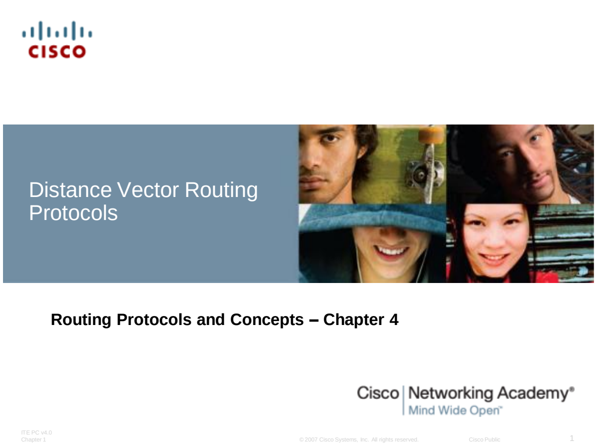
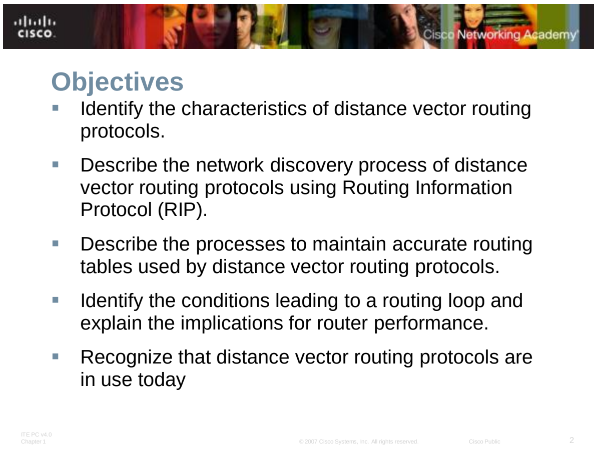


Distance Vector Routing Protocols

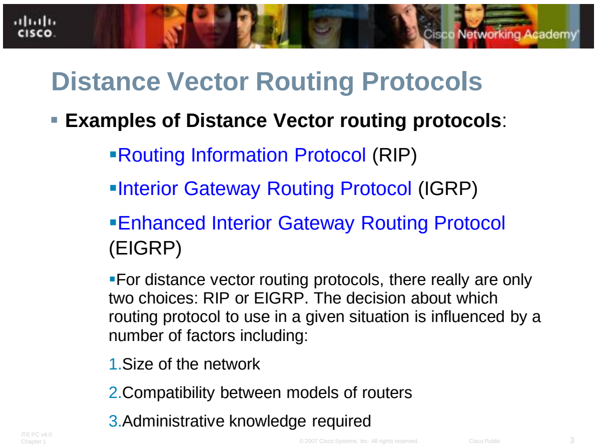
Routing Protocols and Concepts – Chapter 4

Cisco | Networking Academy®
Mind Wide Open™



Objectives

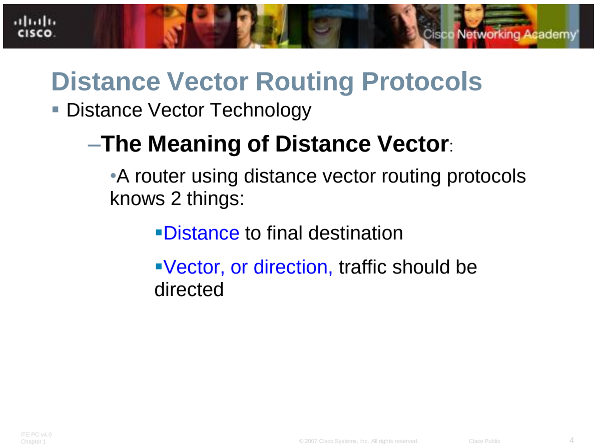
- Identify the characteristics of distance vector routing protocols.
- Describe the network discovery process of distance vector routing protocols using Routing Information Protocol (RIP).
- Describe the processes to maintain accurate routing tables used by distance vector routing protocols.
- Identify the conditions leading to a routing loop and explain the implications for router performance.
- Recognize that distance vector routing protocols are in use today



Distance Vector Routing Protocols

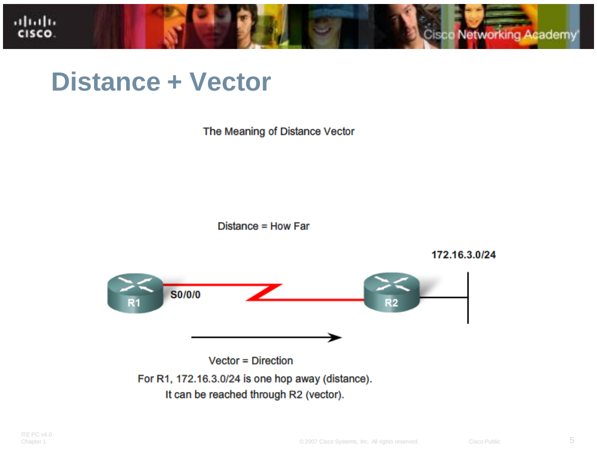
- **Examples of Distance Vector routing protocols**:
  - Routing Information Protocol (RIP)
  - Interior Gateway Routing Protocol (IGRP)
  - Enhanced Interior Gateway Routing Protocol (EIGRP)
  - For distance vector routing protocols, there really are only two choices: RIP or EIGRP. The decision about which routing protocol to use in a given situation is influenced by a number of factors including:

    1. Size of the network
    2. Compatibility between models of routers
    3. Administrative knowledge required



Distance Vector Routing Protocols

- Distance Vector Technology
  - **The Meaning of Distance Vector**:
    - A router using distance vector routing protocols knows 2 things:
      - Distance to final destination
      - Vector, or direction, traffic should be directed



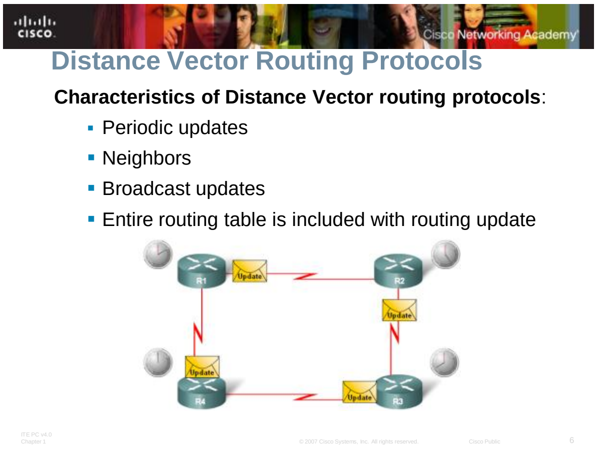
Distance + Vector

The Meaning of Distance Vector

Distance = How Far

Vector = Direction

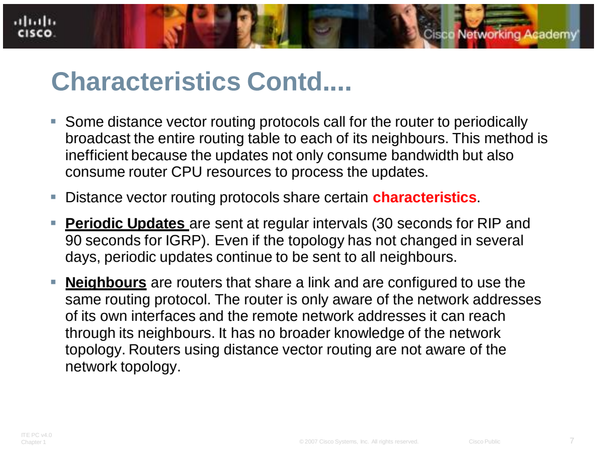
For R1, 172.16.3.0/24 is one hop away (distance).
It can be reached through R2 (vector).



