Advanced Computer Network

LECTURE 3

Introduction to Routing Algorithms

Content:

1 Routing Algorithms and its importance

What Are Routing Algorithms?

- **Definition:** Routing algorithms are methods or protocols used by routers to determine the best path for data packets to travel from the source to the destination.
- **Purpose:**
  - Ensure efficient and reliable data delivery.
  - Adapt to network changes (e.g., link failures, congestion).
- **Key Goals:**
  - Optimality: Find the best path.
  - Scalability: Work in large networks.
  - Robustness: Handle failures gracefully.

How Routing Algorithms Work?

- **Step 1: Information Gathering:**
  - Routers collect data about network topology.
  - Example: OSPF uses LSAs (Link-State Advertisements).
- **Step 2: Path Calculation:**
  - Routers compute the best paths using algorithms.
  - Example: Dijkstra’s algorithm in OSPF.
- **Step 3: Routing Table Update:**
  - Routers update their routing tables.
  - Example: A router adds an entry for destination 192.168.1.0/24.
- **Step 4: Forwarding Packets:**
  - Routers forward packets based on the routing table.

Dynamic Routing Protocol Concepts

The main components of dynamic routing protocols include the following:

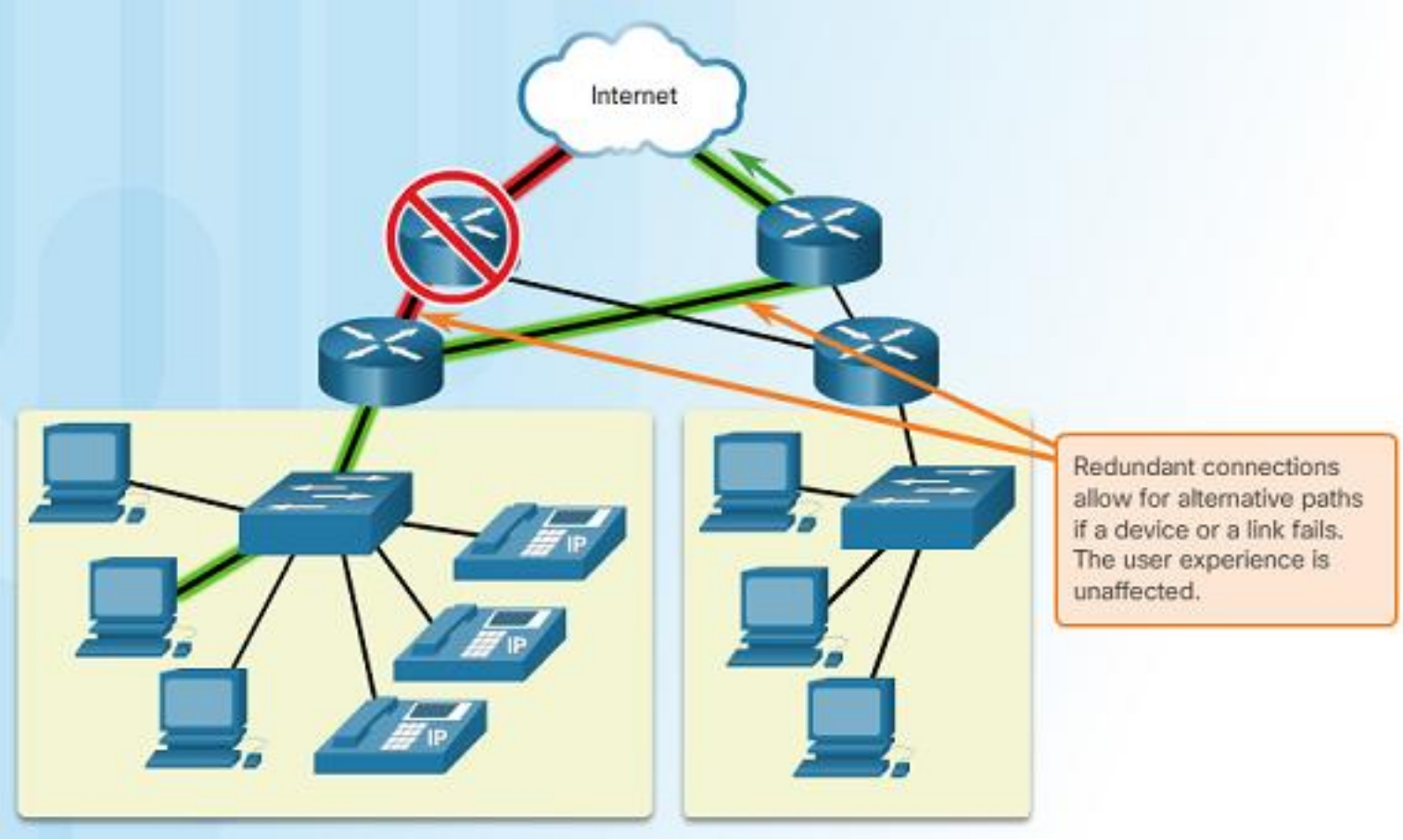
- **Data structures -** Routing protocols typically use tables or databases for their operations. This information is kept in RAM.
- **Routing protocol messages -** Routing protocols use various types of messages to discover neighboring routers, exchange routing information, and other tasks to learn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

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

Importance of Routing Algorithms

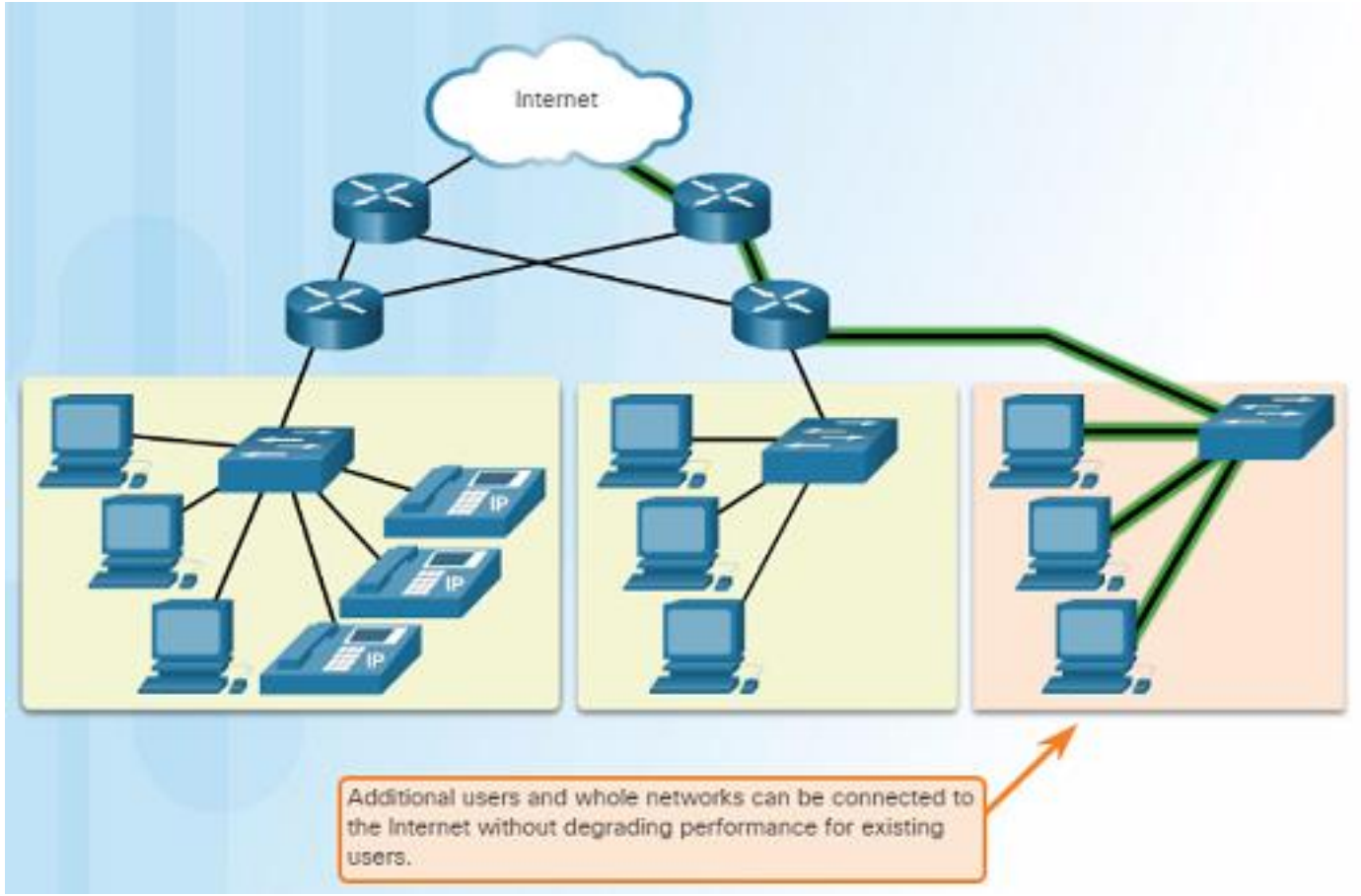
- **Fault Tolerance:** Automatically reroutes traffic in case of link failures.
- **Network Scalability:** Allows networks to grow without performance degradation.
- **Quality of Service:**
- Efficient Data Delivery**:** Ensures packets take the shortest or least congested path.
- Load Balancing**:** Distributes traffic across multiple paths to avoid congestion.
- **Security:**

