Philip Heimer

Halmstad University

- Characteristics, operations, and functionality of distance vector routing protocols
- Types of distance vector routing protocols
- RIP (version 1 and 2)
- EIGRP

- Routes are advertised as vectors of distance and direction
- Distance is defined in terms of a metric (hop count...)
- Direction is the next-hop router or exit interface

- The router does not have the knowledge of the entire path to the destination network, but it knows:
  - The direction or interface in which packets should be forwarded
  - The distance or how far it is to the destination network

Characteristics of Distance Vector Protocols

- Periodic updates
  - Sent at regular intervals
- Neighbors
  - Routers that share a link and are configured to use the same routing protocol
- Broadcast updates
- Entire routing table is included in routing updates

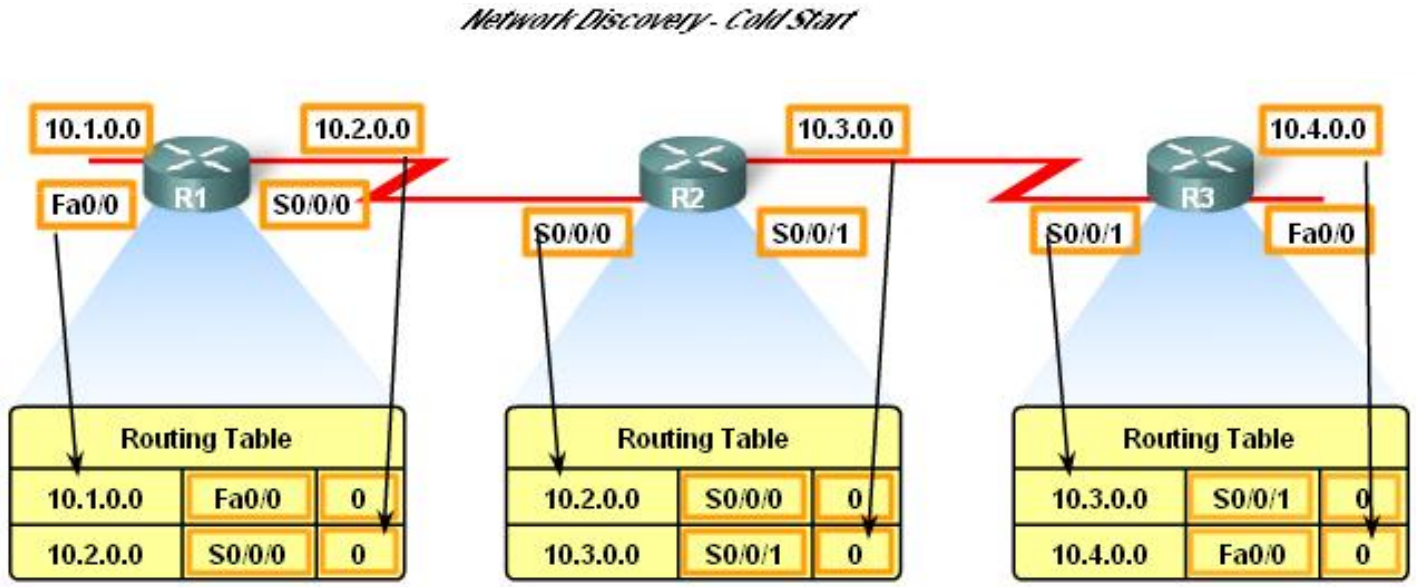
Advantages:

- Simple implementation and maintenance
- Low resource requirements (memory, CPU)

Disadvantages:

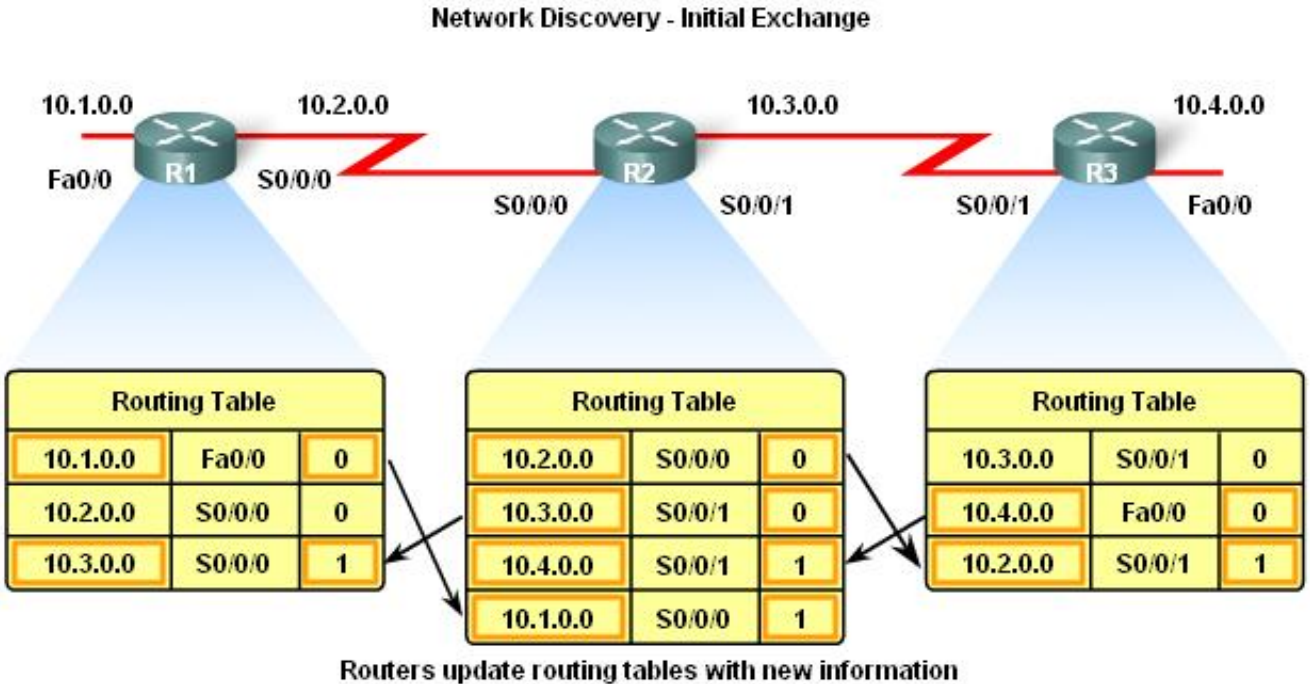
- Slow convergence (periodic updates)
- Limited scalability
- Routing loops (due to slow convergence)