Distance Vector Routing Protocols

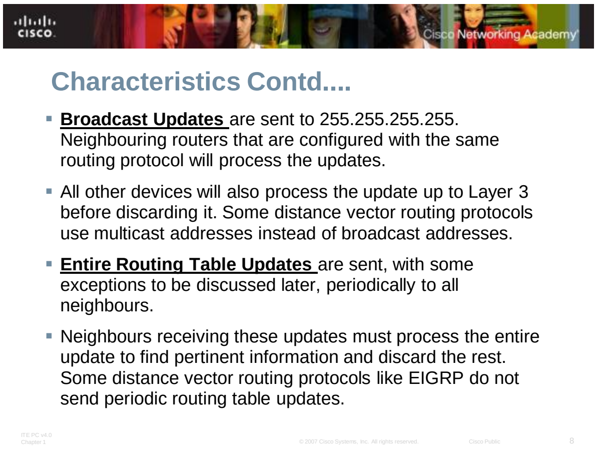
Characteristics of Distance Vector routing protocols:

- Periodic updates
- Neighbors
- Broadcast updates
- Entire routing table is included with routing update


Cisco Networking Academy

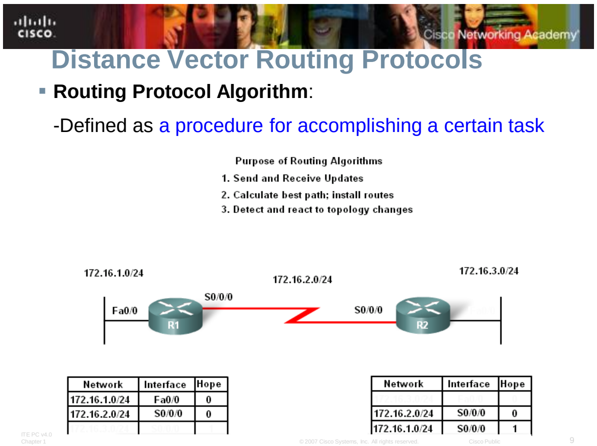
Characteristics Contd....

- Some distance vector routing protocols call for the router to periodically broadcast the entire routing table to each of its neighbours. This method is inefficient because the updates not only consume bandwidth but also consume router CPU resources to process the updates.
- Distance vector routing protocols share certain **characteristics**.
- **Periodic Updates** are sent at regular intervals (30 seconds for RIP and 90 seconds for IGRP). Even if the topology has not changed in several days, periodic updates continue to be sent to all neighbours.
- **Neighbours** are routers that share a link and are configured to use the same routing protocol. The router is only aware of the network addresses of its own interfaces and the remote network addresses it can reach through its neighbours. It has no broader knowledge of the network topology. Routers using distance vector routing are not aware of the network topology.


Cisco Networking Academy

Characteristics Contd....

- **Broadcast Updates** are sent to 255.255.255.255. Neighbouring routers that are configured with the same routing protocol will process the updates.
- All other devices will also process the update up to Layer 3 before discarding it. Some distance vector routing protocols use multicast addresses instead of broadcast addresses.
- **Entire Routing Table Updates** are sent, with some exceptions to be discussed later, periodically to all neighbours.
- Neighbours receiving these updates must process the entire update to find pertinent information and discard the rest. Some distance vector routing protocols like EIGRP do not send periodic routing table updates.



Distance Vector Routing Protocols

- **Routing Protocol Algorithm**:

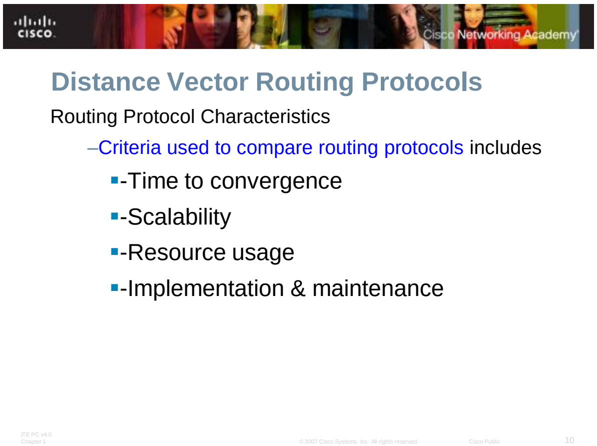
-Defined as a procedure for accomplishing a certain task

Purpose of Routing Algorithms

1. Send and Receive Updates
2. Calculate best path; install routes
3. Detect and react to topology changes

Network	Interface	Hope
172.16.1.0/24	Fa0/0	0
172.16.2.0/24	S0/0/0	0
172.16.3.0/24	S0/0/0	1

Network	Interface	Hope
172.16.3.0/24	Fa0/0	0
172.16.2.0/24	S0/0/0	0
172.16.1.0/24	S0/0/0	1

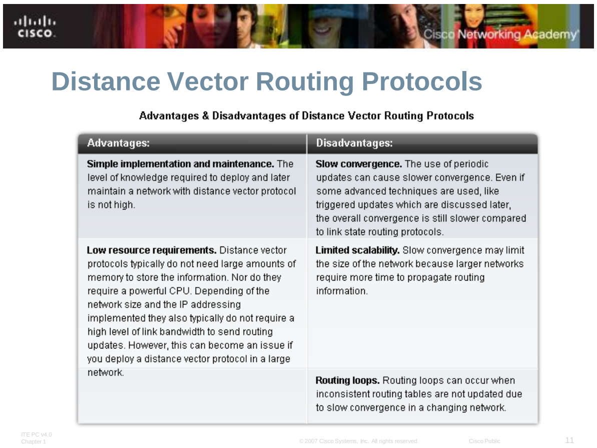


Distance Vector Routing Protocols

Routing Protocol Characteristics

–Criteria used to compare routing protocols includes

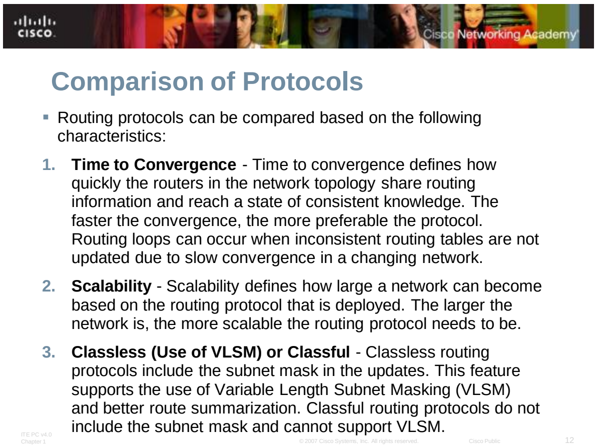
- -Time to convergence
- -Scalability
- -Resource usage
- -Implementation & maintenance



