



Prifysgol Cymru

Y Drindod Dewi Sant

University of Wales

Trinity Saint David

Trawsnewid Addysg, Trawsnewid Bywydau
Transforming Education, Transforming Lives

Routing

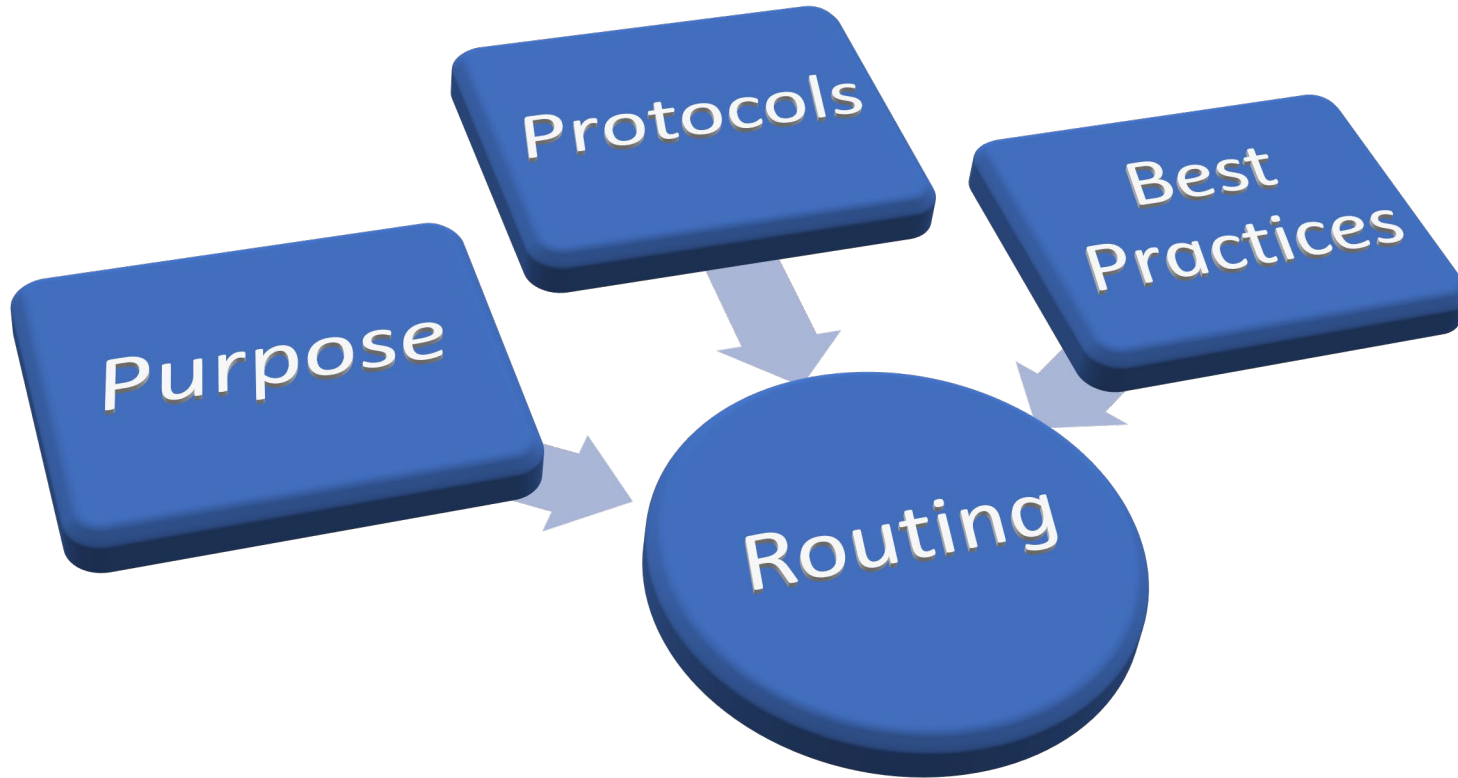
Network Operating Systems and Services ACCA5023

Today's Discussion

In today's discussion, building upon earlier lectures, where we gained an understanding of Directory Services, we now aim to apply this knowledge to deploy and manage network services and resources within an Active Directory environment.

This week, our focus shifts to Routing Protocols. We will commence our exploration with routing fundamentals, emphasizing broadcast containment, security measures,

and the various types of routing protocols available. Our discussions will further extend verification techniques using tools such as ping and traceroute.



