1300 – 1999).
- **Named ACLs** - These ACLs are identified using a user-defined name and can be easily edited.

Standard ACL Usage

- Standard ACLs should be located as close to the destination as possible.
- **Example:** "Only Network A and the host 192.168.2.2 are allowed to access Network C."

```
R3(config)# access-list 1 permit 192.168.1.0 0.0.0.255
R3(config)# access-list 1 permit host 192.168.2.2
R3(config)# access-list 1 deny any
R3(config)# interface Fa0/1
R3(config-if)# ip access-group 1 out
```



3.2 Extended IPv4 ACLs

Structure of an Extended IPv4 ACLs

- Extended IPv4 ACLs provide more precise filtering and are used more often than standard ACLs because they provide a greater degree of control.
- Can create filter criteria specifying
  - Source source and destination IP Address
  - Protocol type
  - Source and destination TCP or UDP ports
  - ICMP message types

- Extended ACLs are numbered 100 to 199 and 2000 to 2699, providing a total of 799 possible extended numbered ACLs.
- Extended ACLs can also be named.
- Extended ACLs are applied to interfaces in the same manner as standard ACLs, except that they are placed as close as possible to the traffic source

Configure Extended IPv4 ACLs

- The full syntax of the extended ACL command is as follows:

```
access-list ACL-# {deny | permit | remark} protocol {source source-
wildcard][operator [port-number | port-name]] {destination destination-
wildcard][operator [port-number | port-name]]
```

  - General traffic can be filtered by source and destination IP address

```
access-list 114 permit ip 192.168.10.0 0.0.0.255 any
```

Configure Extended IPv4 ACLs

- The full syntax of the extended ACL command is as follows:
  - **access-list** *ACL-#* {**deny** | **permit** | **remark**} *protocol* {*source source-wildcard*][*operator* [*port-number* | *port-name*]] {*destination destination-wildcard*][*operator* [*port-number* | *port-name*]]

- ICMP traffic can be filtered based on message type by specifying:
  - The message number

```
access-list 114 permit icmp 192.168.10.0 0.0.0.255 any 8
access-list 114 permit icmp 192.168.10.0 0.0.0.255 any 0
```

  - Or the message name

```
access-list 114 permit icmp 192.168.10.0 0.0.0.255 echo
access-list 114 permit icmp 192.168.10.0 0.0.0.255 echo-reply
```

Configure Extended IPv4 ACLs

- The full syntax of the extended ACL command is as follows:
  - **access-list** *ACL-#* {**deny** | **permit** | **remark**} *protocol* {*source source-wildcard*][*operator* [*port-number* | *port-name*]] {*destination destination-wildcard*][*operator* [*port-number* | *port-name*]]

- A target TCP or UDP application can be specified by configuring either:
  - The port number

```
access-list 114 permit tcp 192.168.10.0 0.0.0.255 any eq 23
access-list 114 permit tcp 192.168.10.0 0.0.0.255 any eq 21
```

  - Or the protocol name

```
access-list 114 permit tcp 192.168.10.0 0.0.0.255 any eq telnet
access-list 114 permit tcp 192.168.10.0 0.0.0.255 any eq ftp
```

Configure Extended IPv4 ACLs

- Extended ACLs can filter traffic by examining port numbers.
- Common TCP and UDP ports numbers include:

Port Number	Protocol	Application	Acronym
20	TCP	File Transfer Protocol (data)	FTP
21	TCP	File Transfer Protocol (control)	FTP
22	TCP	Secure Shell	SSH
23	TCP	Telnet	–
25	TCP	Simple Mail Transfer Protocol	SMTP
53	UDP, TCP	Domain Name Service	DNS
67	UDP	Dynamic Host Configuration Protocol (server)	DHCP
68	UDP	Dynamic Host Configuration Protocol (client)	DHCP
69	UDP	Trivial File Transfer Protocol	TFTP
80	TCP	Hypertext Transfer Protocol	HTTP
110	TCP	Post Office Protocol version 3	POP3
143	TCP	Internet Message Access Protocol	IMAP
161	UDP	Simple Network Management Protocol	SNMP
443	TCP	Hypertext Transfer Protocol Secure	HTTPS

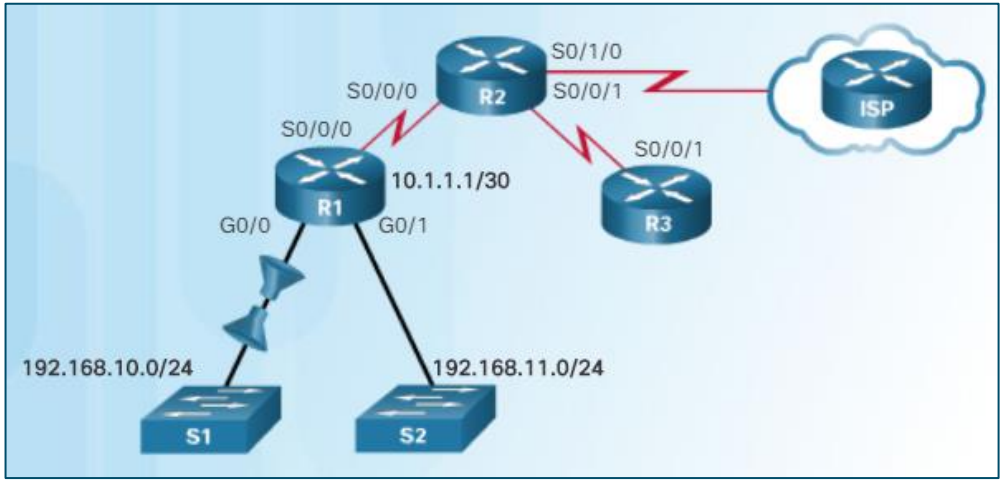
Configure Extended IPv4 ACLs

- Extended ACLs can filter traffic by examining port numbers.
- Operators are used to determine how to evaluate the given port number:

Operator		Example	What it means
eq	Equal to	eq 80	All traffic with port equal to 80
lt, gt	Less than, greater than	lt 80	All traffic with port lower than 80
neq	Not equal to	neq 80	All traffic with port except 80
range	Range of ports	range 20 29	All traffic from port 20 to port 29