- Directly connected networks are initially placed in routing table

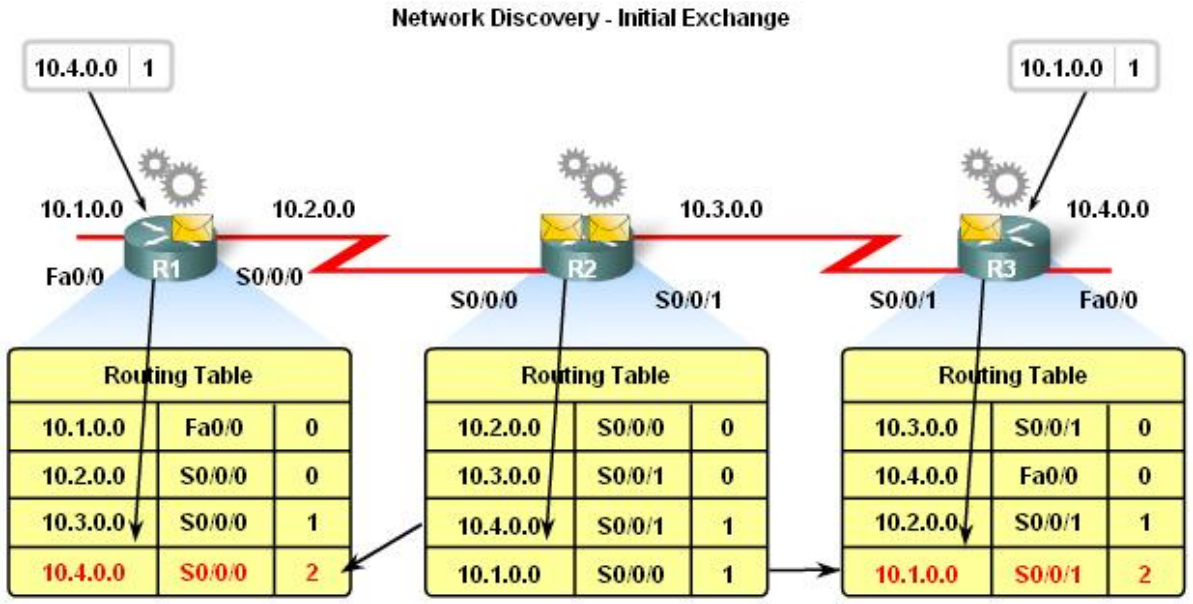


Initial Exchange of Routing Information

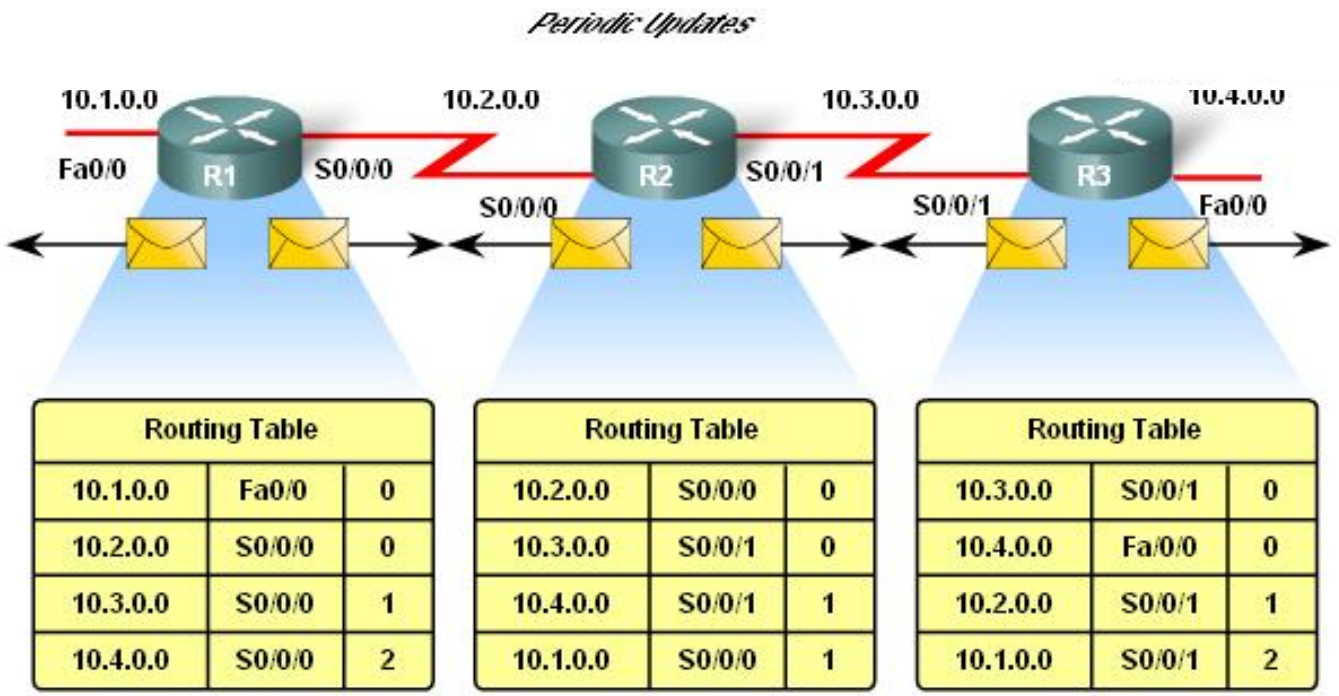
- If a routing protocol is configured, then routers will exchange routing information
- Metric is updated for new information



- Routers continue to exchange routing information
- Convergence is reached if no new information is found, and all routing tables contain the same network information



- Periodic updates
  - Time intervals in which a router sends out its entire routing table