Distance Vector Routing Protocols

Advantages & Disadvantages of Distance Vector Routing Protocols

Advantages:	Disadvantages:
Simple implementation and maintenance. The level of knowledge required to deploy and later maintain a network with distance vector protocol is not high.	**Slow convergence.** The use of periodic updates can cause slower convergence. Even if some advanced techniques are used, like triggered updates which are discussed later, the overall convergence is still slower compared to link state routing protocols.
Low resource requirements. Distance vector protocols typically do not need large amounts of memory to store the information. Nor do they require a powerful CPU. Depending of the network size and the IP addressing implemented they also typically do not require a high level of link bandwidth to send routing updates. However, this can become an issue if you deploy a distance vector protocol in a large network.	**Limited scalability.** Slow convergence may limit the size of the network because larger networks require more time to propagate routing information.
	Routing loops. Routing loops can occur when inconsistent routing tables are not updated due to slow convergence in a changing network.



Comparison of Protocols

- Routing protocols can be compared based on the following characteristics:

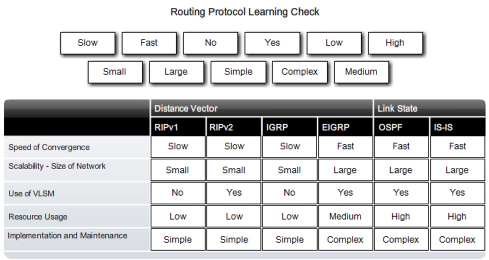
1. **Time to Convergence** - Time to convergence defines how quickly the routers in the network topology share routing information and reach a state of consistent knowledge. The faster the convergence, the more preferable the protocol. Routing loops can occur when inconsistent routing tables are not updated due to slow convergence in a changing network.
2. **Scalability** - Scalability defines how large a network can become based on the routing protocol that is deployed. The larger the network is, the more scalable the routing protocol needs to be.
3. **Classless (Use of VLSM) or Classful** - Classless routing protocols include the subnet mask in the updates. This feature supports the use of Variable Length Subnet Masking (VLSM) and better route summarization. Classful routing protocols do not include the subnet mask and cannot support VLSM.

Comparison of Protocols

4. Resource Usage - Resource usage includes the requirements of a routing protocol such as memory space, CPU utilization, and link bandwidth utilization. Higher resource requirements necessitate more powerful hardware to support the routing protocol operation in addition to the packet forwarding processes.

5. Implementation and Maintenance - Implementation and maintenance describes the level of knowledge that is required for a network administrator to implement and maintain the network based on the routing protocol deployed.

Routing Protocol Comparison



Routing Protocol Learning Check

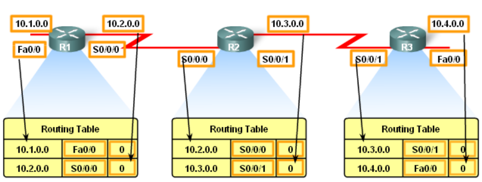
Slow
Fast
No
Yes
Low
High
Small
Large
Simple
Complex
Medium

	Distance Vector				Link State	
	RIPv1	RIPv2	IGRP	EIGRP	OSPF	IS-IS
Speed of Convergence	Slow	Slow	Slow	Fast	Fast	Fast
Scalability - Size of Network	Small	Small	Small	Large	Large	Large
Use of VLSM	No	Yes	No	Yes	Yes	Yes
Resource Usage	Low	Low	Low	Medium	High	High
Implementation and Maintenance	Simple	Simple	Simple	Complex	Complex	Complex

Network Discovery

- **Router initial start up** (Cold Starts)
  - -**Initial network discovery**
    - Directly connected networks are initially placed in routing table

Network Discovery - Cold Start



Routing Table		
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0

Routing Table		
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0

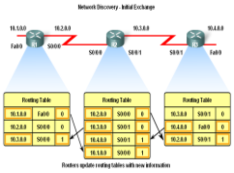
Routing Table		
10.3.0.0	S0/0/1	0
10.4.0.0	Fa0/0	0

Cold Start

- When a router cold starts or powers up, it knows nothing about the network topology. It does not even know that there are devices on the other end of its links.
- The only information that a router has is from its own saved configuration file stored in **NVRAM**. Once a router boots successfully, it applies the saved configuration.
- As described in Chapter 1 and Chapter 2, if the IP addressing is configured correctly, then the router will initially discover its own directly connected networks.
- In the example in the figure, after a cold start and before the exchange of routing information, the routers initially discover their own directly connected networks and subnet masks.
- This information is added to their routing tables.

Network Discovery

- **Initial Exchange** of Routing Information
  - –If a routing protocol is configured then
    - -Routers will exchange routing information
- Routing updates received from other routers
  - -Router checks update for new information
    - If there is new information:
      - -Metric is updated
      - -New information is
      - stored in routing table



Routing Table		
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1

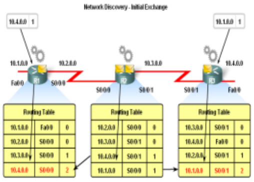
Routing Table		
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.4.0.0	S0/0/1	1
10.1.0.0	S0/0/0	1

Routing Table		
10.3.0.0	S0/0/1	0
10.4.0.0	Fa0/0	0
10.2.0.0	S0/0/1	1

Routers update routing tables with new information

Network Discovery

- **Exchange of Routing Information**
  - –**Router convergence** is reached when
    - -All routing tables in the network contain the same network information
  - –Routers continue to exchange routing information
    - -If no new information is found then Convergence is reached



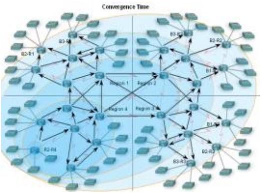
Routing Table		
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1
10.4.0.0	S0/0/0	2

Routing Table		
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.4.0.0	S0/0/1	1
10.1.0.0	S0/0/0	1

Routing Table		
10.3.0.0	S0/0/1	0
10.4.0.0	Fa0/0	0
10.2.0.0	S0/0/1	1
10.1.0.0	S0/0/1	2

Network Discovery

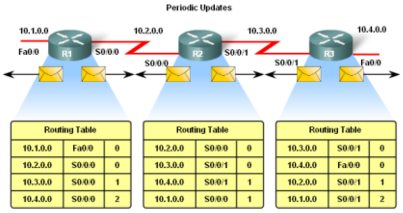
- **Convergence must be reached** before a network is considered completely operable
- Speed of achieving convergence consists of 2 interdependent categories
  - -Speed of broadcasting routing information
  - -Speed of calculating routes



Routing Table Maintenance

- **Periodic Updates**: RIPv1 & RIPv2

  These are time intervals in which a router sends out its entire routing table.