Fault Tolerance



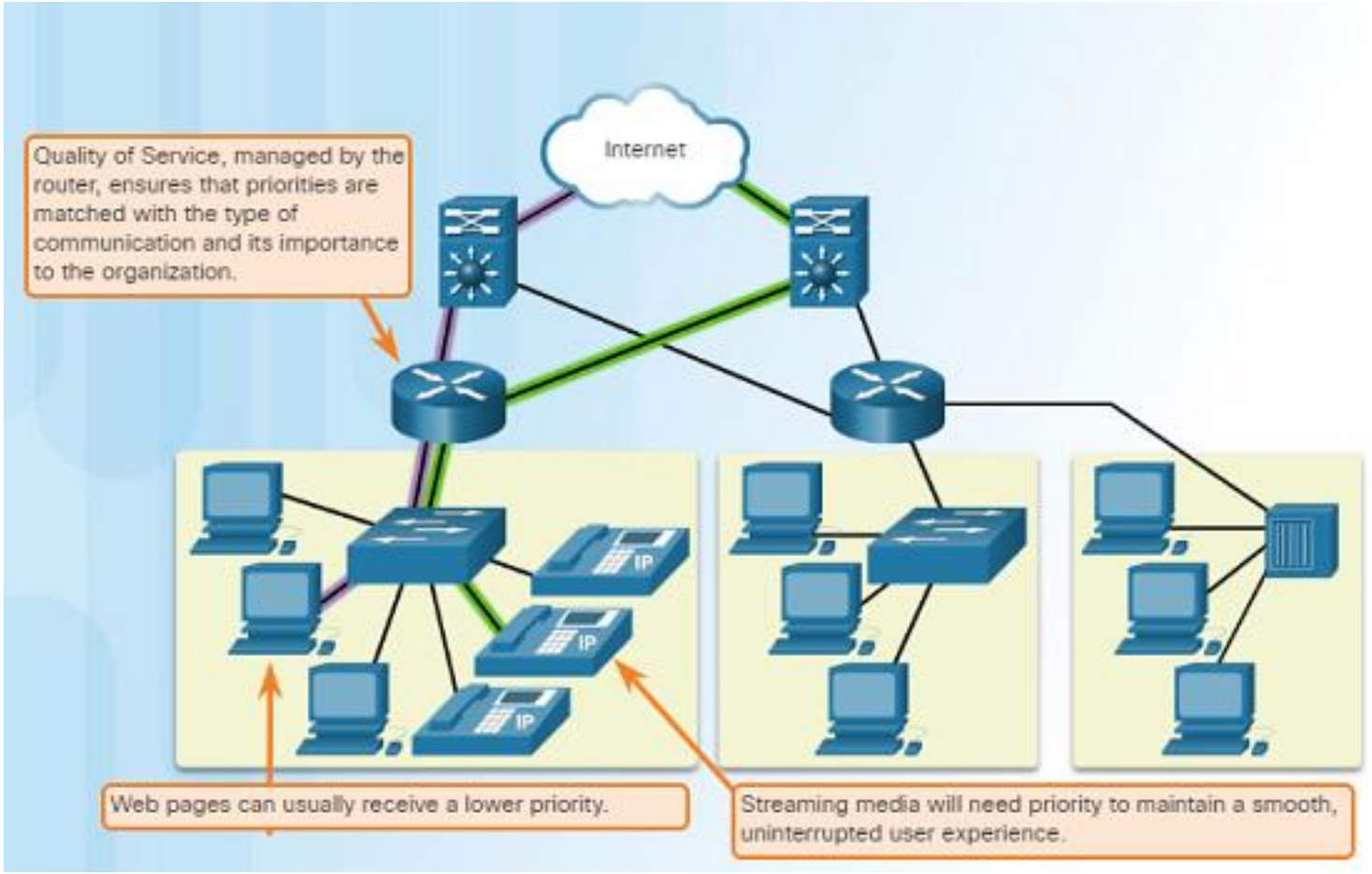
- A fault tolerant network limits the impact of a failure by limiting the number of affected devices.
- Multiple paths are required for fault tolerance.
- Reliable networks provide redundancy by implementing a packet switched network. Packet switching splits traffic into packets that are routed over a network. Each packet could theoretically take a different path to the destination.
- This is not possible with circuit-switched networks which establish dedicated circuits.