Before we dive into today's topics, let's briefly recap what we covered so far.

Last week

☰ Consider the two scenarios below and suggest the type of hypervisor you might choose. Scenario 1: You are implementing a DHCP Server for an Enterprise Network. Scenario 2: You are testing a Certificate Authority for an ISS Server (HTTPS). Select 1 answer for each scenario

30

Scenario 1: Type 1 Hypervisor

34.48%

Scenario 1: Type 2 Hypervisor

18.97%

Scenario 2: Type 1 Hypervisor

12.07%

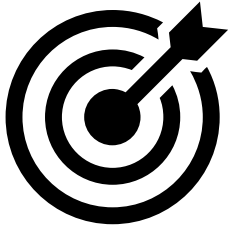
Scenario 2: Type 2 Hypervisor

34.48%

Resources required for your Coursework – Worksheets

- ✍ Download from Microsoft Evaluation Center
- ✍ Download from <https://www.debian.org/distrib/>



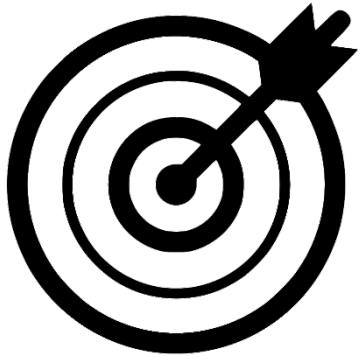


Coursework 1:

- ✍ Choose your Hypervisor based on your research (Q.2.1)
- ✍ Download (use Evaluation Copy) and Setup your Virtual Machines – as per the topology (Q. 2.2)
- ✍ Research on IP Address (Based on the Group Discussion earlier)
- ✍ Download Debian Linux
- ✍ Configure IP Address for Windows Server and Client – Successful Ping
- ✍ **Install Debian Server and Client**
- ✍ Configure IP Address for Debian Server and Client – Successful Ping
- ✍ Test and Troubleshoot (if required) your network.
- ✍ **Research on Routing and Network Services.**
- ✍ Submit your Coursework 1 – **03/03/2026**



Objectives



[This Photo](#) by Unknown Author is licensed under [CC BY-NC](#)

- ✍ Understand Routing Concepts
- ✍ Continue with your Coursework 1. **ASK FOR HELP!!!**
- ✍ Submit your report

Routing

Broadcast Containment

- ✓ Routers in the distribution layer can limit broadcasts to the local network where they need to be heard.
- ✓ Although broadcasts are necessary, too many hosts connected on the same local network can generate excessive broadcast traffic and slow down the network.

Security

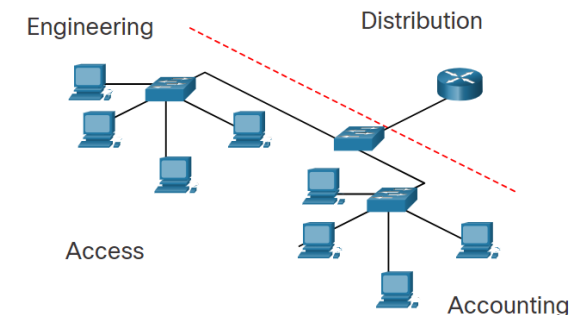
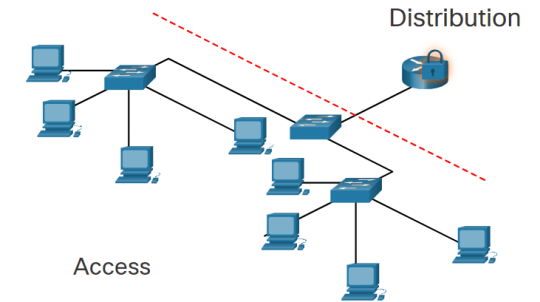
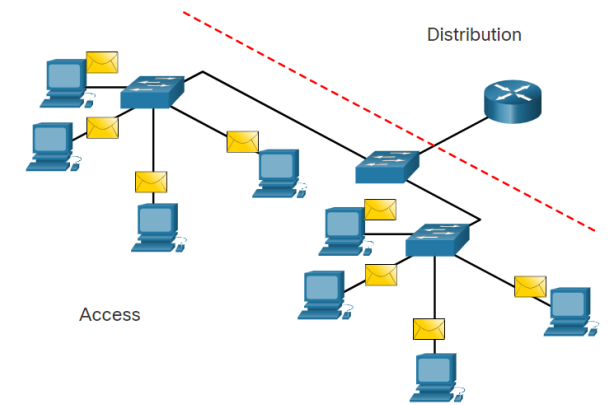
- ✓ Routers in the distribution layer can separate and protect certain groups of computers where confidential information resides.
- ✓ Routers can also hide the addresses of internal computers from the outside world to help prevent attacks, and control who can get into or out of the local network.