Configure Extended IPv4 ACLs

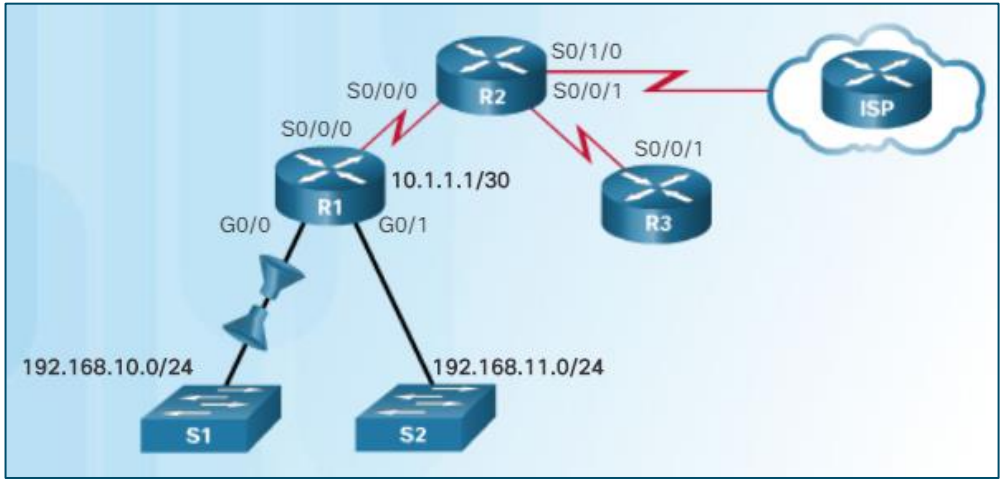
- Practice: Permit only the following traffic from network 192.168.10.0/24:
  - Any traffic to 192.168.11.0/24
  - Outgoing HTTP and DNS traffic from network 192.168.10.0/24 to all other networks



- The full syntax of the extended ACL command is as follows:
  - **access-list** *ACL-#* {**deny** | **permit** | **remark**} *protocol* {*source source-wildcard*][*operator* [*port-number* | *port-name*]] {*destination destination-wildcard*][*operator* [*port-number* | *port-name*]]

Configure Extended IPv4 ACLs

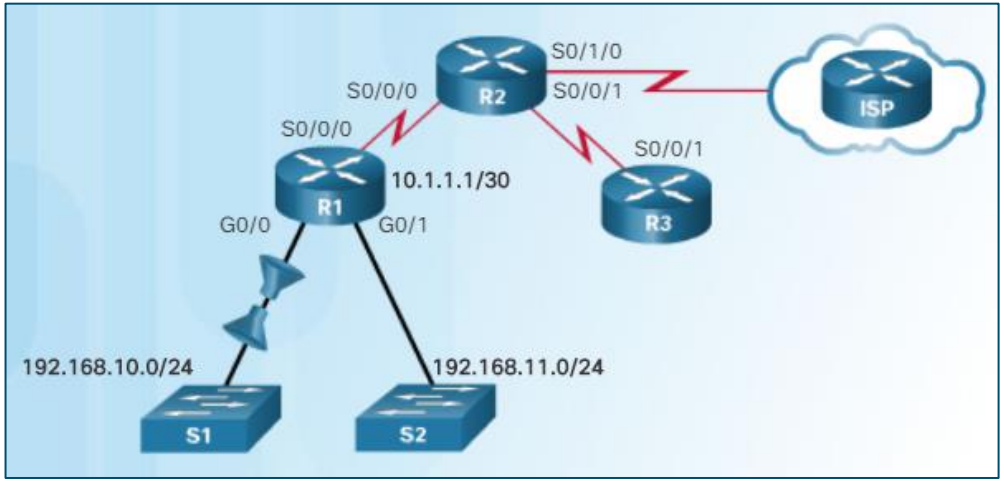
- Practice: Permit only the following traffic from network 192.168.10.0/24:
  - Any traffic to 192.168.11.0/24
  - Outgoing HTTP and DNS traffic from network 192.168.10.0/24 to all other networks




```
R1(config)#access-list 114 permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config)#access-list 114 permit udp 192.168.10.0 0.0.0.255 any eq 53
R1(config)#access-list 114 permit ip 192.168.10.0 0.0.0.255 192.168.11.0 0.0.0.255
R1(config)#access-list 114 deny ip any any
```

Configure Extended IPv4 ACLs

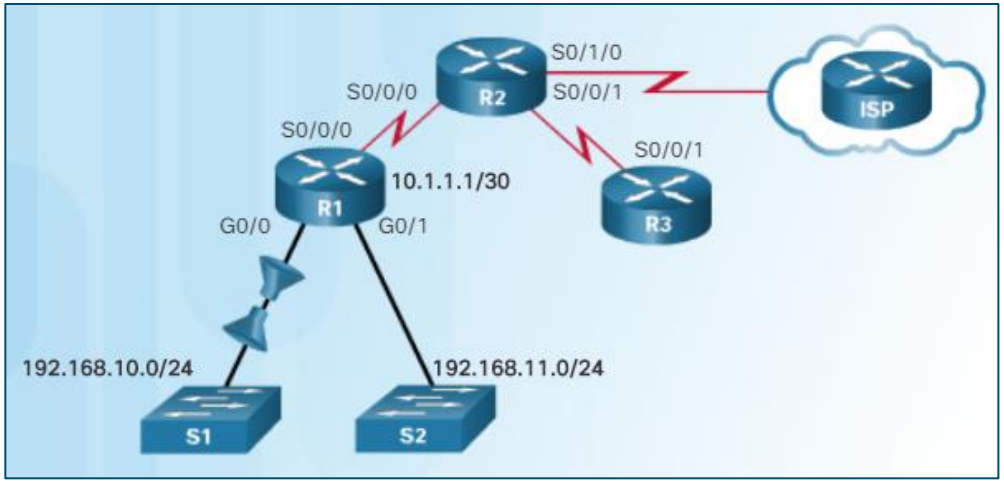
- Practice: Permit only the following traffic from network 192.168.10.0/24:
  - Any traffic to 192.168.11.0/24
  - Outgoing HTTP and DNS traffic from network 192.168.10.0/24 to all other networks
- R1 G0/0 is the interface closest to the traffic source:




```
R1(config)#access-list 114 permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config)#access-list 114 permit udp 192.168.10.0 0.0.0.255 any eq 53
R1(config)#access-list 114 permit ip 192.168.10.0 0.0.0.255 192.168.11.0 0.0.0.255
R1(config)#access-list 114 deny ip any any
R1(config)#interface G0/0
R1(config-if)#ip access-group 114 in
```