Routing Table		
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1
10.4.0.0	S0/0/0	2

Routing Table		
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.4.0.0	S0/0/1	1
10.1.0.0	S0/0/0	1

Routing Table		
10.3.0.0	S0/0/1	0
10.4.0.0	Fa0/0	0
10.2.0.0	S0/0/1	1
10.1.0.0	S0/0/1	2

Periodic Updates

- Many distance vector protocols employ periodic updates to exchange routing information with their neighbours and to maintain up-to-date routing information in the routing table. RIP and IGRP are examples of two such protocols.
- For RIP, these updates are sent every 30 seconds as a broadcast (255.255.255.255) whether or not there has been a topology change.
- This 30-second interval is a route update timer that also aids in tracking the age of routing information in the routing table.
- The age of routing information in a routing table is refreshed each time an update is received. This way information in the routing table can be maintained when there is a topology change. Changes may occur for several reasons, including:

1. Failure of a link
2. Introduction of a new link
3. Failure of a router
4. Change of link parameters

Routing Table Maintenance

- **RIP uses 4 timers**

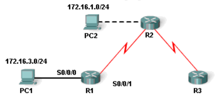
-Update timer

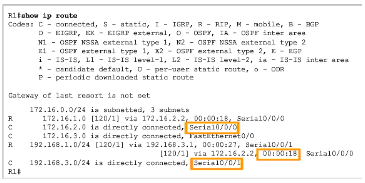
-Invalid timer

-Holddown time

-Flush timer

Verifying Timers





```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 3 subnets
R       172.16.1.0 [120/1] via 172.16.2.2, 00:00:18, Serial0/0/0
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
R    192.168.1.0/24 [120/1] via 192.168.3.1, 00:00:27, Serial0/0/1
                    [120/1] via 172.16.2.2, 00:00:18  Serial0/0/0
C    192.168.3.0/24 is directly connected, Serial0/0/1
R1#
```

Timers

1. **Invalid Timer**. If an update has not been received to refresh an existing route after 180 seconds (the default), the route is marked as invalid by setting the metric to 16. The route is retained in the routing table until the flush timer expires.
2. **Flush Timer**. By default, the flush timer is set for 240 seconds, which is 60 seconds longer than the invalid timer. When the flush timer expires, the route is removed from the routing table.
3. **Holddown Timer**. This timer stabilizes routing information and helps prevent routing loops during periods when the topology is converging on new information. Once a route is marked as unreachable, it must stay in holddown long enough for all routers in the topology to learn about the unreachable network. By default, the holddown timer is set for 180 seconds..

Routing Table Maintenance

- **Bounded Updates: EIGRP**
- EIRPG routing updates are

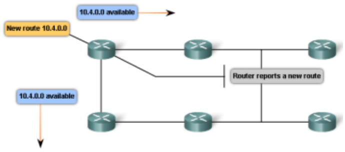
-Partial updates

-Triggered by topology changes

-Bounded

-Non periodic

Bounded Updates: EIGRP



Note on EIGRP Updates

- EIGRP uses updates that are:

1. Non-periodic because they are not sent out on a regular basis.
2. Partial updates sent only when there is a change in topology that influences routing information.
3. Bounded, meaning the propagation of partial updates are automatically bounded so that only those routers that need the information are updated.

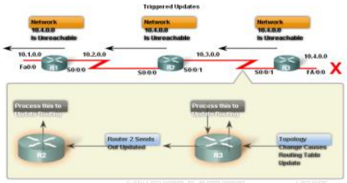
Routing Table Maintenance

- **Triggered Updates**
  - –Conditions in which triggered updates are sent

    -Interface changes state

    -Route becomes unreachable

    -Route is placed in routing table


Triggered Updates
Network 10.4.0.0 Is Unreachable
Network 10.4.0.0 Is Unreachable
Network 10.4.0.0 Is Unreachable
10.1.0.0
10.2.0.0
10.3.0.0
10.4.0.0
Fa0/0
R1
S0/0/0
S0/0/0
R2
S0/0/1
S0/0/1
R3
FA0/0
X
Process this to Update Routing
Process this to Update Routing
R2
Router 2 Sends Out Updated
R3
Topology Change Causes Routing Table Update

Problems with Triggered Updates

- Using only triggered updates would be sufficient if there were a guarantee that the wave of updates would reach every appropriate router immediately. However, there are **two problems** with triggered updates:

1. Packets containing the update message can be dropped or corrupted by some link in the network.
2. The triggered updates do not happen instantaneously. It is possible that a router that has not yet received the triggered update will issue a regular update at just the wrong time, causing the bad route to be reinserted in a neighbour that had already received the triggered update.

Routing Table Maintenance

- **Random Jitter**

  Synchronized updates

  A condition where multiple routers on multi access LAN segments transmit routing updates at the same time.

  - Problems with synchronized updates

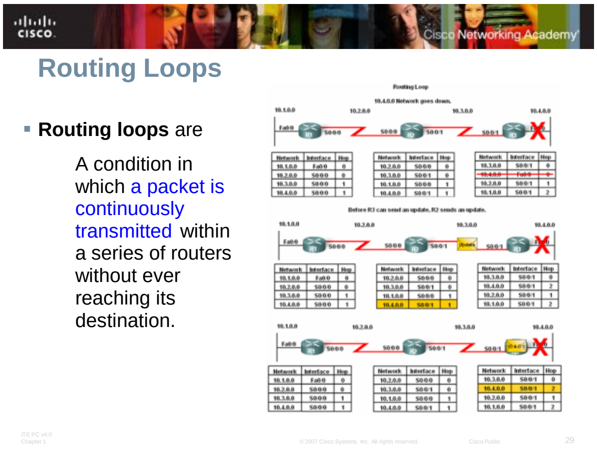
    -Bandwidth consumption

    -Packet collisions

  - Solution to problems with synchronized updates

  - Used of random variable called RIP_JITTER

(which subtracts a variable amount of time to the update interval for each router in the network. This random jitter, or variable amount of time, ranges from 0% to 15% of the specified update interval. In this way, the update interval varies randomly in a range from 25 to 30 seconds for the default 30-second interval.)