- It is a condition in which a packet is continuously transmitted within a series of routers without ever reaching its intended destination network
- May be a result of:
  - Incorrect configured static routes
  - Incorrect configured redistribution
  - Inconsistent routing tables not being updated due to slow convergence
  - Incorrectly configured or installed discarded routes

- Can have a devastating effect on a network, resulting in degraded network performance or downtime
- Link bandwidth can be used for traffic looping back and forth between routers
- Routing updates may get lost, and additional loops can appear
- Router CPU will be strained due to looping packets

Available mechanisms to eliminate routing loops:

- Defining a maximum metric
- Holddown timers
- Split horizon
- Route poisoning or poison reverse
- Triggered updates

- 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
- Can be prevented by setting a maximum metric value, and route will be marked as unreachable when value reached

Count to Infinity

Each round of updates continues to increase hop count.

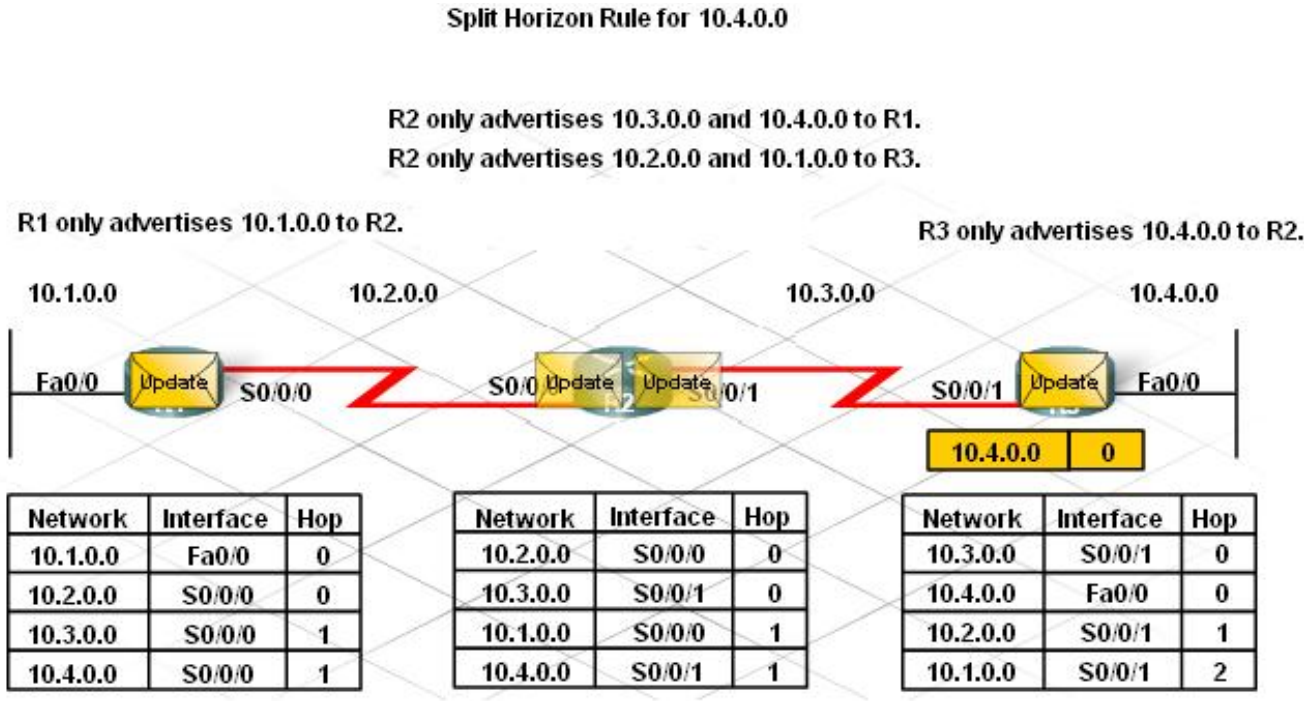
Network	Interface	Hop
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1
10.4.0.0	S0/0/0	24

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	23

Network	Interface	Hop
10.3.0.0	S0/0/1	0
10.4.0.0	S0/0/1	22
10.2.0.0	S0/0/1	1
10.1.0.0	S0/0/1	2