Configure Extended IPv4 ACLs

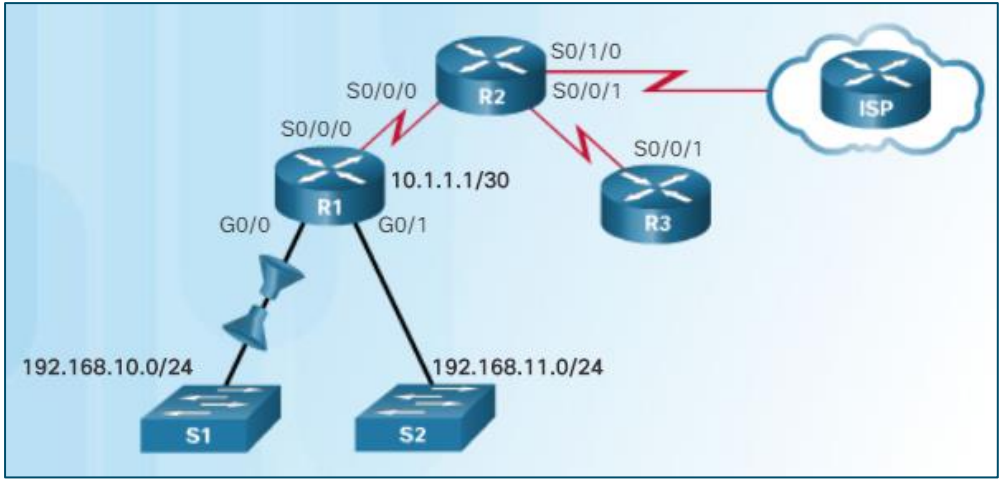
- The 'established' keyword can be added to TCP access control entries to specify that the statement applies only to return traffic by checking for the presence of the TCP ACK flag
- Ex: `access-list 114 permit tcp any any established`
- Practice: Permit only return traffic from the Internet to network 192.168.10.0/24 to enter the network



Configure Extended IPv4 ACLs

- The 'established' keyword can be added to TCP access control entries to specify that the statement applies only to return traffic by checking for the presence of the TCP ACK flag

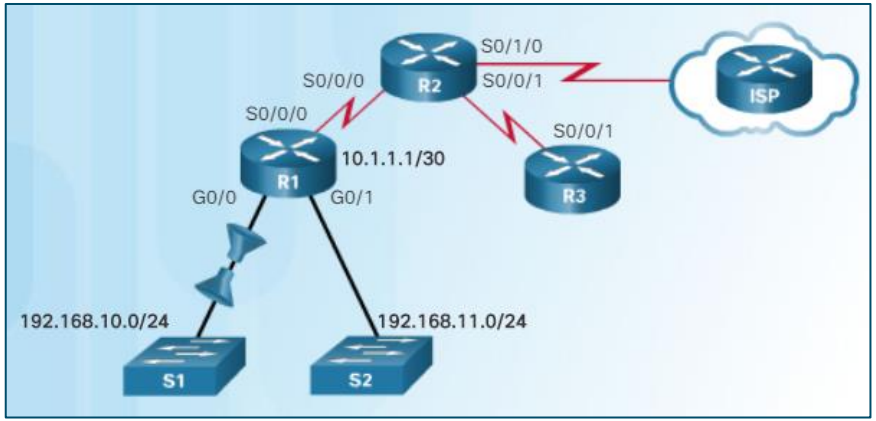
- Practice: Permit only return traffic from the Internet to network 192.168.10.0/24 to enter the network




```
R2(config)#access-list 115 permit tcp any 192.168.10.0 0.0.0.255 established
R2(config)#access-list 115 deny ip any any
R2(config)#interface S0/1/0
R2(config-if)#ip access-group 115 in
```

Configure Extended IPv4 ACLs

- Named extended ACLs are created and edited in the same way as named standard ACLs




```
R1(config)#ip access-list extended SURFING
R1(config-ext-nacl)#permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config-ext-nacl)#permit udp 192.168.10.0 0.0.0.255 any eq 53
R1(config-ext-nacl)#permit ip 192.168.10.0 0.0.0.255 192.168.11.0 0.0.0.255
R1(config-ext-nacl)#deny ip any any
R1(config-ext-nacl)#exit
R1(config)#interface G0/0
R1(config-if)#ip access-group SURFING in
```

Configure Extended IPv4 ACLs

- The **show ip interface** and **show access-lists** commands can be used to verify the content of extended ACLs.
  - The **show access-lists** command outputs all ACLs with their statements and line numbers if applicable

```
R1#show access-lists
Extended IP access list SURFING
  10 permit tcp 192.168.10.0 0.0.0.255 any eq 80
  20 permit udp 192.168.10.0 0.0.0.255 any eq 53
  30 permit ip 192.168.10.0 0.0.0.255 192.168.11.0 0.0.0.255
  40 deny ip any any
R1#
```

  - The **show ip interface** command is used to verify the ACL on the interface and the direction in which it was applied.

```
R1#show ip interface G0/0
FastEthernet0/0 is up, line protocol is up
...
  Outgoing access list is not set
  Inbound  access list is SURFING
R1#
```

3.3 Troubleshoot ACLs

Processing Packets with ACLs

- The most common ACL errors are entering ACEs in the wrong order or not applying adequate criteria to the ACL rules.
- Remember: The Cisco IOS software tests addresses against the ACL ACEs.
  - The first match determines whether the software accepts or rejects the address.
  - Because the software stops testing conditions after the first match, the order of the conditions is critical.
  - If no conditions match, the address is rejected.
- Standard ACLs only examine the source IPv4 address.
  - The destination of the packet and the ports involved are not considered.
- Extended ACLs filter on protocol, source address, destination address, and port numbers.
  - The ACL first filters on the source address, then on the port and protocol of the source.
  - It then filters on the destination address, then on the port and protocol of the destination, and makes a final permit or deny decision.