Routing Loops

- **Routing loops** are

  A condition in which a packet is continuously transmitted within a series of routers without ever reaching its destination.

Routing Loop

10.4.0.0 Network goes down.

10.1.0.0
10.2.0.0
10.3.0.0
10.4.0.0
Fa0/0
S0/0/0
S0/0/0
S0/0/1
S0/0/1
Fa0/0
R1
R2
R3

Network	Interface	Hop
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1
10.4.0.0	S0/0/0	1

Network	Interface	Hop
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	1

Network	Interface	Hop
10.3.0.0	S0/0/1	0
~~10.4.0.0~~	~~Fa0/0~~	~~0~~
10.2.0.0	S0/0/1	1
10.1.0.0	S0/0/1	2

Before R3 can send an update, R2 sends an update.

Network	Interface	Hop
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1
10.4.0.0	S0/0/0	1

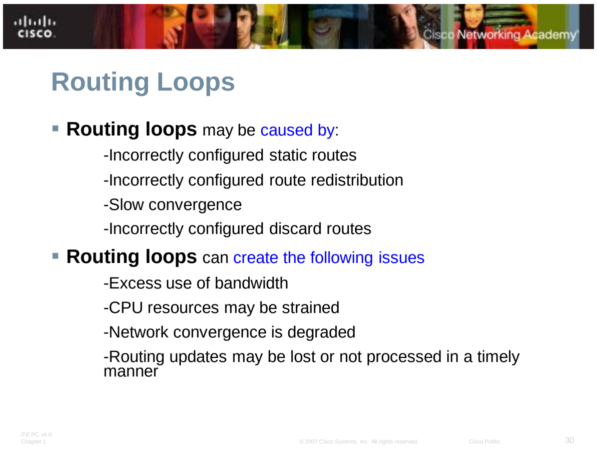
Network	Interface	Hop
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	1

Network	Interface	Hop
10.3.0.0	S0/0/1	0
10.4.0.0	S0/0/1	2
10.2.0.0	S0/0/1	1
10.1.0.0	S0/0/1	2

Network	Interface	Hop
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1
10.4.0.0	S0/0/0	1

Network	Interface	Hop
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	1

Network	Interface	Hop
10.3.0.0	S0/0/1	0
10.4.0.0	S0/0/1	2
10.2.0.0	S0/0/1	1
10.1.0.0	S0/0/1	2



Routing Loops

- **Routing loops** may be caused by:

  -Incorrectly configured static routes

  -Incorrectly configured route redistribution

  -Slow convergence

  -Incorrectly configured discard routes

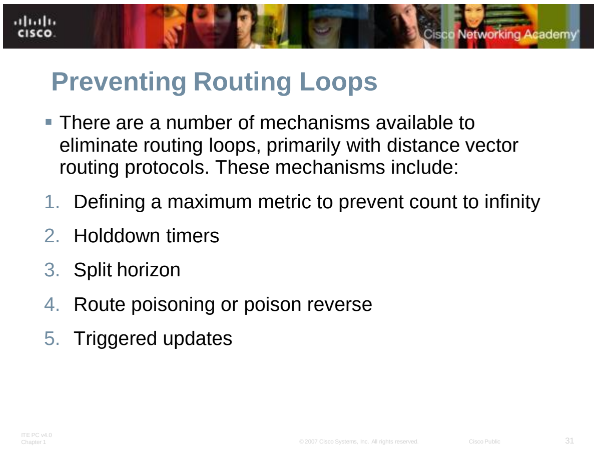
- **Routing loops** can create the following issues

  -Excess use of bandwidth

  -CPU resources may be strained

  -Network convergence is degraded

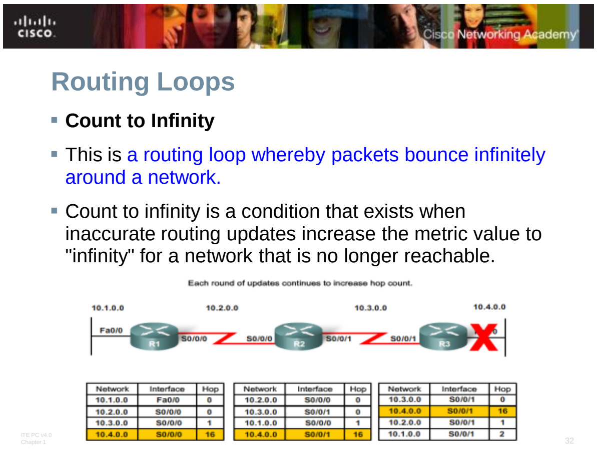
  -Routing updates may be lost or not processed in a timely manner



Preventing Routing Loops

- There are a number of mechanisms available to eliminate routing loops, primarily with distance vector routing protocols. These mechanisms include:

1. Defining a maximum metric to prevent count to infinity
2. Holddown timers
3. Split horizon
4. Route poisoning or poison reverse
5. Triggered updates



Routing Loops

- **Count to Infinity**
- This is a routing loop whereby packets bounce infinitely around a network.
- Count to infinity is a condition that exists when inaccurate routing updates increase the metric value to "infinity" for a network that is no longer reachable.

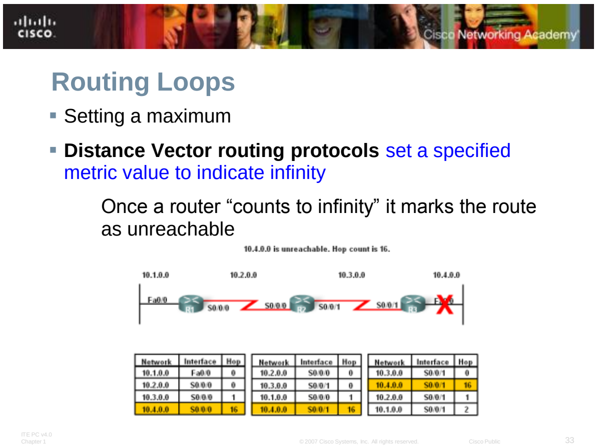
Each round of updates continues to increase hop count.