- Used to prevent regular update messages in instable networks (route flapping up and down)
- Start the holddown timer before the route is removed from the routing table, and mark the network as possibly down
- Holddown time is long enough for updates to propagate the routing tables with the most current information

- A technique used to prevent routing loops
- A router should never advertise a network through the interface from which the update came



- Used to mark a route as unreachable in a routing update sent to other routers
- The metric is set to the maximum value, which speeds up the convergence process. Does not need to wait until the metric reaches ”Infinity”

- “The poison reverse is an acknoledgment of reception of route
poisoning. And ALL routers on the segment connected to the router
issuing route poison MUST send back a poison reverse. If the routers
dont send poison reverse, this means that the router has lost the
right way to reach the dead network. This is considered neccessary in
distance vector protocols because they don't see the full scope of the
network. “

- Used to speed up the convergence
- Routing update, sent immediately after a routing change
- Sent if
  - An interface changes state (up or down)
  - A route has entered the unreachable state
  - A route is installed in the routing table

Problems with triggered updates:

- Packets containing the update message can be dropped or corrupted
- A router can send a regular update before the triggered update is received, which cause the bad route to be re-inserted in the routing table

- RIP
- IGRP (not used anymore)
- EIGRP

Decisions about which to use depends by a number of factors:

  - Size of network
  - Compatibility between models of routers
  - Administrative knowledge required

- A standardized routing protocol that works in a mixed vendor router environment
- Characteristics of RIP
  - Mature
  - Stable
  - Widely supported
  - Easy to configure

- Metric = hop count
- Maximum 16 hops. Advertised routes with hop counts greater than 15 are unreachable
- Updates broadcasted every 30 seconds
- RIP v1 is classfull
- Has a default administrative distance (AD) of 120
- Compared to other routing protocols, RIP is the least preferred. All other protocols has lower default AD values

- Classful
  - No subnet mask information in updates
  - Does not support VLSM
- Broadcasts routing updates
- Does not support authentication

- Addition of Subnet mask
  - VLSM
  - Classless routing
- Authentication for routing updates
- Next hop IP address
- Supports manual route summarization
- Multicasting RIP v2 routing updates
  - Class D address: 224.0.0.9

- Distance vector protocol
  - Metric = hop count
  - Infinite distance = 16 hops
- Holddown timers
  - Prevents routing loops
  - Default = 180 s
- Split horizon
  - Prevents routing loops

- Proprietary protocol developed by Cisco
- Enhancement of IGRP
  - Main purpose to create a classless version of IGRP
- Distance vector protocol
- Some features from link-state routing protocols

Includes some features that are not commonly found in other distance vector protocols

- Reliable Transport Protocol – RTP
- Bounded updates
- Diffusing Update Algorithm - DUAL
- Establishing adjacencies
- Neighbor and Topology tables

- Metrics
  - Bandwidth (default)
  - Delay (default)
  - Reliability (optional)
  - Load (optional)

- Diffusing Update Algorithm – DUAL
- No periodic updates needed
- Update when topology changes
  - Fast convergence
- Hello protocol to find neighbors
- Update directly connected neighbors with vectors of distances

- DUAL maintains a topology table including best path and backup path to destination networks
- If a route becomes unavailable, DUAL will search its topology table for a backup route
  - If a backup route exists, it will be inserted in the routing table immediately
  - If a backup route not exist, DUAL performs a network discovery process

- Successor
  - The neighboring router used for packet forwarding with the least cost to the destination network
  - Inserted in the routing table
- Feasible successor
  - The backup route (in topology table)
- Feasible distance
  - The lowest calculated metric to reach the destination network

- EIGRP can route several different routed protocols (IP, IPX, AppleTalk)
- PDMs are responsible for the specific routing tasks for each Network layer protocol
- Builds one separate neighbor, topology and routing table for each Network layer protocol

- EIGRP is independent of the Network layer protocol, and can not use services of UDP and TCP
- RTP is used for the delivery and reception of EIGRP packets
- Supports both reliable and unreliable delivery, similar to TCP and UDP

- Not periodic updates. Only send updates when the metric for a route changes
- Bounded/partial updates
  - Only sent to the routers that are affected by the change
  - The update only includes information about the route changes
- Minimizes the bandwidth required to send EIGRP packets