What to Look For

- ✓Wrong order of statements
- ✓Errors in protocol criteria
- ✓Inverted source and destination criteria
- ✓Incorrect placement of ACL

What to Look For

✓Wrong order of statements

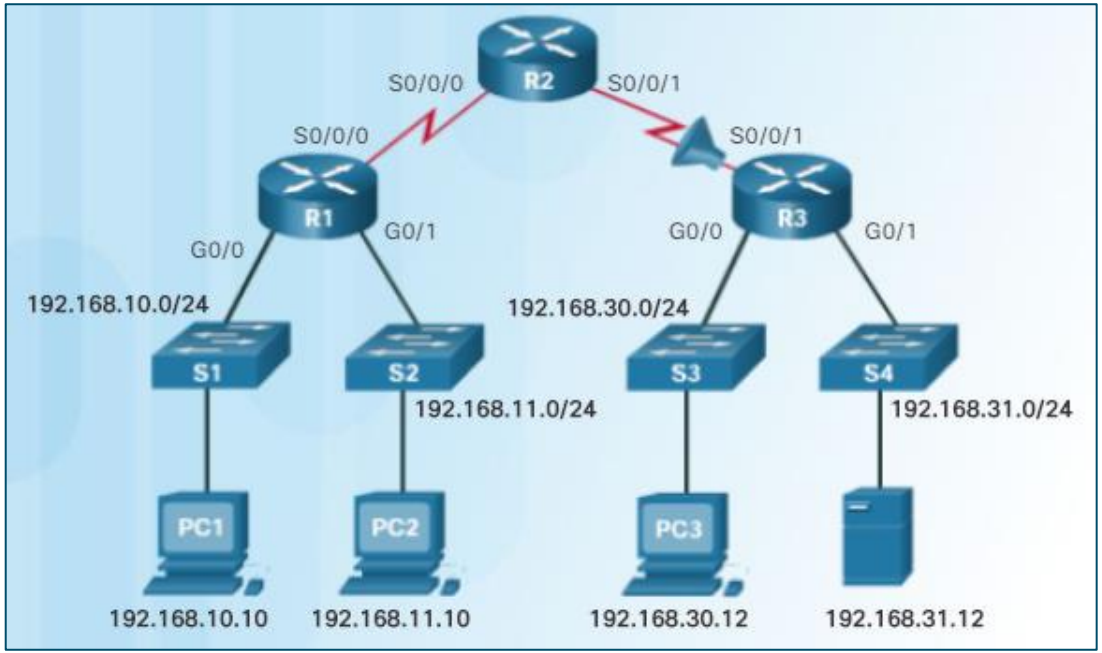
- ACL statements are processed from top to bottom; and checking stops on the first match
- In general, statements should be ordered from most specific to least specific

1. Source and Destination port numbers / ICMP messages
2. Transport protocol (TCP / UDP / ICMP)
3. IP addresses
4. Network protocol (IP, IPv6)

Common ACLs Errors – Spot the Error

- Example 1: Host 192.168.10.10 has no Telnet connectivity with 192.168.30.12.

```
R3# show access-lists
Extended IP access list 110
 10 deny tcp 192.168.10.0 0.0.0.255
             any
 20 permit tcp 192.168.10.0 0.0.0.255
             any eq telnet
 30 permit ip any any
```

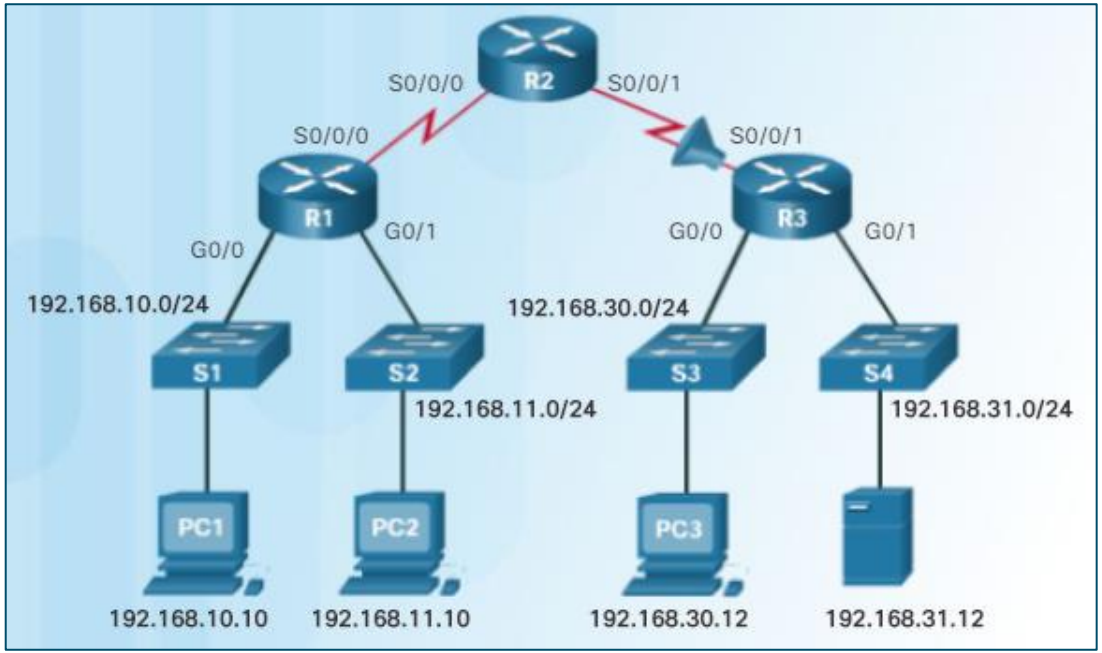


Common ACLs Errors

- Host 192.168.10.10 has no Telnet connectivity with 192.168.30.12.

```
R3# show access-lists
Extended IP access list 110
 10 deny tcp 192.168.10.0 0.0.0.255
             any
 20 permit tcp 192.168.10.0 0.0.0.255
             any eq telnet
 30 permit ip any any
```

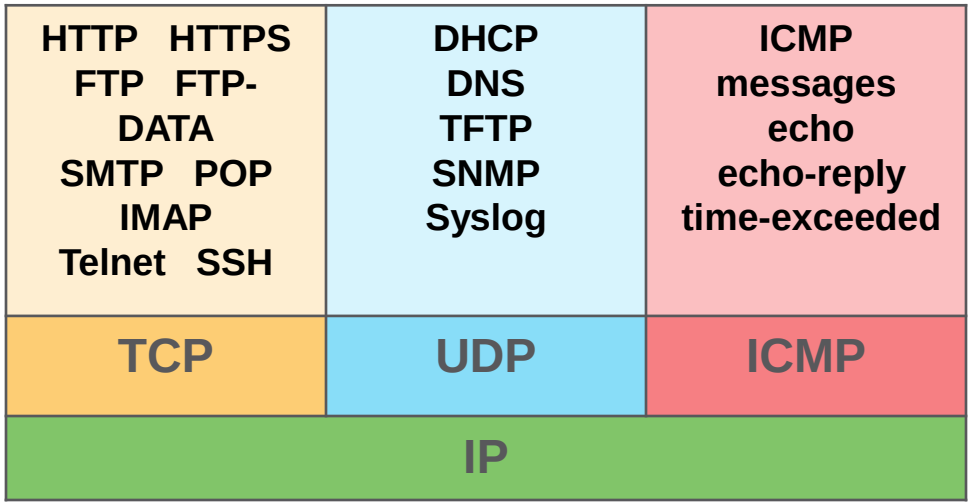
- **Solution:**
  - Statement 10 denies host 192.168.10.10, therefore statement 20 can never be matched.
  - Statements 10 and 20 should be reversed.