Locations

- ✓ Routers in the distribution layer can be used to interconnect local networks at various locations of an organization that are geographically separated.

Logical Grouping

- ✓ Routers in the distribution layer can be used to logically group users, such as departments within a company, who have common needs or for access to resources.



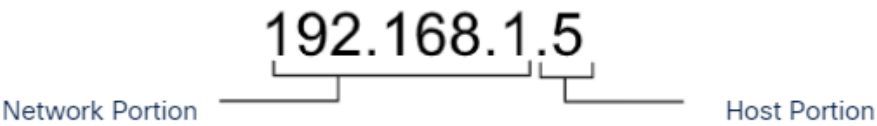
Routing



A switch examines MAC addresses.

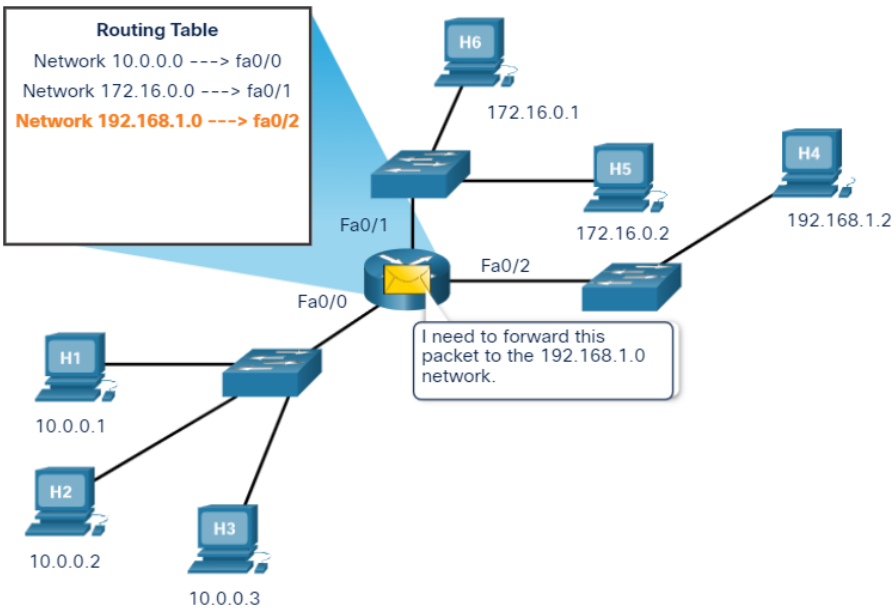


A router examines IP addresses.



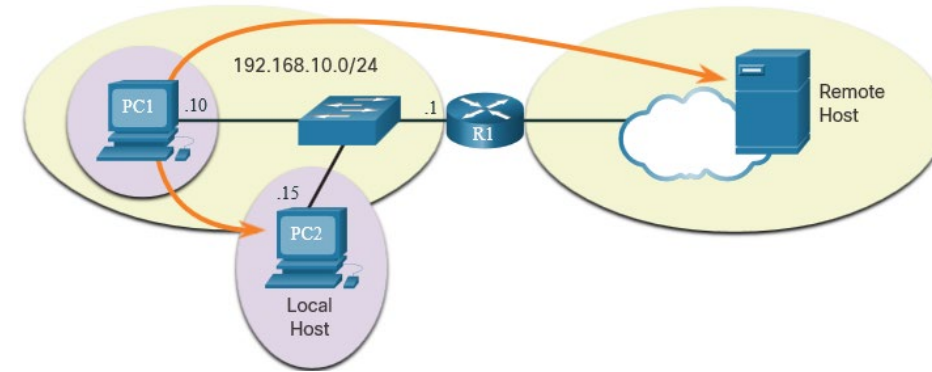
Path Selection

- ✓ Each router interface connects to a different network.
- ✓ A routing table contains information for how to reach local and remote networks.
- ✓ The destination IP address is used and compared with the networks in the routing table to determine the interface to forward the packet out of.