Scalability



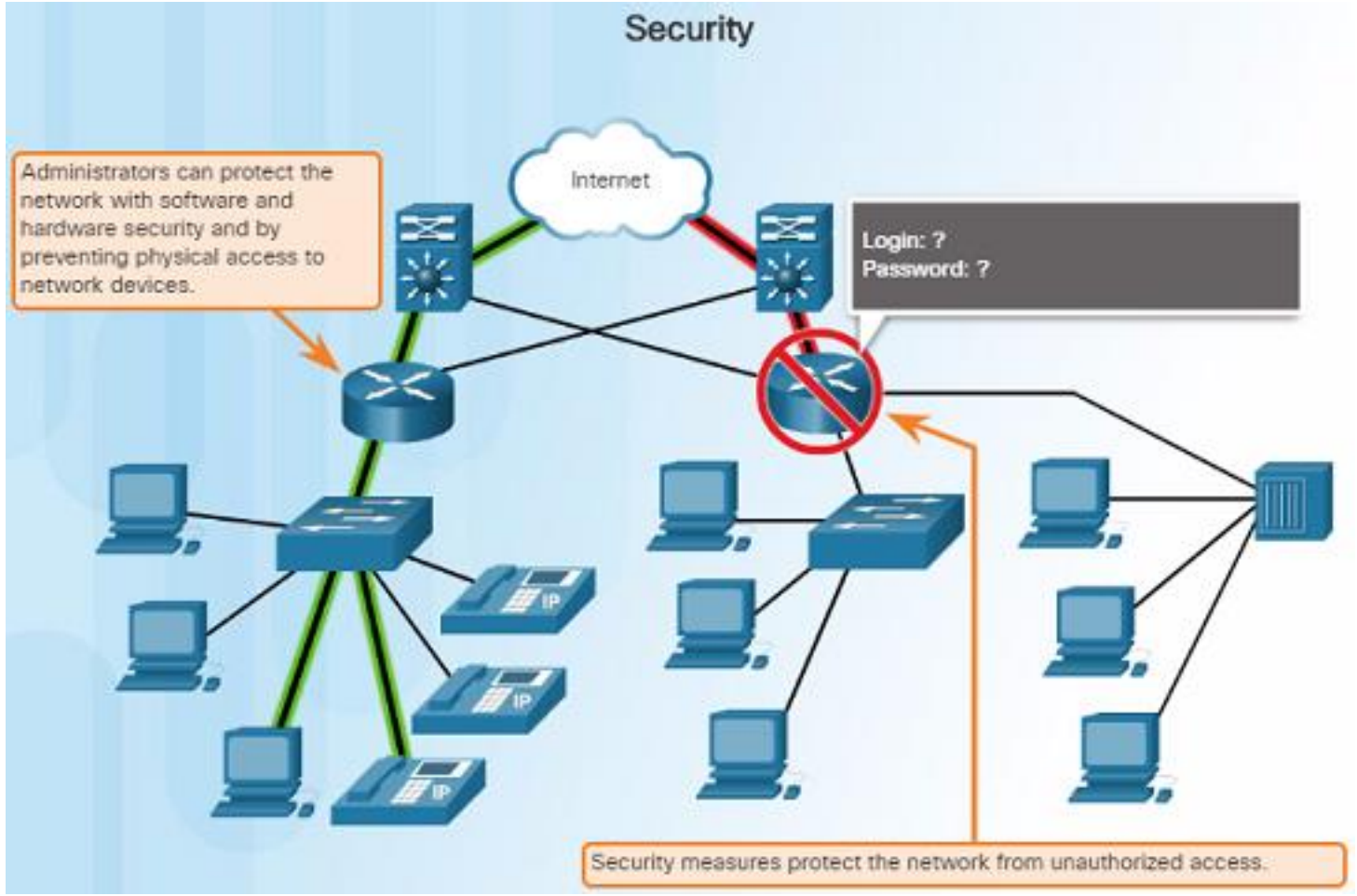
- A scalable network can expand quickly and easily to support new users and applications without impacting the performance of services to existing users.
- Network designers follow accepted standards and protocols in order to make the networks scalable.

Quality of Service



- Voice and live video transmissions require higher expectations for those services being delivered.
- Have you ever watched a live video with constant breaks and pauses? This is caused when there is a higher demand for bandwidth than available – and QoS isn't configured.
- Quality of Service (QoS) is the primary mechanism used to ensure reliable delivery of content for all users.
- With a QoS policy in place, the router can more easily manage the flow of data and voice traffic.

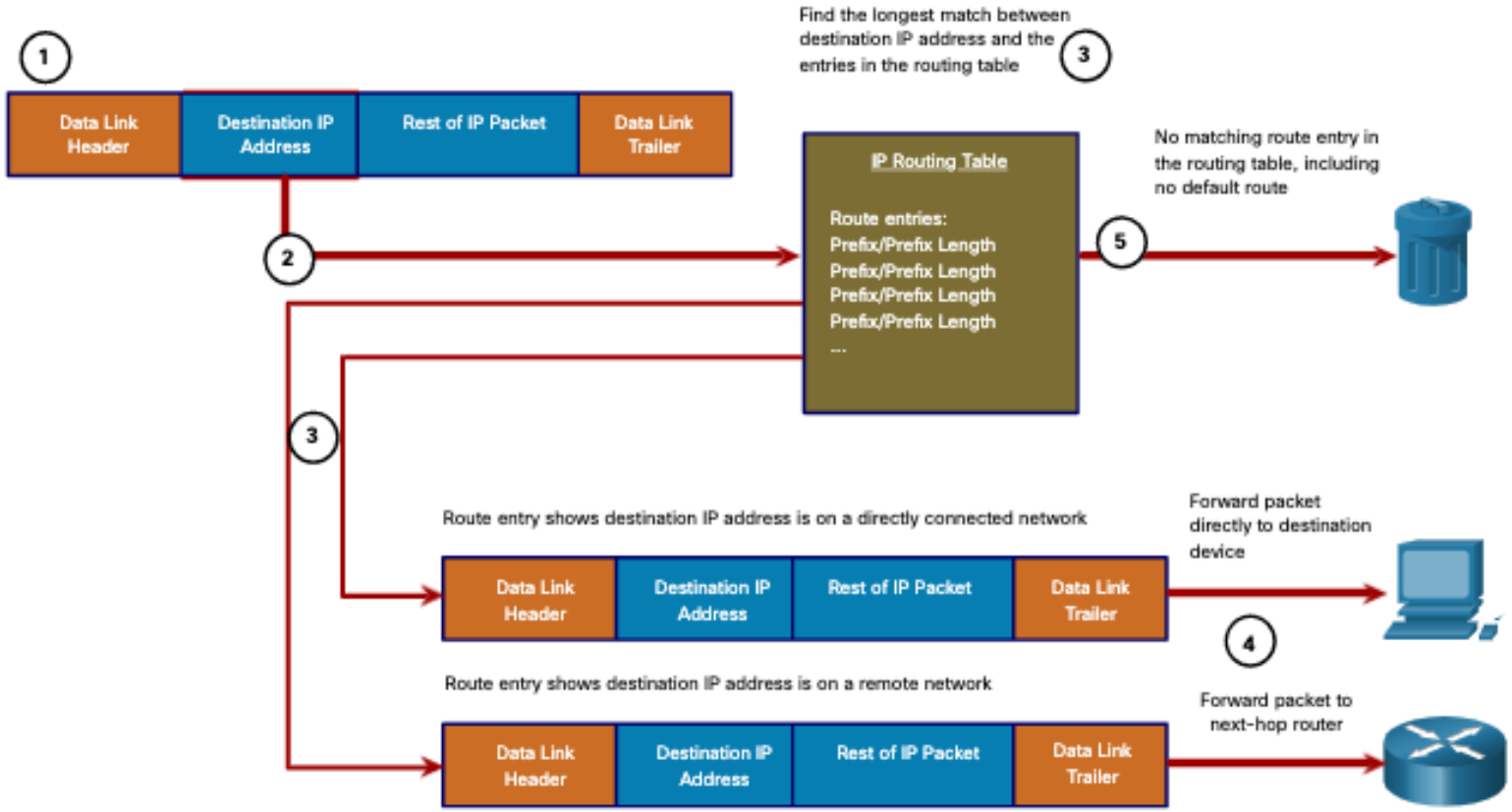
Reliable Network
Security



- There are two main types of network security that must be addressed:
  - Network infrastructure security
    - Physical security of network devices
    - Preventing unauthorized access to the management software on those devices
  - Information Security
    - Protection of the information or data transmitted over the network
- Three goals of network security:
  - Confidentiality – only intended recipients can read the data
  - Integrity – assurance that the data has not be altered with during transmission
  - Availability – assurance of timely and reliable access to data for authorized users

2 Packet Forwarding

Packet Forwarding Decision Process



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

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

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

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

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

Packet Forwarding Decision Process (Cont.)

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

Forward the Packet to a Device on a Directly Connected Network

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

- **Egress** refers to the act of exiting or going out of a place or system.
- **Ingress** refers to the act of entering or going into a place or system.

Packet Forwarding Decision Process (Cont.)

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

Forward the Packet to a Next-Hop Router

- If the route entry indicates that the destination IP address is **on a remote network**, meaning a device on network that is **not directly connected**. The packet must be **forwarded to the next-hop router**. The next-hop address is indicated in the route entry.

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

Note: This process will vary for other types of Layer 2 networks.

Packet Forwarding Decision Process (Cont.)

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

Drop the Packet - No Match in Routing Table

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

End-to-End Packet Forwarding

The **primary responsibility** of the packet forwarding function is to **encapsulate packets in the appropriate data link frame type for the outgoing interface**.