What to Look For

✓Error in protocol criteria

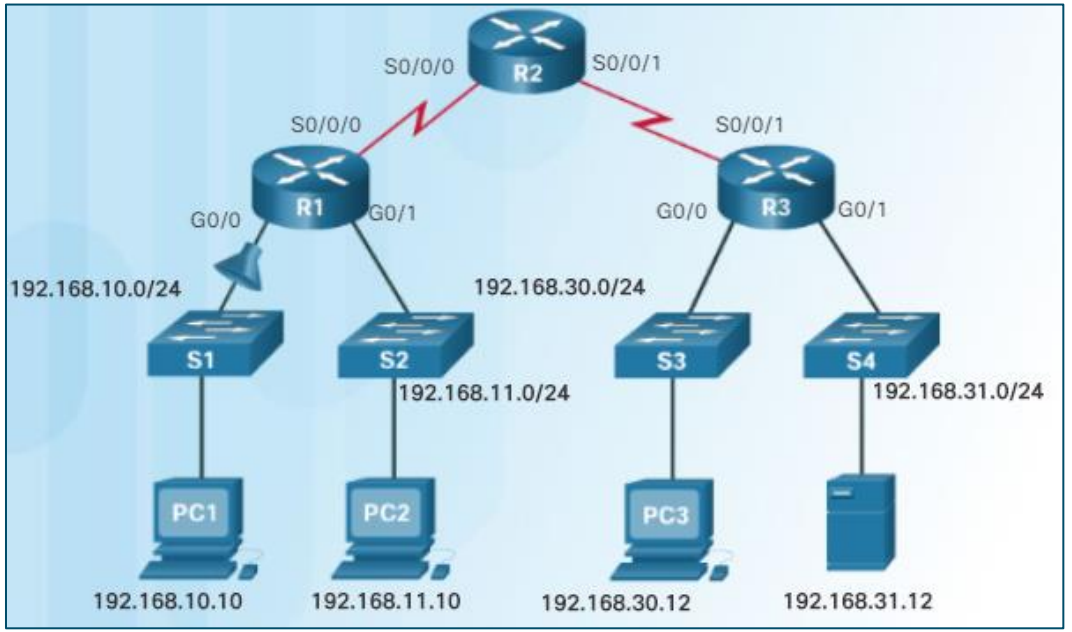
- Be familiar with protocol layers based on the TCP/IP stack
- Blocking / Permitting a lower layer protocol affects all higher layer protocols that depend on it



Common ACLs Errors – Spot the Error

- Example 2: 192.168.10.0/24 network cannot use TFTP to connect to the 192.168.30.0/24 network.

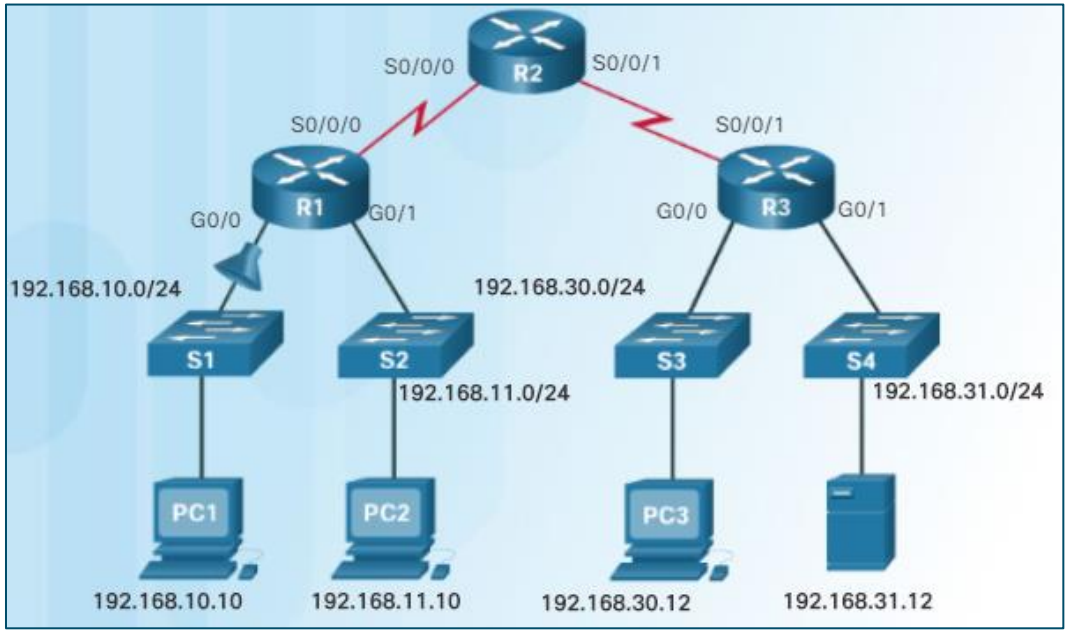
```
R1# show access-lists
Extended IP access list 120
 10 deny tcp 192.168.10.0 0.0.0.255
             any eq telnet
 20 deny tcp 192.168.10.0 0.0.0.255
             host 192.168.31.12 eq
             smtp
 30 permit tcp any any
```



Common ACLs Errors

- Example 2: 192.168.10.0/24 network cannot use TFTP to connect to the 192.168.30.0/24 network.