10.1.0.0
10.2.0.0
10.3.0.0
10.4.0.0
Fa0/0
S0/0/0
S0/0/0
S0/0/1
S0/0/1
R1
R2
R3

Network	Interface	Hop
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1
10.4.0.0	S0/0/0	16

Network	Interface	Hop
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	16

Network	Interface	Hop
10.3.0.0	S0/0/1	0
10.4.0.0	S0/0/1	16
10.2.0.0	S0/0/1	1
10.1.0.0	S0/0/1	2



Routing Loops

- Setting a maximum
- **Distance Vector routing protocols** set a specified metric value to indicate infinity

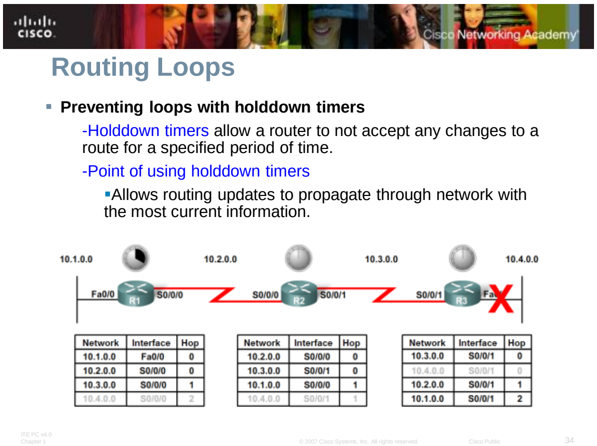
  Once a router "counts to infinity" it marks the route as unreachable

10.4.0.0 is unreachable. Hop count is 16.

Network	Interface	Hop
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1
10.4.0.0	S0/0/0	16

Network	Interface	Hop
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	16

Network	Interface	Hop
10.3.0.0	S0/0/1	0
10.4.0.0	S0/0/1	16
10.2.0.0	S0/0/1	1
10.1.0.0	S0/0/1	2



Routing Loops

- **Preventing loops with holddown timers**

  -Holddown timers allow a router to not accept any changes to a route for a specified period of time.

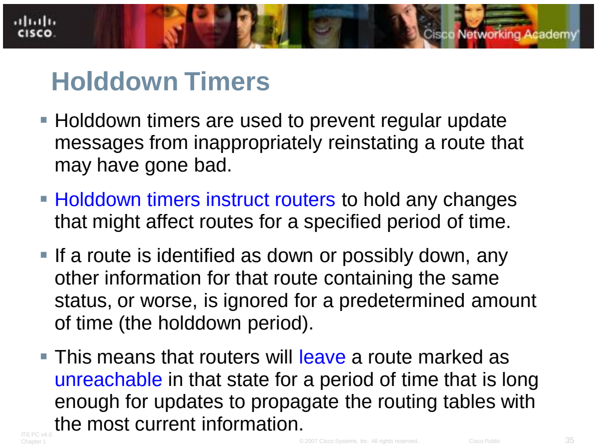
  -Point of using holddown timers

  - Allows routing updates to propagate through network with the most current information.

Network	Interface	Hop
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1
10.4.0.0	S0/0/0	2

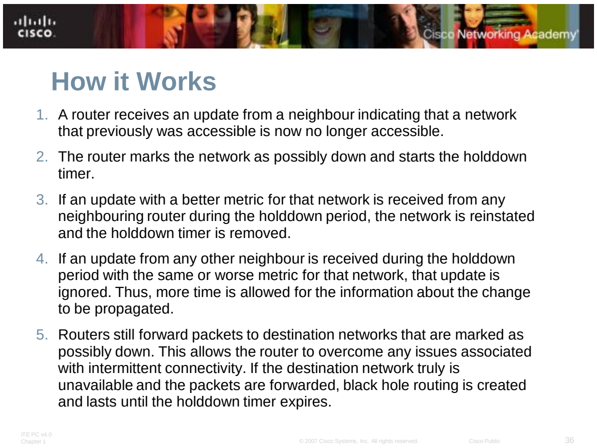
Network	Interface	Hop
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	1

Network	Interface	Hop
10.3.0.0	S0/0/1	0
10.4.0.0	S0/0/1	0
10.2.0.0	S0/0/1	1
10.1.0.0	S0/0/1	2


Cisco Networking Academy

Holddown Timers

- Holddown timers are used to prevent regular update messages from inappropriately reinstating a route that may have gone bad.
- Holddown timers instruct routers to hold any changes that might affect routes for a specified period of time.
- If a route is identified as down or possibly down, any other information for that route containing the same status, or worse, is ignored for a predetermined amount of time (the holddown period).
- This means that routers will leave a route marked as unreachable in that state for a period of time that is long enough for updates to propagate the routing tables with the most current information.


Cisco Networking Academy

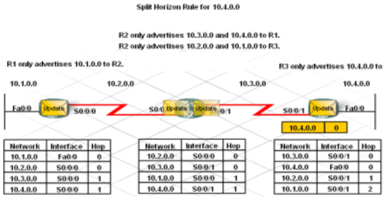
How it Works

1. A router receives an update from a neighbour indicating that a network that previously was accessible is now no longer accessible.
2. The router marks the network as possibly down and starts the holddown timer.
3. If an update with a better metric for that network is received from any neighbouring router during the holddown period, the network is reinstated and the holddown timer is removed.
4. If an update from any other neighbour is received during the holddown period with the same or worse metric for that network, that update is ignored. Thus, more time is allowed for the information about the change to be propagated.
5. Routers still forward packets to destination networks that are marked as possibly down. This allows the router to overcome any issues associated with intermittent connectivity. If the destination network truly is unavailable and the packets are forwarded, black hole routing is created and lasts until the holddown timer expires.

Routing Loops

- The **Split Horizon Rule** is used to prevent routing loops
- **Split Horizon rule**:

  A router should not advertise a network through the interface from which the update came.



Split Horizon Rule for 10.4.0.0

R2 only advertises 10.3.0.0 and 10.4.0.0 to R1.
R2 only advertises 10.2.0.0 and 10.1.0.0 to R3.

R1 only advertises 10.1.0.0 to R2.

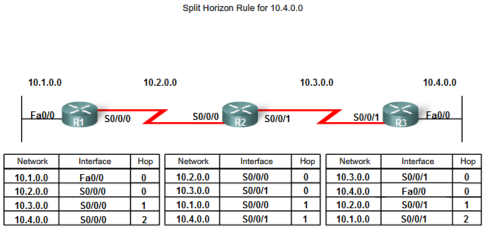
R3 only advertises 10.4.0.0 to R2.

Network	Interface	Hop
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1
10.4.0.0	S0/0/0	1

Network	Interface	Hop
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	1

Network	Interface	Hop
10.3.0.0	S0/0/1	0
10.4.0.0	Fa0/0	0
10.2.0.0	S0/0/1	1
10.1.0.0	S0/0/1	2

Split Horizon Example



Split Horizon Rule for 10.4.0.0

Network	Interface	Hop
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1
10.4.0.0	S0/0/0	2

Network	Interface	Hop
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	1

Network	Interface	Hop
10.3.0.0	S0/0/1	0
10.4.0.0	Fa0/0	0
10.2.0.0	S0/0/1	1
10.1.0.0	S0/0/1	2

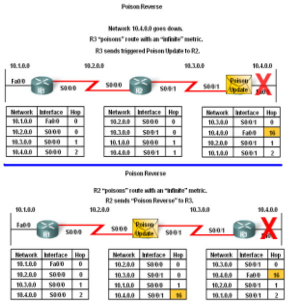
How it Works

- R3 advertises the 10.4.0.0 network to R2.
- R2 receives the information and updates its routing table.
- R2 then advertises the 10.4.0.0 network to R1 out S0/0/0. R2 does not advertise 10.4.0.0 to R3 out S0/0/1, because the route originated from that interface.
- R1 receives the information and updates its routing table.
- Because of split horizon, R1 also does not advertise the information about network 10.4.0.0 back to R2.
- **Complete routing updates are exchanged, with the exception of routes that violate the split horizon rule. The results look like this:**
- R2 advertises networks 10.3.0.0 and 10.4.0.0 to R1.
- R2 advertises networks 10.1.0.0 and 10.2.0.0 to R3.
- R1 advertises network 10.1.0.0 to R2.
- R3 advertises network 10.4.0.0 to R2.