For example, the data link frame format for a serial link could be

- ✓ **Point-to-Point (PPP)** protocol,
- ✓ High-Level **Data Link Control (HDLC)** protocol,
- ✓ or some other **Layer 2 protocol such Ethernet protocol**.

Packet Forwarding Mechanisms

The primary responsibility of the packet forwarding function is to encapsulate packets in the appropriate data link frame type for the outgoing interface.

The more **efficiently a router** can perform this task, the **faster packets** can be forwarded by the router.

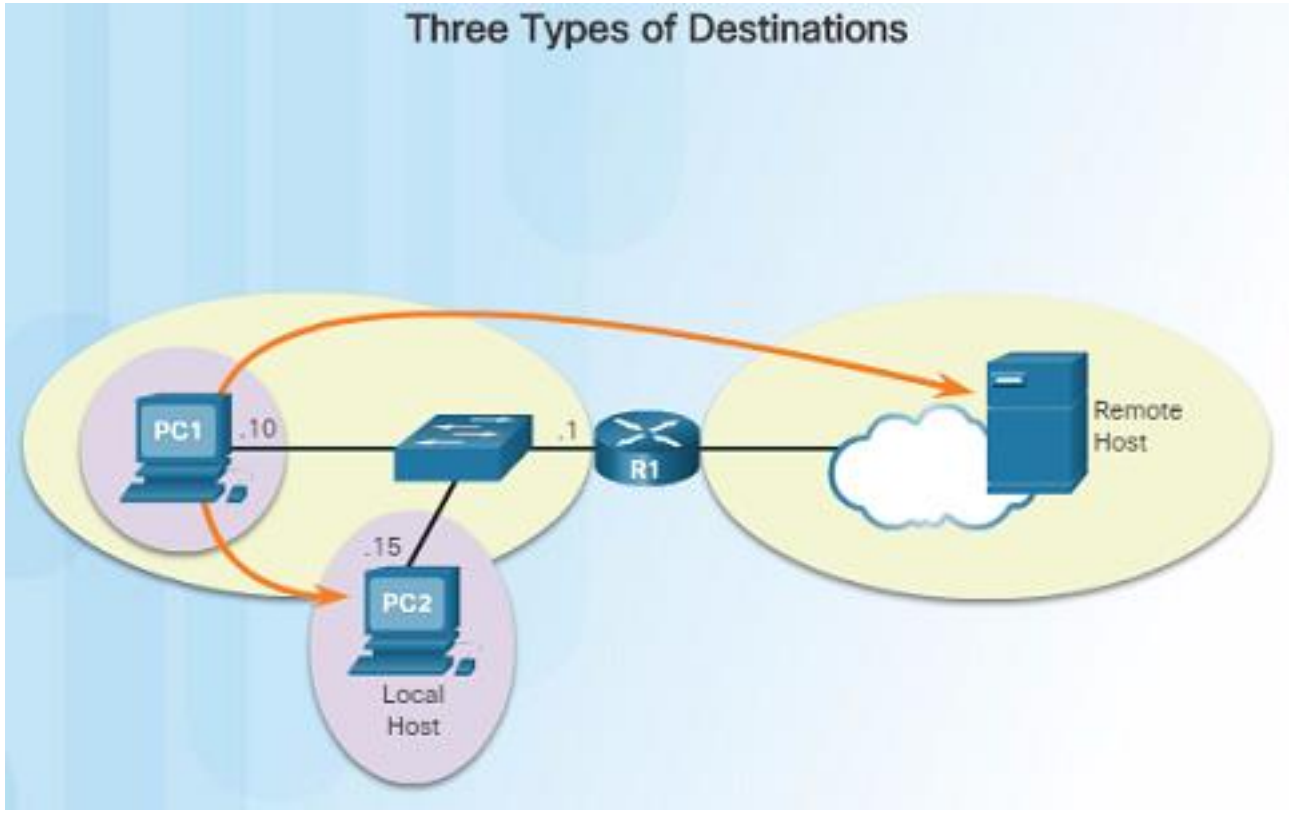
Routers support the following three packet forwarding mechanisms:

- Process switching
- Fast switching
- Cisco Express Forwarding (CEF)

3 Routing

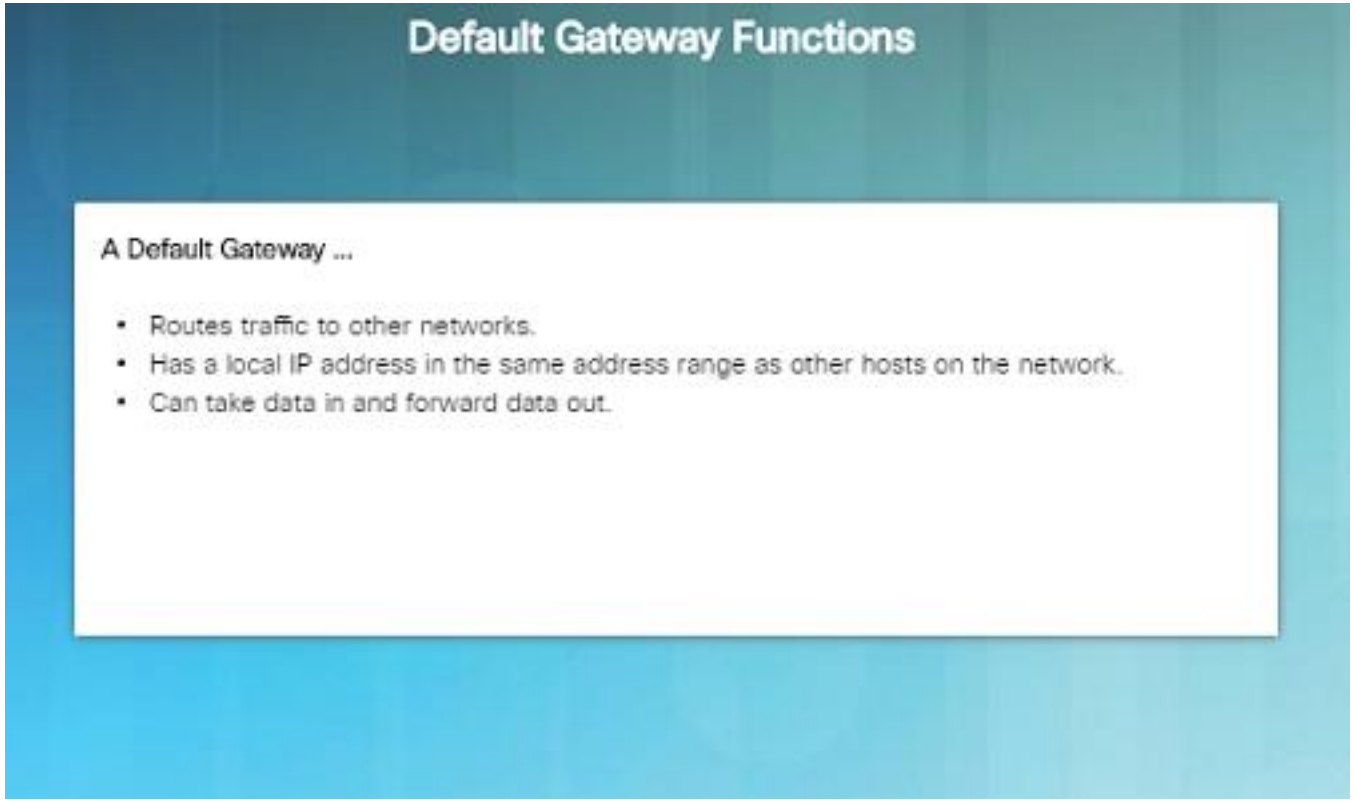
3.1 Routing at Host

Host Forwarding Decision



- An important role of the network layer is to direct packets between hosts. A host can send a packet to:
  - **Itself** – A host can **ping itself** for testing purposes using 127.0.0.1 which is referred to as the **loopback** interface.
  - **Local host** – This is a host on the same local network as the sending host. The **hosts share the same network address**.
  - **Remote host** – This is a host on a remote network. The hosts do not share the same network address.
- The **source** IPv4 address and subnet mask is **compared** with the **destination address** and subnet mask in order to determine if the host is on the **local network** or **remote network**.

