**CCNA **

640-802

**IP ROUTING**







Revision no.: PPT/2K804/04

Revision no.: PPT/2K804/04



# Routing Basics

* The term routing is used for taking a packet from one device and sending it through the network to another device on a different network.
* Routers route traffic to all the networks in your internetwork. To be able to route packets, a router must know, at a minimum, the following:



* + Destination address
  + Neighbor routers from which it can learn about remote networks
  + Possible routes to all remote networks
  + The best route to each remote network
  + How to maintain and verify routing information



Revision no.: PPT/2K804/04



**Routing Basics (contd.)**

## The router learns about remote networks from neighbor routers or from an administrator.

* The router then builds a routing table that describes how to find the remote networks.



* If a network is directly connected, then the router already knows how to get to it.
* If a network isn’t connected, the router must learn how to get to the remote network in two ways by using static routing, or dynamic routing.



Revision no.: PPT/2K804/04



**Routing Basics (contd.)**

## Static Routing: The administrator must hand-type all network locations into the routing table.

* + In Static Routing, the administrator is responsible for updating all changes by hand into all routers.



## Dynamic Routing: Dynamic routing is the process of routing protocols running on the router communicating with neighbor routers.

* + If a change occurs in the network the dynamic routing protocols automatically inform all routers about the change.



Revision no.: PPT/2K804/04

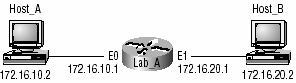


# The IP Routing Process

## The IP routing process is fairly simple and doesn’t change regardless of the size of the network.



* Fig. Explains connecting two networks through a router.





Revision no.: PPT/2K804/04



# Static Route Configuration

* Router(config)#**ip route** *network* **[***mask***]**

{*address* | *interface*}**[***distance***] [permanent]**



* **Defines a path to an IP destination network or subnet or host**
  + **ip route** The command used to create the static route.
  + ***destination\_network*** The network you’re placing in the routing table.
  + ***mask*** The subnet mask being used on the network.
  + ***next-hop\_address*** The address of the next-hop router that will receive the packet and forward it to the remote network. This is a router interface that’s on a directly connected network.
  + ***exitinterface*** You can use it in place of the next-hop address if you want, but it’s got to be on a point-to-point link, such as a WAN. This command won’t work on a LAN such as Ethernet.
  + ***administrative\_distance*** By default, static routes have an administrative distance of 1 (or even 0 is you use an exit interface instead of a next hop address). You can change the default.
  + **Permanent** Permanent option keeps the entry in the routing table no matter what happens.



Revision no.: PPT/2K804/04



# Default Routing

## The default routing sends packets to remote destination network when not found in the routing table to the next- hop router.

* ip route 0.0.0.0 0.0.0.0 [ip of next-hop router]





Revision no.: PPT/2K804/04



# Dynamic Routing

## Dynamic routing is when protocols are used to find networks and update routing tables on routers.

* A routing protocol defines the set of rules used by a router when it communicates routing information between neighbor routers.



* Once the path is determined, a router can route a routed protocol



Revision no.: PPT/2K804/04



# Routing Protocol Basics

## Administrative Distances

* + The administrative distance (AD) is used to rate the trustworthiness of routing information received on a router from a neighbor router.



## Default Administrative Distances

* + Route Source Default AD
  + Connected interface 0
  + Static route 1
  + EIGRP 90
  + IGRP 100
  + OSPF 110
  + RIP 120
  + External EIGRP 170
  + Unknown 255 (this route will never be used)



Revision no.: PPT/2K804/04



# Classes of Routing Protocols

* There are Three classes of routing protocols
  + Distance Vector



* + - The distance vector routing approach determines the direction (vector) and distance to any link in the internetwork. Example is RIP & IGRP.
  + Link State
    - The link-state (also called shortest path first) approach recreates the exact topology of the entire internetwork for route computation. Examples are OSPF & NLSP.
  + Balanced Hybrid
    - A balanced hybrid approach combines aspects of the link-state and distance vector algorithms. An example would be EIGRP.