Routing

- Packets are always created at the source. Each host devices creates their own routing table.
- A host can send packets to the following:
 - ✓ **Itself** – 127.0.0.1 (IPv4), ::1 (IPv6)
 - ✓ **Local Hosts** – destination is on the same LAN
 - ✓ **Remote Hosts** – devices are not on the same LAN
- The Source device determines whether the destination is local or remote
- Method of determination:
 - IPv4 – Source uses its **own IP address and Subnet mask**, along with the destination IP address
 - IPv6 – Source uses the **network address and prefix** advertised by the local router
- Local traffic is dumped out the host interface to be handled by an intermediary device.
- Remote traffic is forwarded directly to the **default gateway** on the LAN.
- A router or layer 3 switch can be a default-gateway. It must have an IP address in the same range as the rest of the LAN.
- It can accept data from the LAN and is capable of forwarding traffic out of the LAN. It can route to other networks.
- If a device has no default gateway or a bad default gateway, its traffic will not be able to leave the LAN.

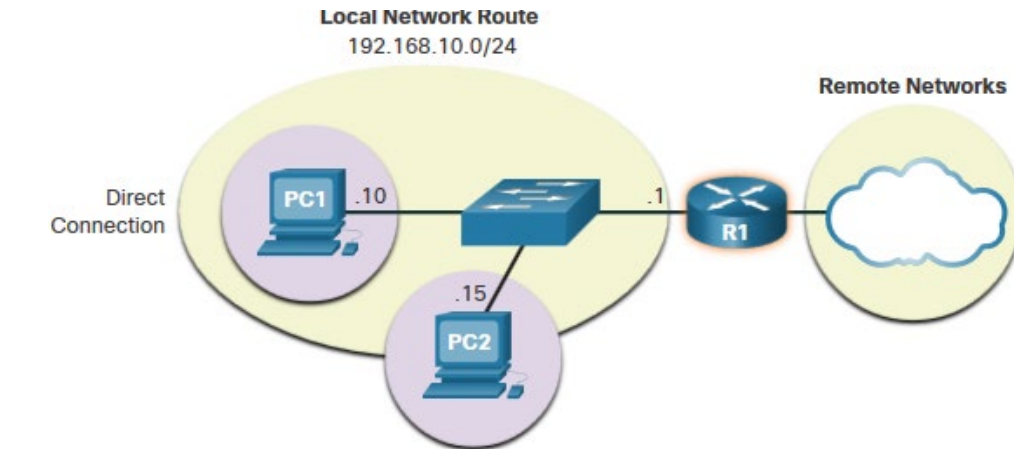


Routing

- The host will know the default gateway (DGW) either statically or through DHCP in IPv4.
- IPv6 sends the DGW through a router solicitation (RS) or can be configured manually.
- A DGW is static route which will be a last resort route in the routing table.
- All device on the LAN will need the DGW of the router if they intend to send traffic remotely.
- On Windows, route print or netstat -r to display the PC routing table
- Three sections displayed by these two commands:
 - Interface List – all potential interfaces and MAC addressing
 - IPv4 Routing Table
 - IPv6 Routing Table

```
C:\Users\PC1> netstat -r

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          192.168.10.1     192.168.10.10    25
127.0.0.0                  255.0.0.0        On-link          127.0.0.1        306
127.0.0.1                  255.255.255.255  On-link          127.0.0.1        306
127.255.255.255            255.255.255.255  On-link          127.0.0.1        306
192.168.10.0                255.255.255.0    On-link          192.168.10.10    281
192.168.10.10              255.255.255.255  On-link          192.168.10.10    281
192.168.10.255             255.255.255.255  On-link          192.168.10.10    281
224.0.0.0                  240.0.0.0        On-link          127.0.0.1        306
224.0.0.0                  240.0.0.0        On-link          192.168.10.10    281
255.255.255.255            255.255.255.255  On-link          127.0.0.1        306
255.255.255.255            255.255.255.255  On-link          192.168.10.10    281
```