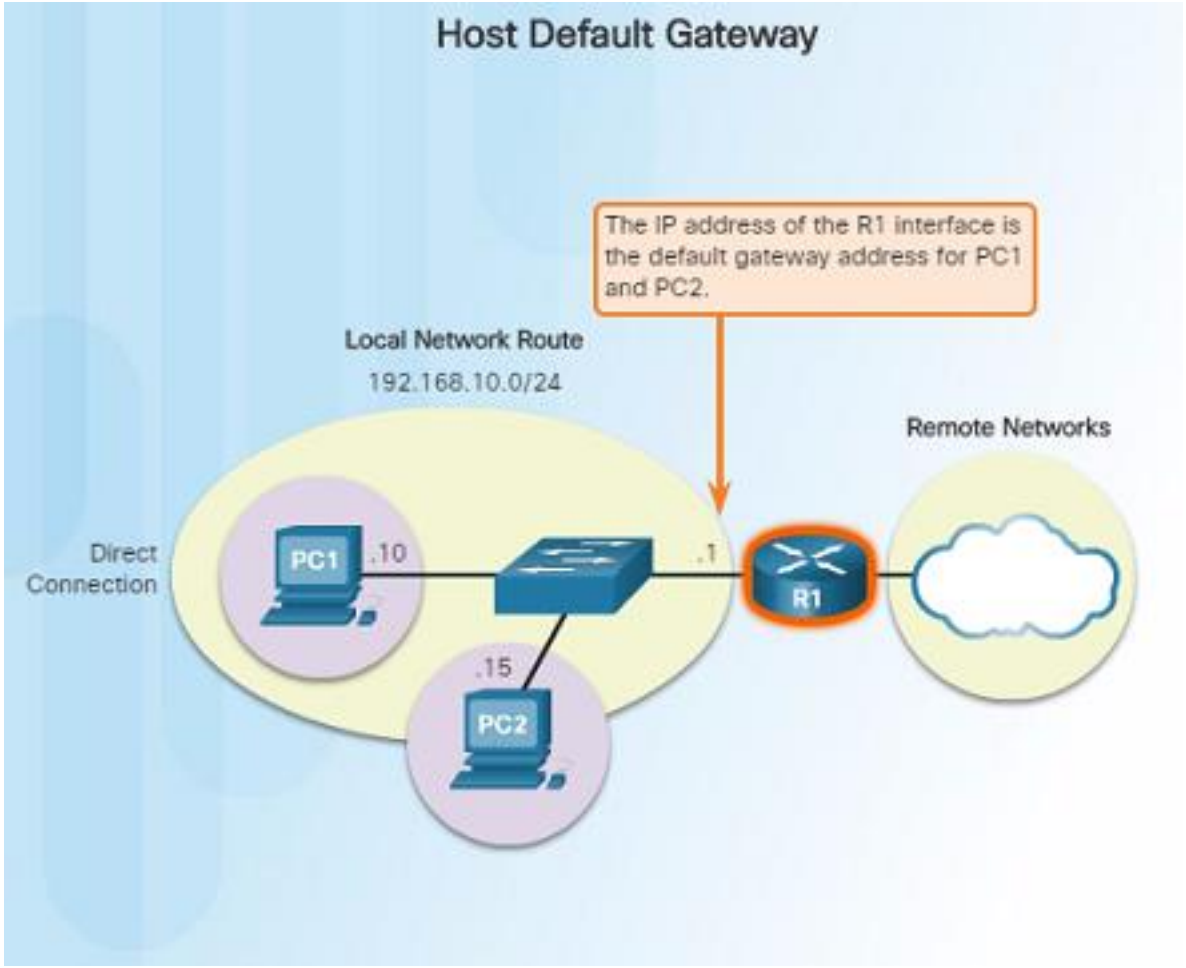
Default Gateway



- The **default gateway** is the network device that can route traffic out to other networks. It is the router that routes traffic out of a local network.
- This **occurs** when the **destination** host is **not on the same local network** as the sending host.
- The default gateway will know where to send the packet using its **routing table**.
- The sending host does not need to know where to send the packet other than to the default **gateway** – or router.

Using the Default Gateway

- A **host's routing table** usually includes a **default gateway** address – which is the router IP address for the network that the host is on.
- The **host receives the IPv4 address** for the default gateway **from (1) DHCP**, or it is **(2)manually configured**.
- Having a default gateway configured creates a **default route in the routing table of a host** - which is the route the computer will send a packet to when it needs to contact a **remote network**.



3.2 Routing in Routers

Routing Table Principles

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

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

Route Sources

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

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

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

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

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

Static Routes

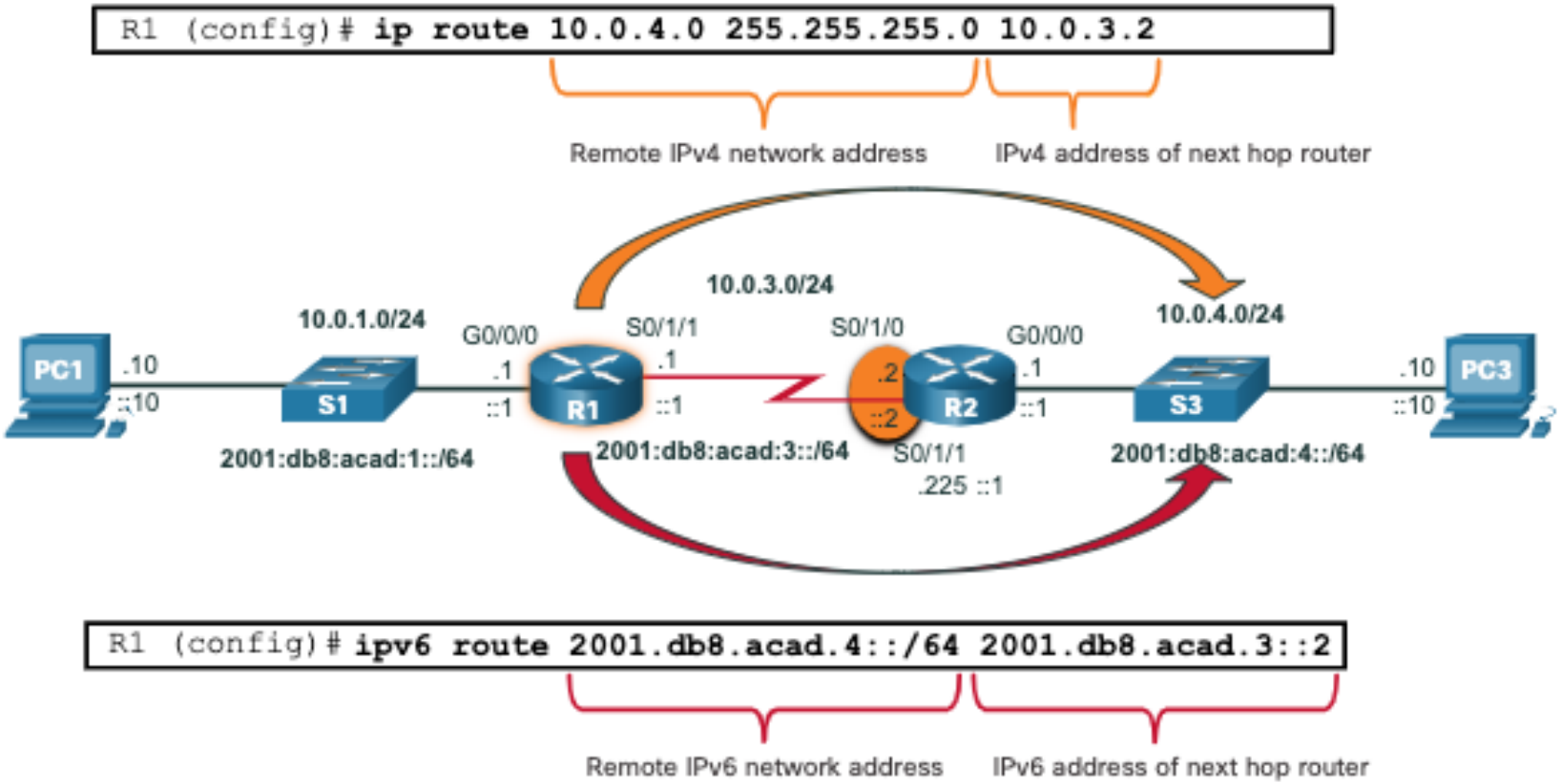
After directly connected interfaces are configured and added to the routing table, static or dynamic routing can be implemented for accessing remote networks. Static routes are manually configured. They define an explicit path between two networking devices. They are not automatically updated and must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