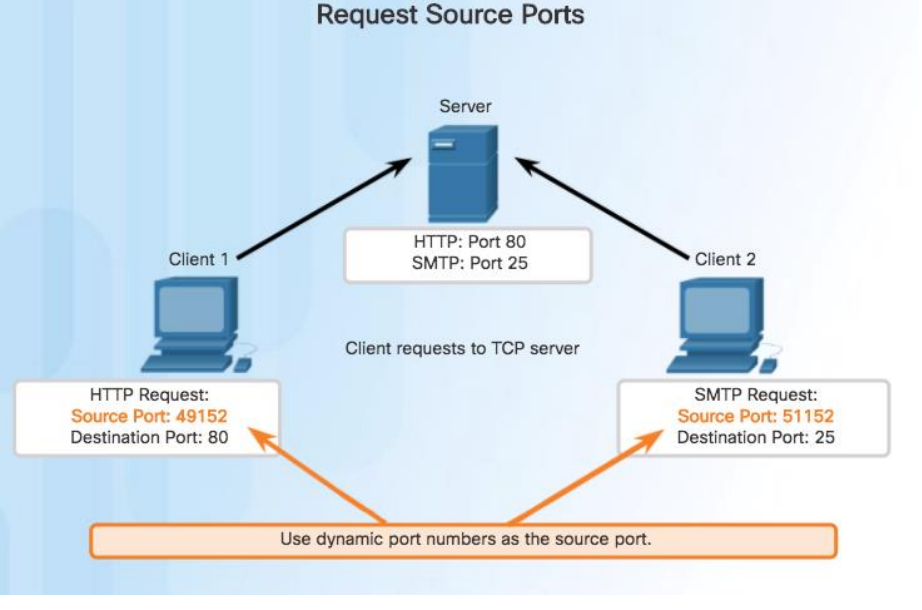
```
R1# show access-lists
Extended IP access list 120
 10 deny tcp 192.168.10.0 0.0.0.255
             any eq telnet
 20 deny tcp 192.168.10.0 0.0.0.255
             host 192.168.31.12 eq
             smtp
 30 permit tcp any any
```

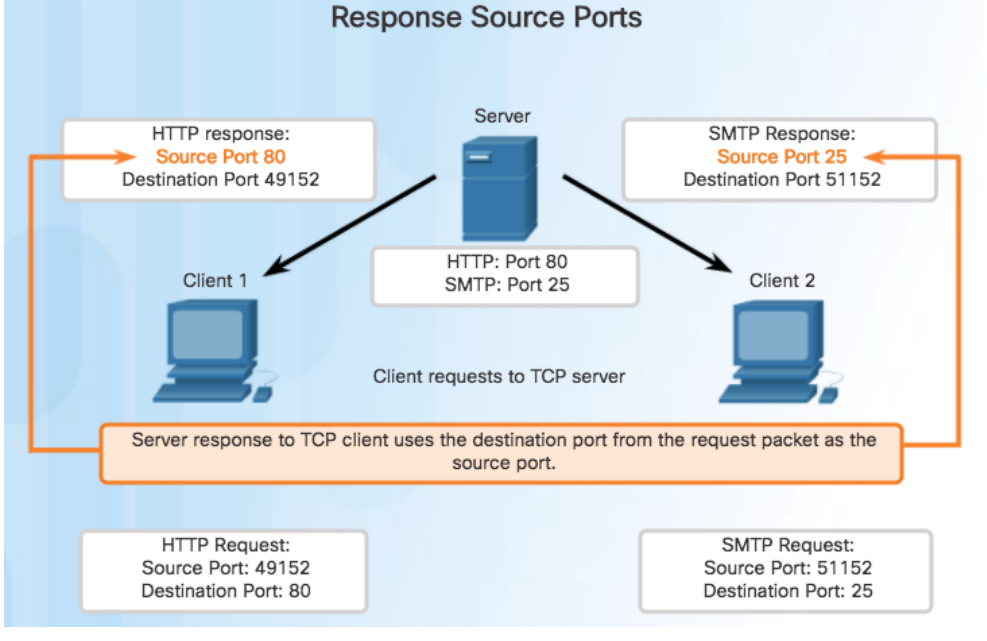


- **Solution:**
  - Statement 30 allows all TCP traffic. However, TFTP uses UDP instead of TCP and is implicitly denied.
  - Statement 30 should be **permit ip any any**.

What to Look For

- ✓ Inverted source and destination criteria
  - ACL Syntax Source_address <source_port> Dest_address <dest_port>
  - For most applications, client initiates the connection using a random port to a known port on the server

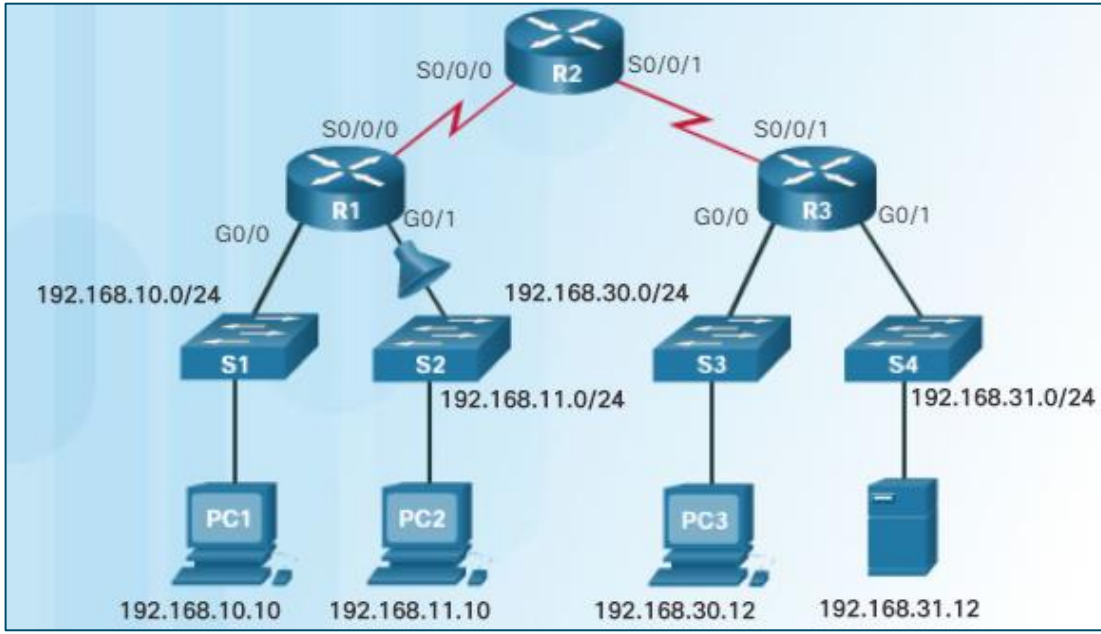




Common ACLs Errors – Spot the Error

- Example 3: The 192.168.11.0/24 network can use Telnet to connect to 192.168.30.0/24, but this connection should not be allowed.