IPv4 Routing Table for PC1



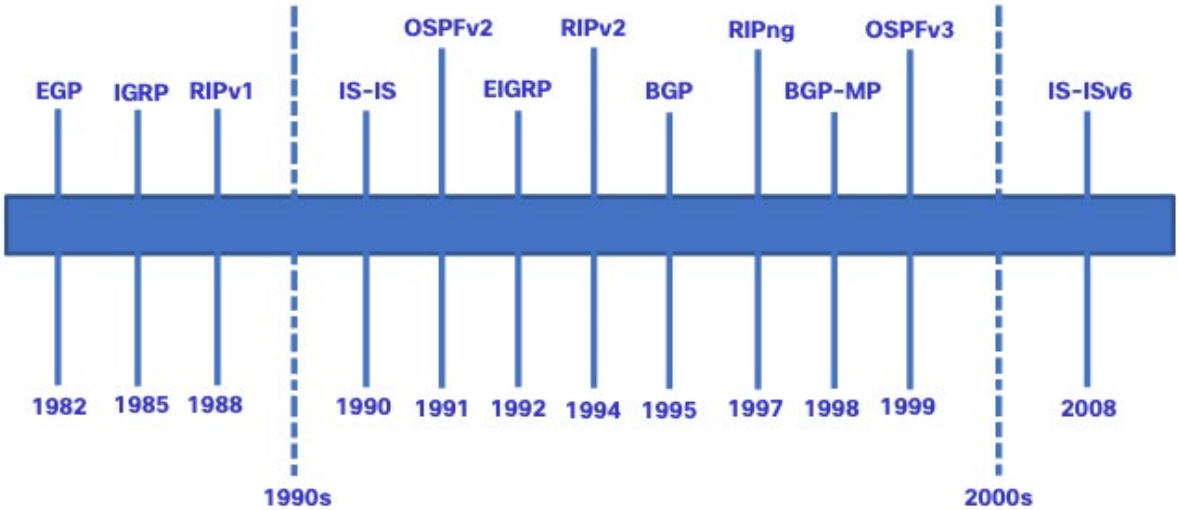
Static or Dynamic?

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

Dynamic Routing Evolution

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

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



Static Routes

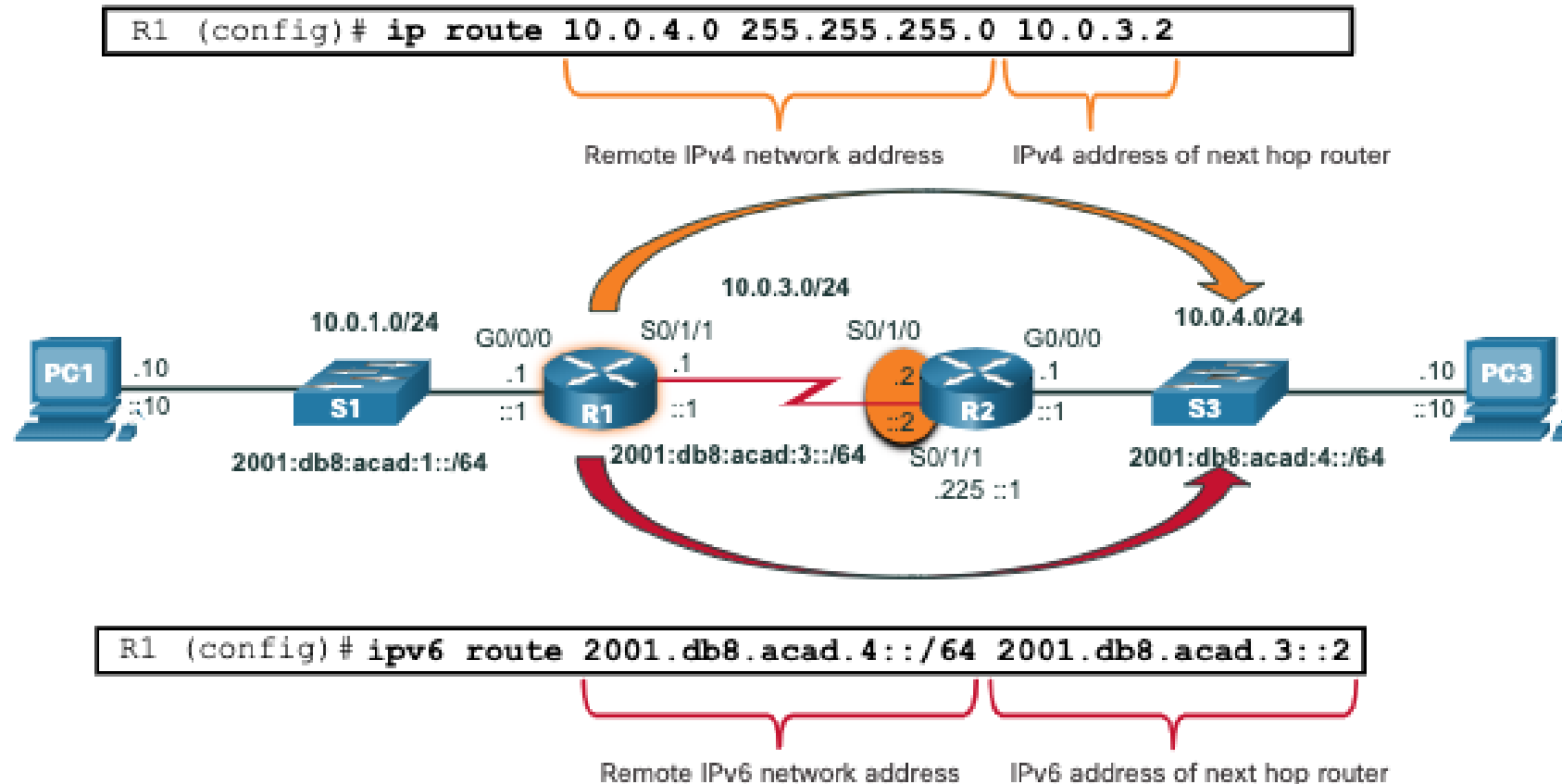
- After directly connected interfaces are configured and added to the routing table, static or dynamic routing can be implemented for accessing remote networks.
- **Static routes are manually configured.**
- They **define an explicit path between two networking devices.**
- They are not automatically updated and must be manually reconfigured if the network topology changes.