Static routing has three primary uses:

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

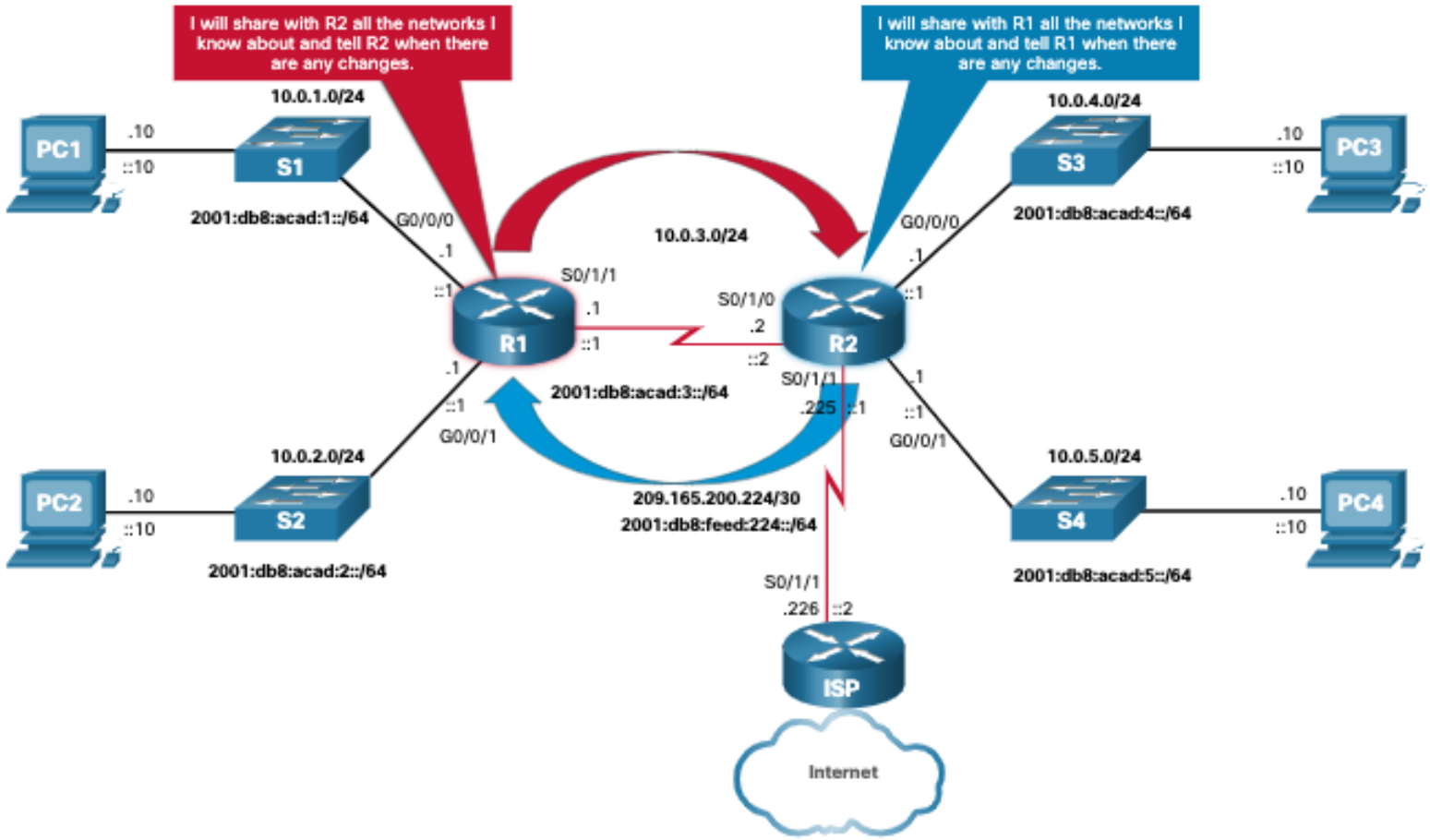
Static Routes in the IP Routing Table

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



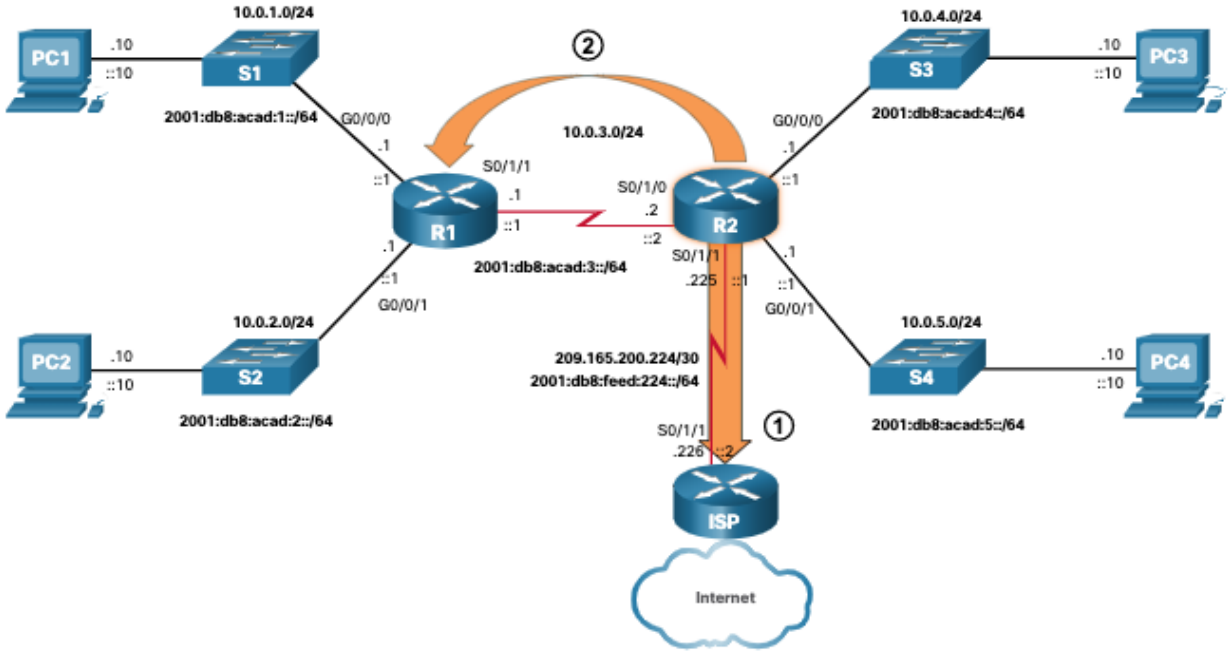
Dynamic Routing Protocols

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



Default Route

The default route specifies a next-hop router to use when the routing table does not contain a specific route that matches the destination IP address. A default route can be either a static route or learned automatically from a dynamic routing protocol. A default route has an IPv4 route entry of 0.0.0.0/0 or an IPv6 route entry of ::/0. This means that zero or no bits need to match between the destination IP address and the default route.