Routing Loops

- **Split horizon with poison reverse**

  The rule states that once a router learns of an unreachable route through an interface, advertise it as unreachable back through the same interface



Poison Reverse

Network 10.4.0.0 goes down.
R3 "poisons" route with an "infinite" metric.
R3 sends triggered Poison Update to R2.

Network	Interface	Hop
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1
10.4.0.0	S0/0/0	2

Network	Interface	Hop
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	1

Network	Interface	Hop
10.3.0.0	S0/0/1	0
10.4.0.0	Fa0/0	16
10.2.0.0	S0/0/1	1
10.1.0.0	S0/0/1	2

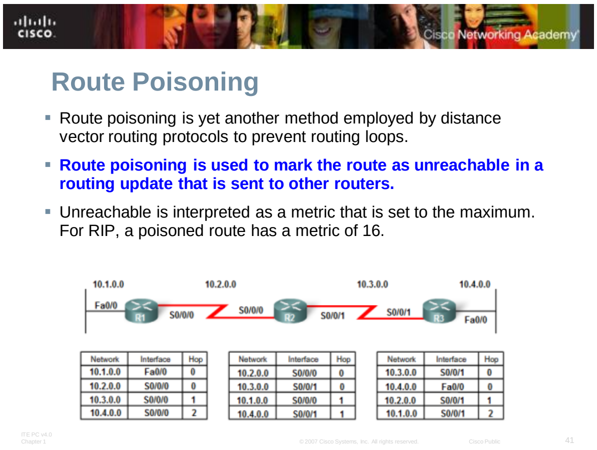
Poison Reverse

R2 "poisons" route with an "infinite" metric.
R2 sends "Poison Reverse" to R3.

Network	Interface	Hop
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1
10.4.0.0	S0/0/0	2

Network	Interface	Hop
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	16

Network	Interface	Hop
10.3.0.0	S0/0/1	0
10.4.0.0	Fa0/0	16
10.2.0.0	S0/0/1	1
10.1.0.0	S0/0/1	2



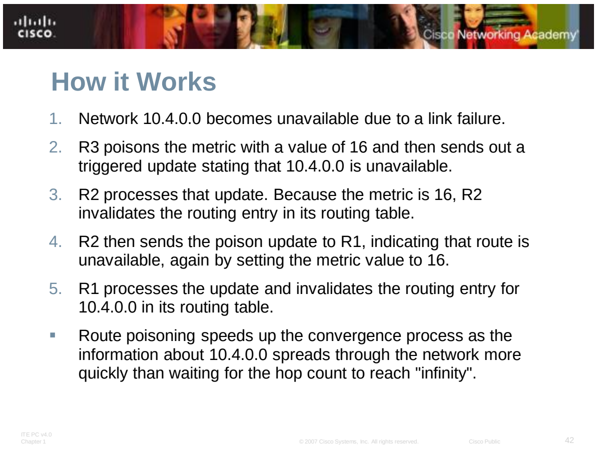
Route Poisoning

- Route poisoning is yet another method employed by distance vector routing protocols to prevent routing loops.
- **Route poisoning is used to mark the route as unreachable in a routing update that is sent to other routers.**
- Unreachable is interpreted as a metric that is set to the maximum. For RIP, a poisoned route has a metric of 16.

Network	Interface	Hop
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1
10.4.0.0	S0/0/0	2

Network	Interface	Hop
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	1

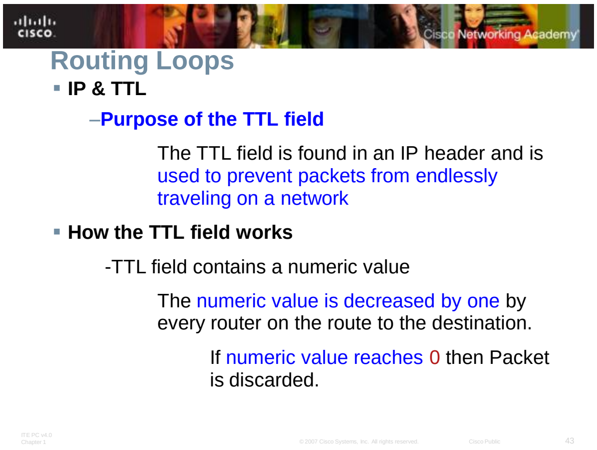
Network	Interface	Hop
10.3.0.0	S0/0/1	0
10.4.0.0	Fa0/0	0
10.2.0.0	S0/0/1	1
10.1.0.0	S0/0/1	2



How it Works

1. Network 10.4.0.0 becomes unavailable due to a link failure.
2. R3 poisons the metric with a value of 16 and then sends out a triggered update stating that 10.4.0.0 is unavailable.
3. R2 processes that update. Because the metric is 16, R2 invalidates the routing entry in its routing table.
4. R2 then sends the poison update to R1, indicating that route is unavailable, again by setting the metric value to 16.
5. R1 processes the update and invalidates the routing entry for 10.4.0.0 in its routing table.

- Route poisoning speeds up the convergence process as the information about 10.4.0.0 spreads through the network more quickly than waiting for the hop count to reach "infinity".



Routing Loops

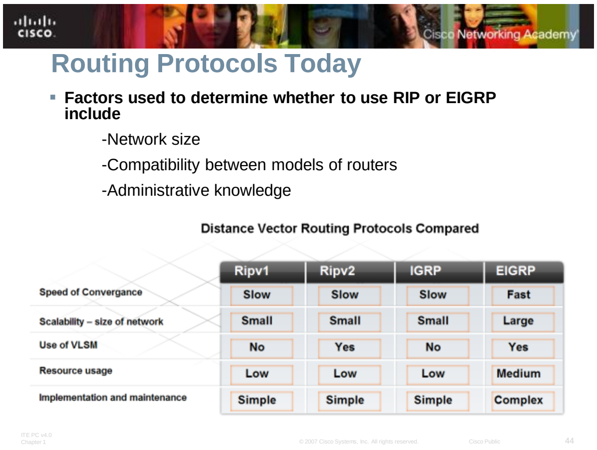
- **IP & TTL**
  - –**Purpose of the TTL field**

    The TTL field is found in an IP header and is used to prevent packets from endlessly traveling on a network
- **How the TTL field works**

  -TTL field contains a numeric value

  The numeric value is decreased by one by every router on the route to the destination.