Static routing has three primary uses:

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

Static Routes

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



Dynamic Routing Protocols

- Dynamic routing protocols are used by routers **to automatically share information about the reachability and status of remote networks**. Dynamic routing protocols perform several activities, including network discovery and maintaining routing tables.

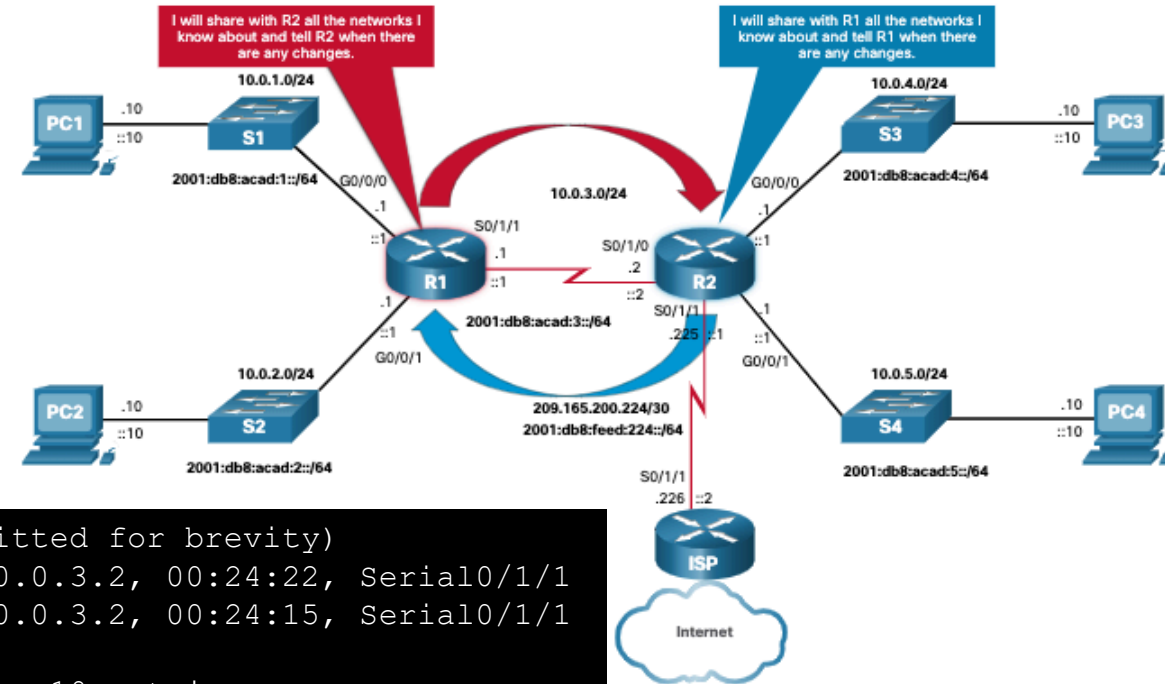
OSPF is now being used in our sample topology to dynamically learn all the networks connected to R1 and R2.