Structure of an IPv4 Routing Table

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

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

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.

Administrative Distance (Cont.)

The table lists various routing protocols and their associated ADs.

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

3.3 Static or Dynamic Routing

Static or Dynamic?

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

Static routes are commonly used in the following scenarios:

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

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

Static or Dynamic? (Cont.)

Dynamic routing protocols are implemented in any type of network consisting of more than just a few routers. Dynamic routing protocols are scalable and automatically determine better routes if there is a change in the topology.

Dynamic routing protocols are commonly used in the following scenarios:

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

Static or Dynamic? (Cont.)

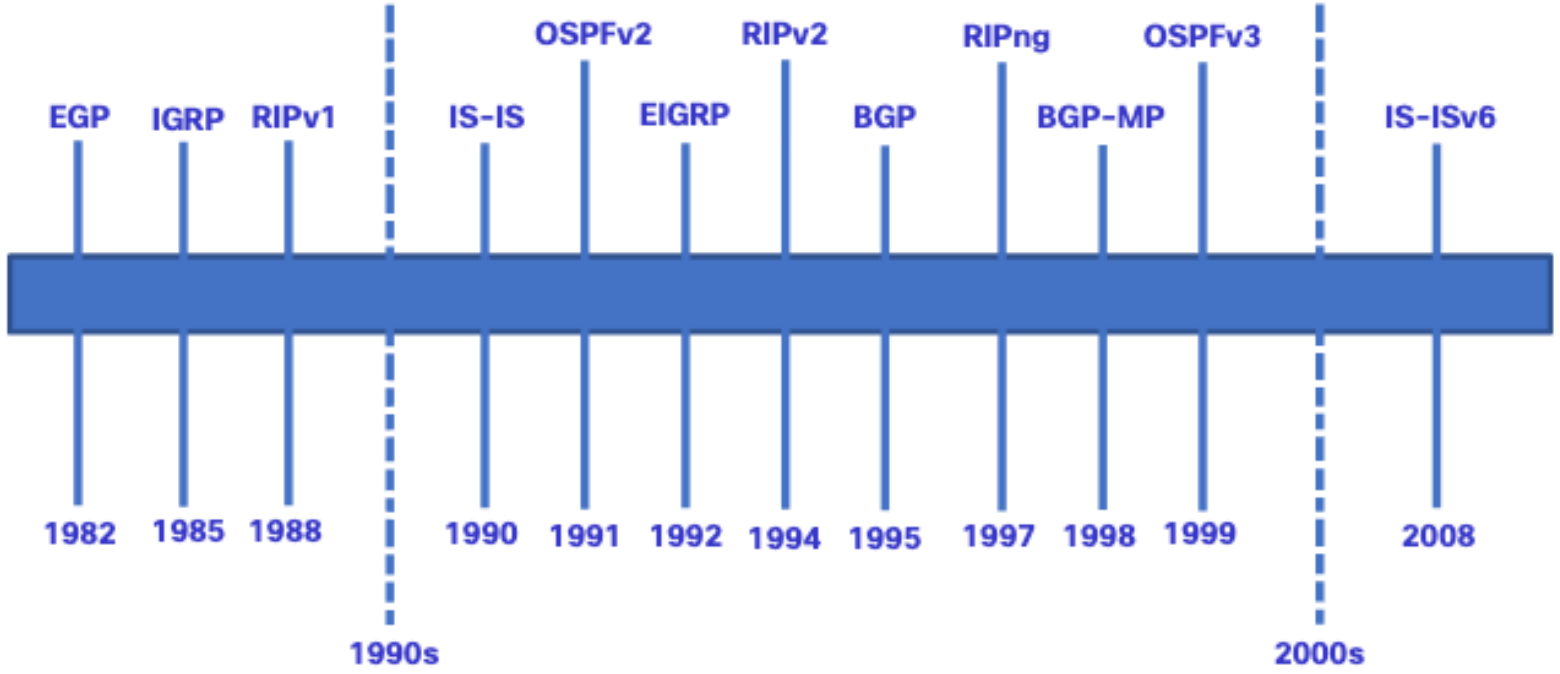
The table shows a comparison of some the differences between dynamic and static routing.

Feature	Dynamic Routing	Static Routing
Configuration complexity	Independent of network size	Increases with network size
Topology changes	Automatically adapts to topology changes	Administrator intervention required
Scalability	Suitable for simple to complex network topologies	Suitable for simple topologies
Security	Security must be configured	Security is inherent
Resource Usage	Uses CPU, memory, and link bandwidth	No additional resources needed

3.4 Dynamic Routing

Dynamic Routing Evolution

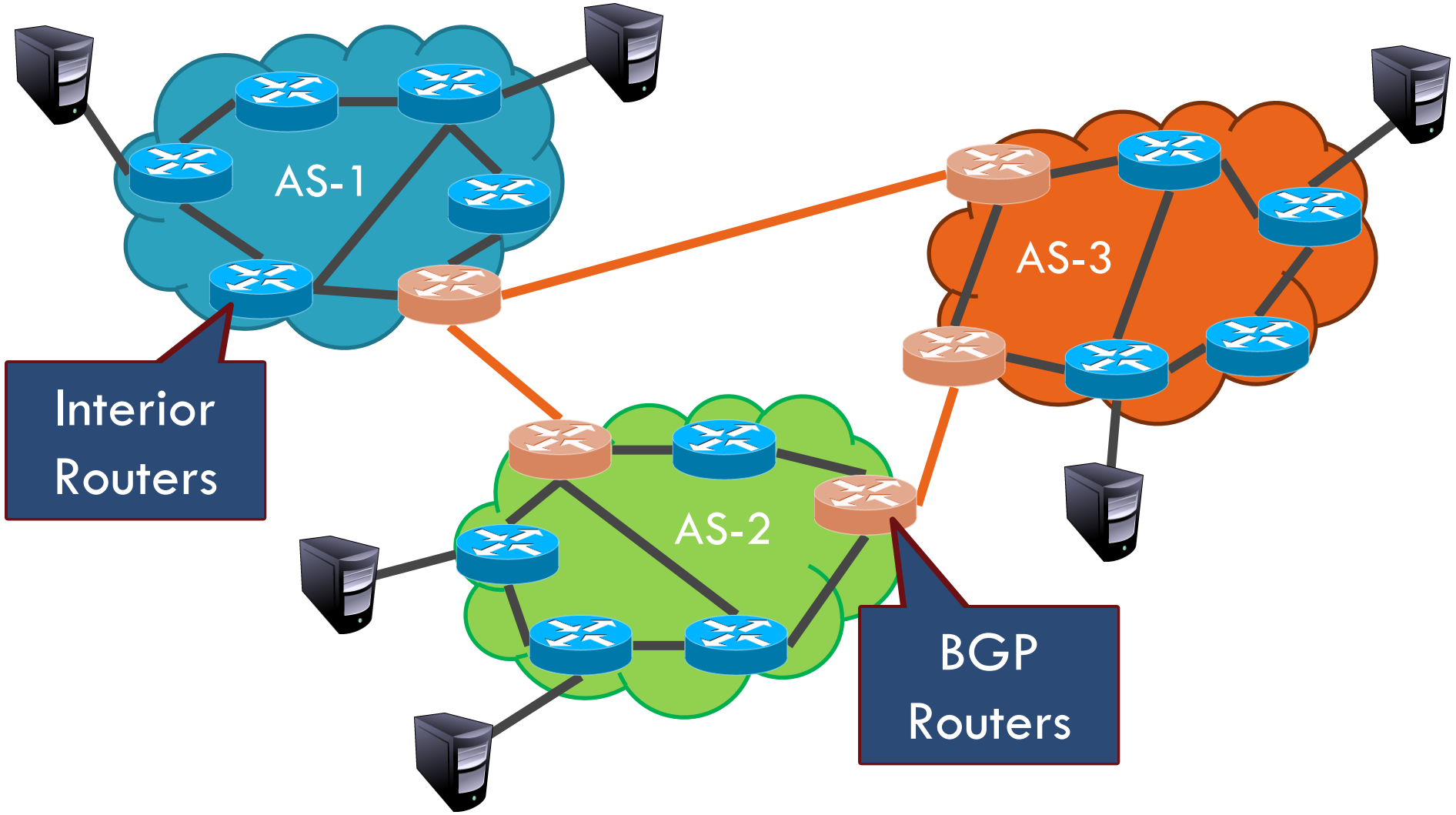
Dynamic routing protocols have been used in networks since the late 1980s. One of the first routing protocols was RIP. RIPv1 was released in 1988, but some of the basic algorithms within the protocol were used on the Advanced Research Projects Agency Network (ARPANET) as early as 1969. As networks evolved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