  If numeric value reaches 0 then Packet is discarded.



Routing Protocols Today

- **Factors used to determine whether to use RIP or EIGRP include**

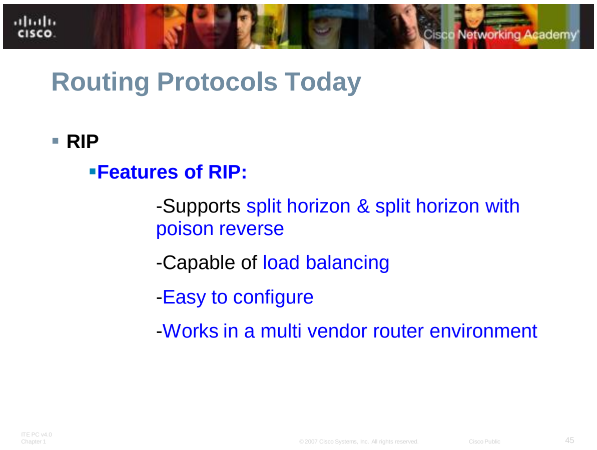
  -Network size

  -Compatibility between models of routers

  -Administrative knowledge

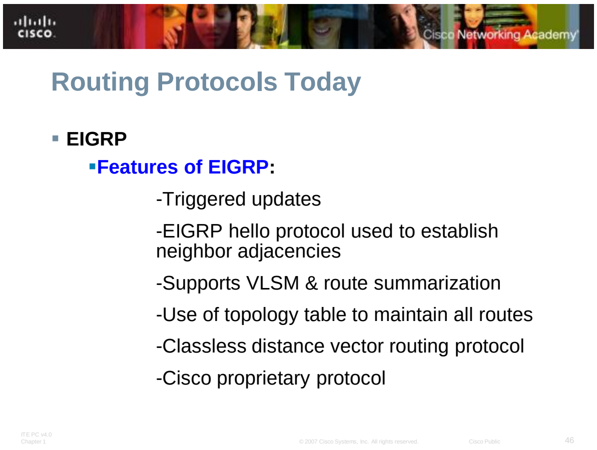
Distance Vector Routing Protocols Compared

	Ripv1	Ripv2	IGRP	EIGRP
Speed of Convergance	Slow	Slow	Slow	Fast
Scalability – size of network	Small	Small	Small	Large
Use of VLSM	No	Yes	No	Yes
Resource usage	Low	Low	Low	Medium
Implementation and maintenance	Simple	Simple	Simple	Complex



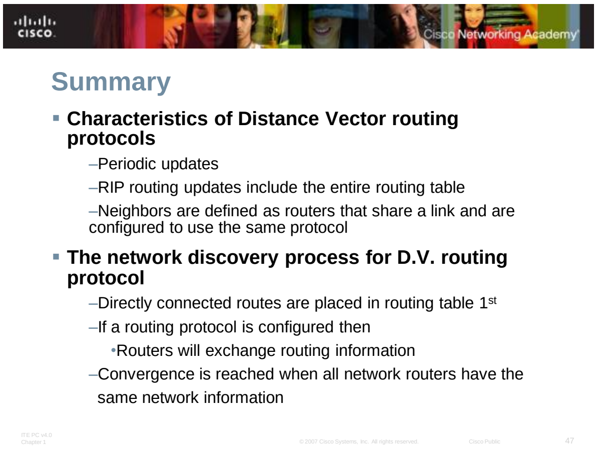
Routing Protocols Today

- **RIP**
  - **Features of RIP:**
    - -Supports split horizon & split horizon with poison reverse
    - -Capable of load balancing
    - -Easy to configure
    - -Works in a multi vendor router environment



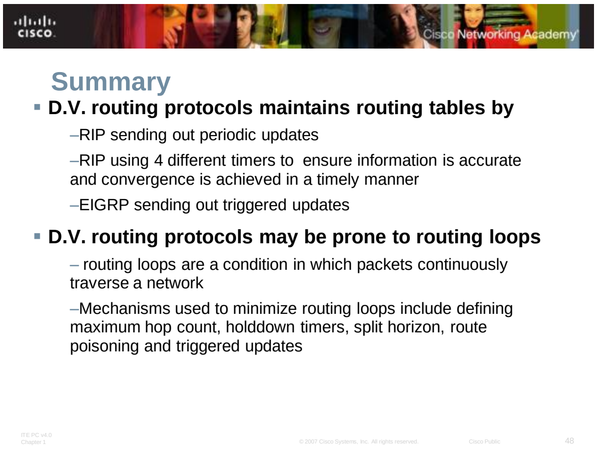
Routing Protocols Today

- **EIGRP**
  - **Features of EIGRP:**
    - -Triggered updates
    - -EIGRP hello protocol used to establish neighbor adjacencies
    - -Supports VLSM & route summarization
    - -Use of topology table to maintain all routes
    - -Classless distance vector routing protocol
    - -Cisco proprietary protocol



Summary

- **Characteristics of Distance Vector routing protocols**
  - –Periodic updates
  - –RIP routing updates include the entire routing table
  - –Neighbors are defined as routers that share a link and are configured to use the same protocol
- **The network discovery process for D.V. routing protocol**
  - –Directly connected routes are placed in routing table 1st
  - –If a routing protocol is configured then
    - •Routers will exchange routing information
  - –Convergence is reached when all network routers have the same network information



Summary

- **D.V. routing protocols maintains routing tables by**
  - –RIP sending out periodic updates
  - –RIP using 4 different timers to ensure information is accurate and convergence is achieved in a timely manner
  - –EIGRP sending out triggered updates
- **D.V. routing protocols may be prone to routing loops**
  - – routing loops are a condition in which packets continuously traverse a network
  - –Mechanisms used to minimize routing loops include defining maximum hop count, holddown timers, split horizon, route poisoning and triggered updates

Summary

- **Conditions that can lead to routing loops include**
  - –Incorrectly configured static routes
  - –Incorrectly configured route redistribution
  - –Slow convergence
  - –Incorrectly configured discard routes
- **How routing loops can impact network performance includes:**
  - –Excess use of bandwidth
  - –CPU resources may be strained
  - –Network convergence is degraded
  - –Routing updates may be lost or not processed

Summary

- **Routing Information Protocol (RIP)**

  A distance vector protocol that has 2 versions

  RIPv1 – a classful routing protocol

  RIPv2 - a classless routing protocol
- **Enhanced Interior Gateway Routing Protocol (EIGRP)**
  - –A distance vector routing protocols that has some features of link state routing protocols
  - –A Cisco proprietary routing protocol

CISCO