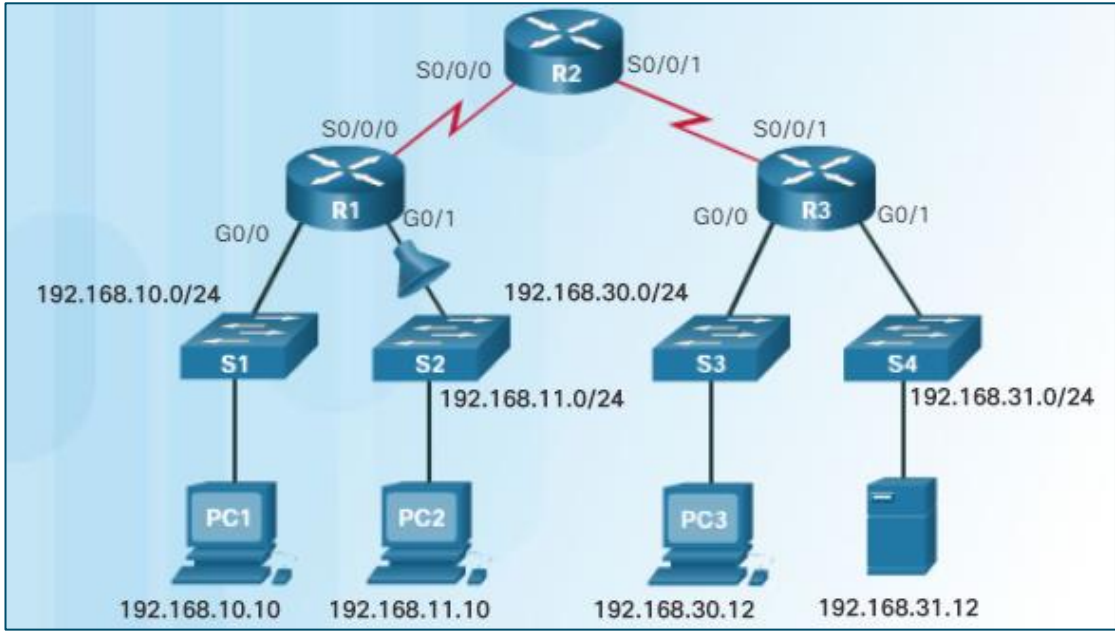
```
R1# show access-lists
Extended IP access list 130
 10 deny any eq telnet any
 20 deny tcp 192.168.11.0 0.0.0.255
             host 192.168.31.12 eq
             smtp
 30 permit tcp any any
```



Common ACLs Errors

- Example 3: The 192.168.11.0/24 network can use Telnet to connect to 192.168.30.0/24, but this connection should not be allowed.

```
R1# show access-lists
Extended IP access list 130
 10 deny any eq telnet any
 20 deny tcp 192.168.11.0 0.0.0.255
             host 192.168.31.12 eq
             smtp
 30 permit tcp any any
```



- **Solution:**
  - The Telnet port number in statement 10 of ACL 130 is listed in the wrong order as it currently denies any source packet with a port number equal to Telnet.
  - Configure **10 deny tcp 192.168.11.0 0.0.0.255 192.168.30.0 0.0.0.255 eq telnet**.

What to Look For

✓Wrong placement of ACL

- Make sure that the ACL is configured on the correct router, interface and direction
- As a general rule of thumb:
  - For standard ACL – as close as possible to the destination

    Last router in the path

    Outbound on the interface connected to the destination network
  - For IPv4 extended ACL – as close as possible to the source

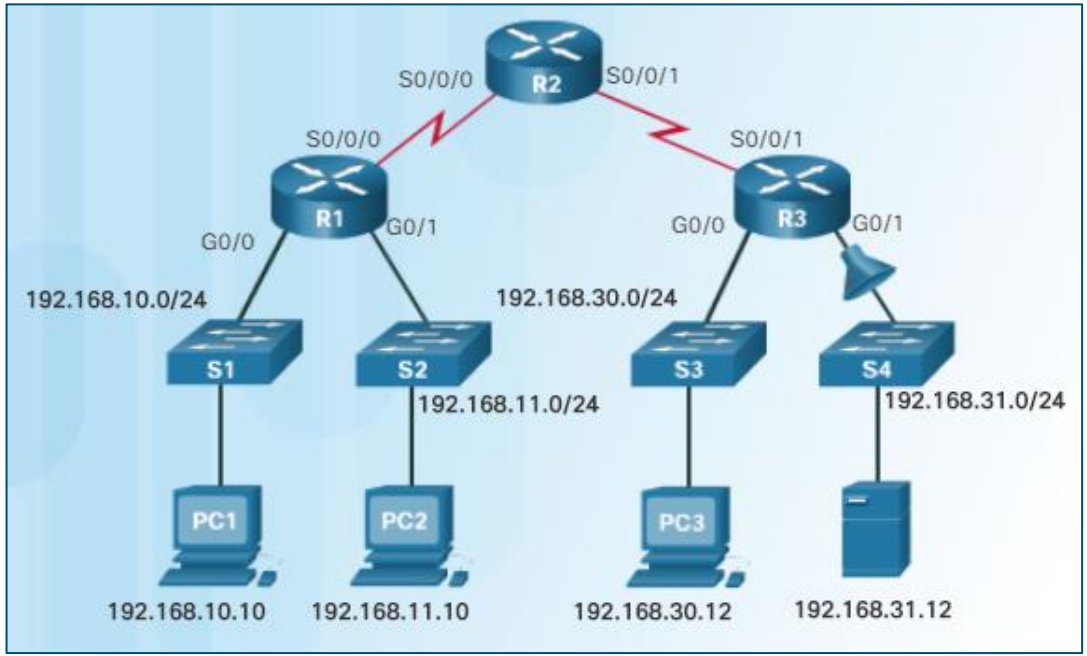
    First router in the path

    Inbound on the interface connected to the source network

Common ACLs Errors – Spot the Error

- Example 4: Host 192.168.30.12 can use Telnet to connect to 192.168.31.12, but this connection should not be allowed.