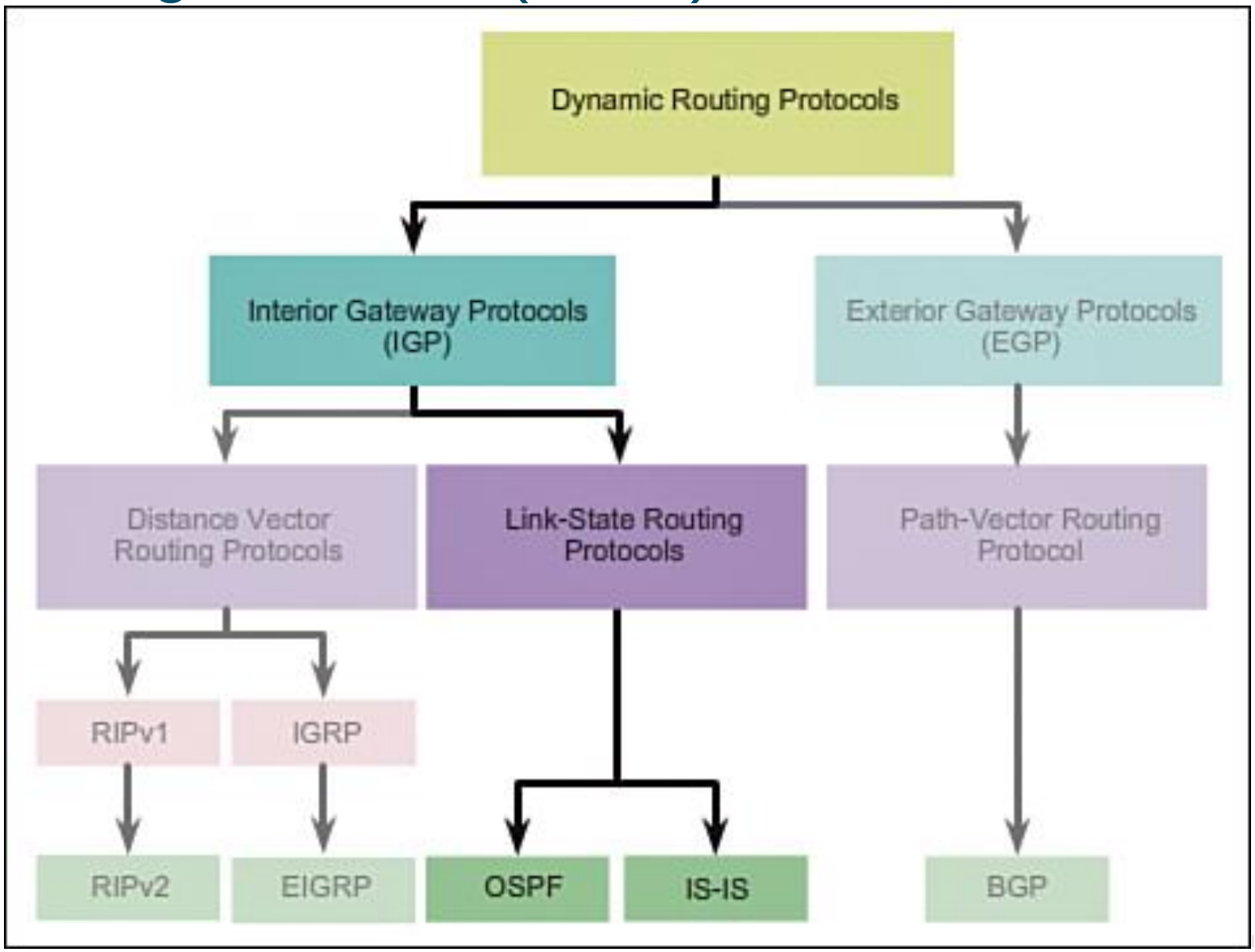
Dynamic Routing Evolution (Cont.)

- Internet organized as a two-level hierarchy
- First level – autonomous systems (AS's)
  - AS – region of network under a single administrative domain
  - AS's use intra-domain routing protocols internally
    - Distance Vector, e.g., Routing Information Protocol (RIP)
    - Link State, e.g., Open Shortest Path First (OSPF)
- Second level – Connections between AS's use inter-domain routing protocols
  - Border Gateway Routing (BGP)
  - De facto standard today, BGP-4

AS Example



Dynamic Routing Evolution (Cont.)



Distance-Vector Routing Algorithms

- **How It Works:**
  - Routers share their routing tables with neighbors.
  - Each router updates its table based on received information.
  - Uses the Bellman-Ford algorithm to compute paths.
- **Advantages:**
  - Simple to implement.
  - Low overhead in small networks.
- **Example:** RIP (Routing Information Protocol).

Link-State Routing Algorithms

- **How It Works:**
  - Routers share information about their directly connected links.
  - Each router builds a complete map of the network.
  - Uses Dijkstra's algorithm to compute the shortest path.
- **Advantages:**
  - Fast convergence.
  - Supports large networks.
- **Example:** OSPF (Open Shortest Path First).

Best Path

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

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

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

Features	Distance Vector	Link State
Convergence	Slow	Fast
Updates	Frequently	Event Triggered
Loops	Prone to routing Loops	Less Subjected to Routing Loops
Configuration	Easy	Difficult
Network Types	Broadcast for updates sent	Multicast for updates sent
Topology	doesn't know Network Topology	Knows entire Network Topology
Automatic Route Summarization	No	Yes
Path Calculation	Hop Count	Shortest Path -Metric
Scalability	Limited	Can be highly scalable
Protocols	RIP, IGRP	OSPF, IS-IS
Algorithm	Bredford Algorithm	Dijkstra-algorithm
Manual Route Summarization	Yes	Yes
Metric	Hop Count	Link Cost

Challenges in Routing Algorithms

- **1. Scalability:**
  - Handling large networks with millions of routes.
  - Example: BGP scales to the global Internet.

- **2. Convergence Time:**
  - Time for all routers to agree on the network topology.
  - Example: Slow convergence can cause routing loops.

- **3. Security:**
  - Protecting against attacks like route hijacking.
  - Example: BGPsec enhances BGP security.

- **4. Load Balancing:**
  - Distributing traffic across multiple paths.
  - Example: OSPF supports ECMP (Equal-Cost Multipath).

Load Balancing

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

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

Note: Only EIGRP supports unequal cost load balancing.

Thank you

Verification Commands

Common verification commands include the following:

- **show ip interface brief**
- **show running-config interface** *interface-type number*
- **show interfaces**
- **show ip interface**
- **show ip route**
- **ping**

In each case, replace **ip** with **ipv6** for the IPv6 version of the command.