*The routing table entries use the status code of **O** to indicate the route was learned by the OSPF routing protocol.*

Both entries also include the IP address of the next-hop router, via ip-address.

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

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



```
R1# show ip route (output omitted for brevity)
O 10.0.4.0/24 [110/50] via 10.0.3.2, 00:24:22, Serial0/1/1
O 10.0.5.0/24 [110/50] via 10.0.3.2, 00:24:15, Serial0/1/1
R1# show ipv6 route
IPv6 Routing Table - default - 10 entries
(Output omitted)
NDR - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
O 2001:DB8:ACAD:4::/64 [110/50]
  via FE80::2:C, Serial0/1/1
O 2001:DB8:ACAD:5::/64 [110/50]
  via FE80::2:C, Serial0/1/1
```

Administrative Distance

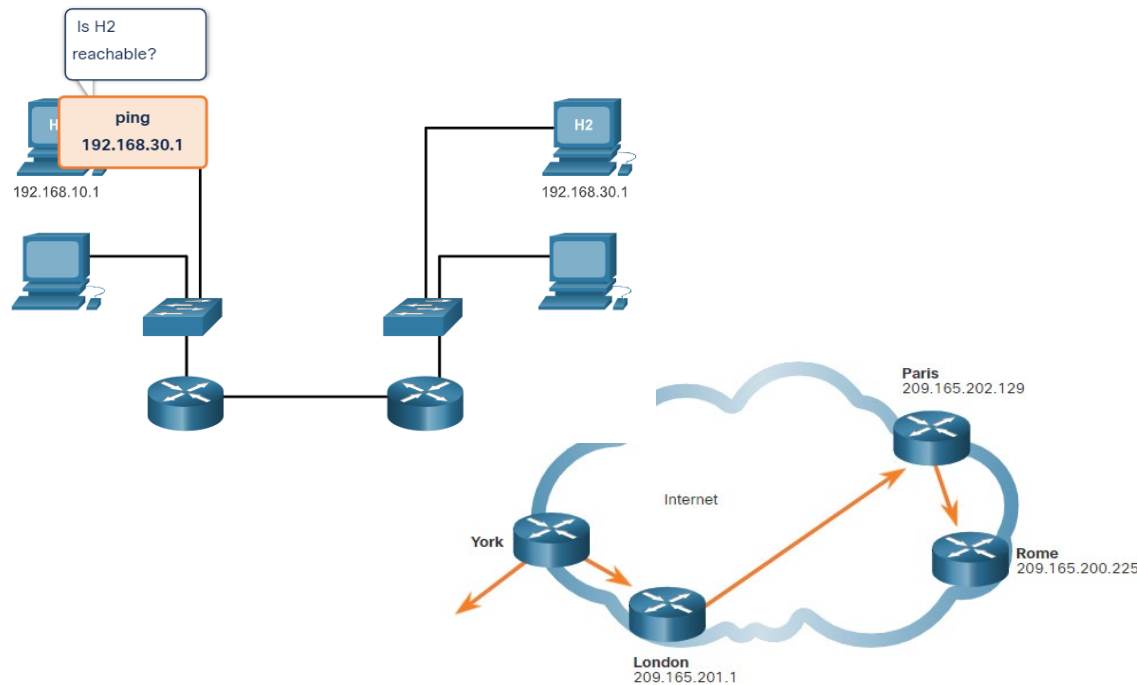
- A route entry for a specific network address (prefix and prefix length) can only appear once in the routing table. However, it is possible that the routing table learns about the same network address from more than one routing source.
- Except for very specific circumstances, only **one dynamic routing protocol should be implemented on a router**.
- Each routing protocol may decide on a different path to reach the destination based on the metric of that routing protocol.
- This raises a few questions, such as the following:
 - ❑ How does the router know which source to use?
 - ❑ Which route should it install in the routing table?
- Cisco IOS uses what is known as the **administrative distance (AD)** to determine the route to install into the IP routing table.
- The AD represents the "trustworthiness" of the route. The lower the AD, the more trustworthy the route source.