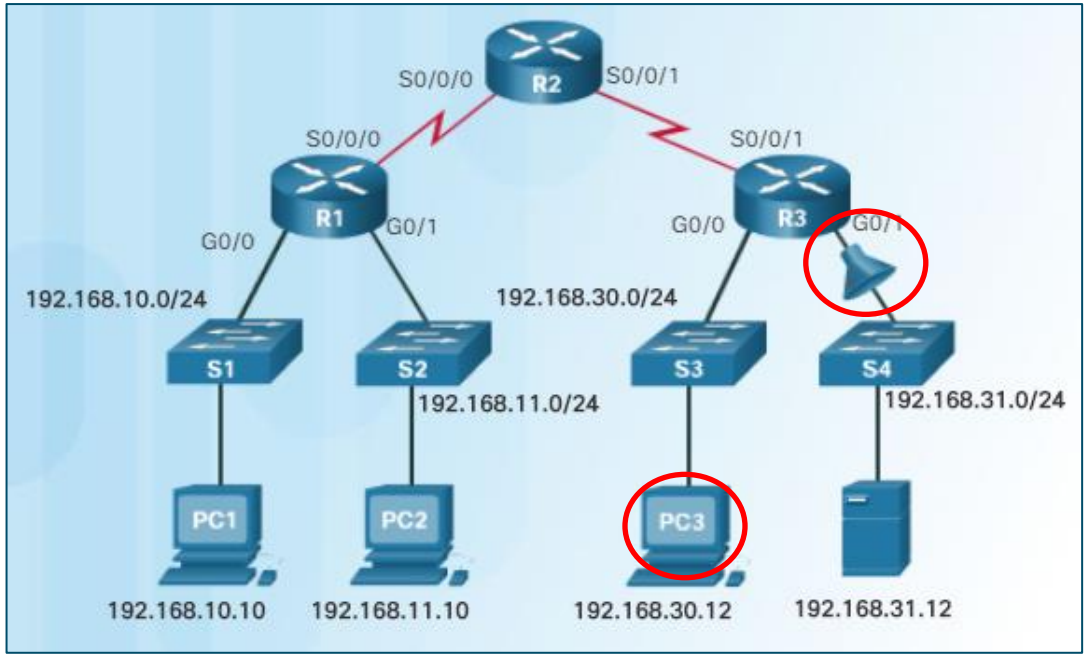
```
R1# show access-lists
Extended IP access list 150
 10 deny tcp any host 192.168.31.12
             eq telnet
 20 permit ip any any
R1#show ip interface G0/1
GigabitEthernet0/1 is up, line
protocol is up
...
  Outgoing access list is not set
  Inbound  access list is 150
```



Common ACLs Errors

- Example 4: Host 192.168.30.12 can use Telnet to connect to 192.168.31.12, but this connection should not be allowed.

```
R1# show access-lists
Extended IP access list 150
 10 deny tcp any host 192.168.31.12
              eq telnet
 20 permit ip any any
R1#show ip interface G0/1
GigabitEthernet0/1 is up, line
protocol is up
...
  Outgoing access list is not set
  Inbound  access list is 150
```



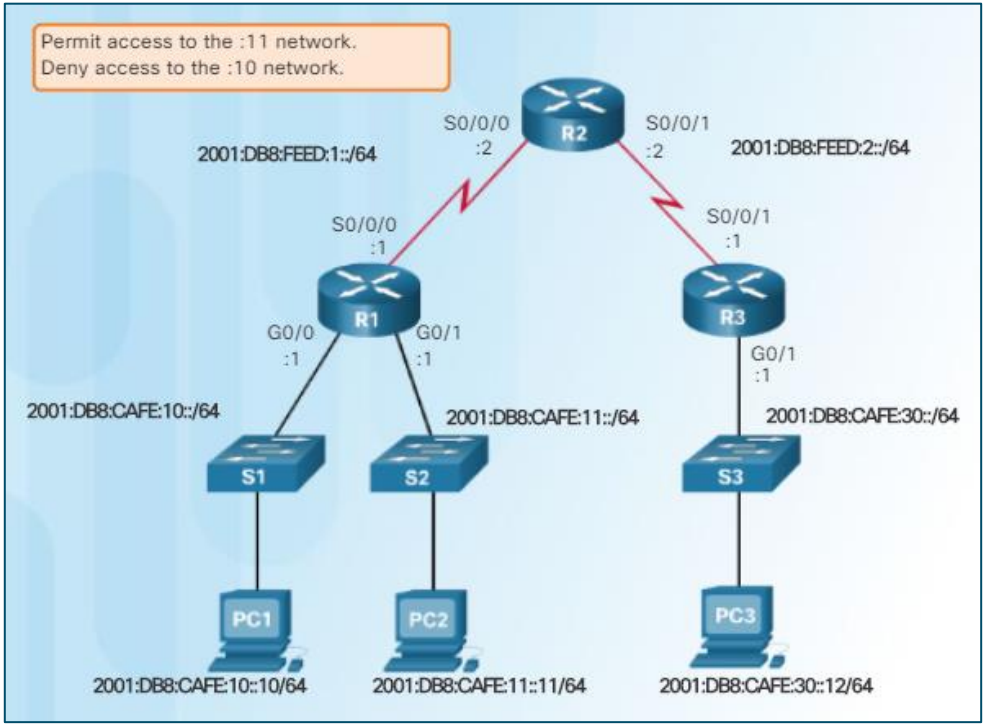
Solution:

- The ACL is correct but placed on the wrong interface
- This filter should be applied inbound on G0/0 to filter correctly.

Common ACLs Errors – Spot the Error

- Example 5: R1 is configured with an IPv6 ACL named DENY-ACCESS that should permit access to the :11 network from the :30 network, but deny access to the :10 network.

```
R1# show access-lists
IPv6 access list DENY-ACCESS
 permit ipv6 any 2001:DB8:CAFÉ:11::/64
              sequence 10
 deny ipv6 any 2001:Db8:CAFÉ:10/64
              sequence 20
R1#show ip interface G0/1
GigabitEthernet0/1 is up, line
protocol is up
...
  Outgoing access list is DENY-ACCESS
  Inbound  access list is not set
```



What Did You Learn In This Module?

- Access Control Lists (ACLs) enable a router to perform traffic filtering to manage network traffic or enforce access rules
- An ACL is a sequential list of permit and deny statements which allow or block network packets based on a defined criteria
  - Packets are always evaluated against ACL statements from top to bottom; and the checking stops as soon as the first statement match is found
  - If a packet cannot be matched with any of the ACL statements, it is automatically blocked because of an implicit ‘deny any’ at the end of each ACL
  - On a Cisco router, 1 ACL per protocol per interface per direction may be applied
- Standard and extended ACLs can be number or named
  - Numbered ACLs are identified using a numerical ID and are not easily modified once configured
  - Named ACLs are identified using an alphanumeric ID and use sequence numbers. They are easier to revise compared to numbered ACLs

What Did You Learn In This Module?

- Extended IPv4 ACLs filter traffic based on:
  - Source and destination IP address
  - Message types when filtering ICMP traffic
  - Source and destination port when filtering TCP or UDP traffic
  - Presence of the ACK flag for TCP traffic
- Extended ACLs are applied as close as possible to traffic to filter out unwanted traffic from the network as early as possible
- When troubleshooting ACLs, the following are common causes of issues:
  - Wrong order of statements
  - Errors in protocol criteria
  - Inverted source and destination criteria
  - Incorrect placement of ACL