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

Static or Dynamic?

- Static and dynamic routing are not mutually exclusive. Rather, most networks use a combination of dynamic routing protocols and static routes.
- Static routes are commonly used in the following scenarios:
 - ✓ As a default route forwarding packets to a service provider
 - ✓ For routes outside the routing domain and not learned by the dynamic routing protocol
 - ✓ When the network administrator wants to explicitly define the path for a specific network
 - ✓ For routing between stub networks
- **Static routes are useful for smaller networks with only one path to an outside network.** They also provide security in a larger network for certain types of traffic, or links to other networks that need more control.
- Dynamic routing protocols are implemented in any type of network consisting of more than just a few routers.
- Dynamic routing protocols are **scalable and automatically determine better routes** if there is a change in the topology.
- Dynamic routing protocols are commonly used in the following scenarios:
 - ✓ In networks consisting of more than just a few routers
 - ✓ When a change in the network topology requires the network to automatically determine another path
 - ✓ For scalability. As the network grows, the dynamic routing protocol automatically learns about any new networks.

Verification Ping and Trace Route



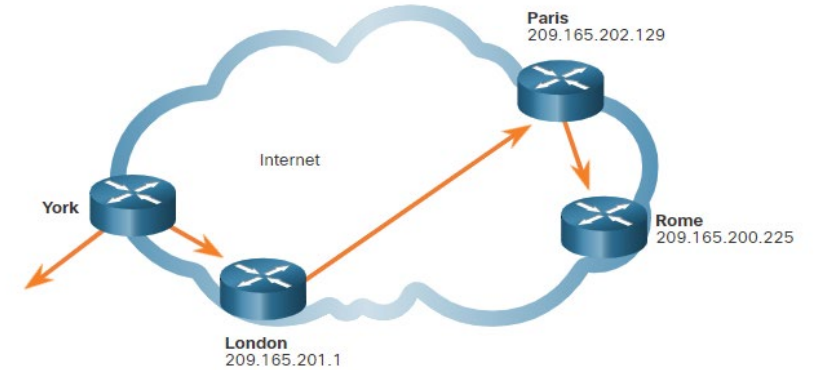
```
York# traceroute ROME
Type escape to abort.
Tracing the route to Rome (209.165.200.225)

 1. LONDON (209.165.201.1) 8msec 8 msec 4 msec
 2. PARIS (209.165.202.129) 8 msec 8 msec 8 msec
 3. ROME (209.165.200.225) 8msec 8 msec 4 msec
York#
```

- ✓ A host that sends messages across the internet must have an IP address to identify it to the other devices in the network.
- ✓ The ping utility can be used to test end-to-end connectivity between the IP address of the sending host and the IP address of the destination host.
- ✓ It measures the time that it takes test messages to make a round trip from the source to the destination, and whether the transmission is successful.
- ✓ However, if the test message does not reach the destination, or if delays are encountered along the way, ping cannot determine where the problem is located.
- ✓ The format of the ping command is ping x.x.x.x, where x.x.x.x is an IP address or domain name of the destination host:
- ✓ For example, ping 192.168.30.1, ping www.cisco.com, etc.
- ✓ The traceroute utility traces the route a message takes from its source to the destination.
- ✓ Each individual network through which the message travels is referred to as a hop.
- ✓ The traceroute command displays each hop along the way and the time it takes for the message to get to that network and back.

The traceroute Command

- The **traceroute** utility traces the route a message takes from its source to the destination.
- Each individual network through which the message travels is referred to as a hop.
- The **traceroute** command displays each hop along the way and the time it takes for the message to get to that network and back.
- If a problem occurs, the output of the traceroute utility can help determine where a message was lost or delayed.
- The traceroute utility is called **tracert** in the Windows environment.



```
York# traceroute ROME

Type escape to abort.
Tracing the route to Rome (209.165.200.225)

 1. LONDON (209.165.201.1)  8msec  8 msec  4 msec
 2. PARIS (209.165.202.129) 8 msec  8 msec  8 msec
 3. ROME (209.165.200.225) 8msec  8 msec  4 msec
York#
```



Any Questions?