Revision no.: PPT/2K804/04



# Distance-Vector Routing Protocols

## The distance-vector routing algorithm passes complete routing tables to neighbor routers.

* The neighbor routers then combine the received routing table with their own routing tables to complete the internetwork map.



* This is called routing by rumor, because a router receiving an update from a neighbor router believes the information about remote networks without actually finding out for itself.
* It is possible to have a network that has multiple links to the same remote network. If that is the case, the administrative distance is first checked.
* If the administrative distance is the same, it will have to use other metrics to determine the best path to use to that remote network.



Revision no.: PPT/2K804/04



# Distance-Vector Routing Protocols (contd.)

* RIP uses only hop count to determine the best path to an internetwork.



* If RIP finds more than one link to the same remote network with the same hop count, it will automatically perform a round-robin load balance.
* RIP can perform load balancing for up to six equal-cost links.
* The problem arises when the two links to a remote network are different bandwidths but the same hop counts.



Revision no.: PPT/2K804/04



# Routing Metrics

Hop Count: Number of routers through which a packet will pass Ticks: Delay on a data link using IBM PC clock ticks

(approximately 55 milliseconds)



Cost: Arbitrary value, usually based on bandwidth, dollar expense, or another measurement, that may be assigned by a network administrator.

Bandwidth: Data capacity of a link. For instance, normally a 10

Mbps Ethernet Link is preferable to a 64 kbps leased line.

Delay: Length of time required to move a packet from source to destination

Load: Amount of activity on a network resource, such as a router or link.

Reliability: Usually refers to the bit-error rate of each network link.

MTU: Maximum transmission unit. The maximum frame length in octets that is acceptable to all links on the path.



Revision no.: PPT/2K804/04



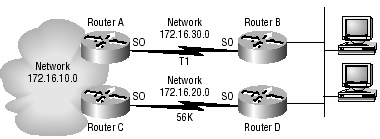
# Pinhole Congestion

* Since network 172.16.30.0 is a T1 link with a bandwidth of 1.544Mbps, and network 172.16.20.0 is a 56K link.
* You would want the router to choose the T1 over the 56K link.



**©**

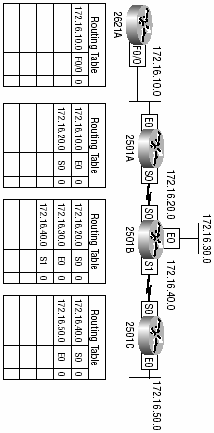
* Since hop count is the only metric used with RIP routing, they would both be seen as equal-cost links.
* This is called pinhole congestion











Revision no.: PPT/2K804/04

**The Internetwork with Distance-Vector Routing**

Revision no.: PPT/2K804/04



# Distance Vector Characteristics

* Distance based routing decision
* Constant Frequent Broadcast



* + RIP sends Broadcast after every 30 seconds.
* Second hand information is propagated / sent.
* Convergence
  + Time taken by all the Routers to update themselves about the topology change is high.
* Routing decisions are based solely on the basis of hop count.
* Note: RIP Metric = Distance
  + IGRP Metric = Distance + Bandwidth+delay



Revision no.: PPT/2K804/04



# Convergence

## The routing tables are complete because they include information about all the networks in the internetwork.

* They are considered converged.



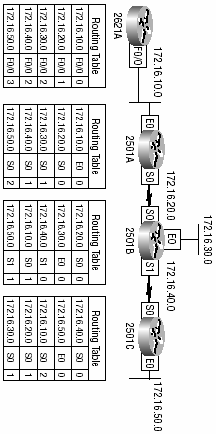
* When the routers are converging, no data is passed.
* That’s why fast convergence time is a plus.
* One of the problems with RIP, in fact is, its slow convergence time.







Revision no.: PPT/2K804/04

.

**Converged Routing Tables**

Revision no.: PPT/2K804/04



# Routing Loops

## Distance-vector routing protocols keep track of any changes to the internet-work by broadcasting periodic routing updates to all active interfaces.

* This broadcast includes the complete routing table.



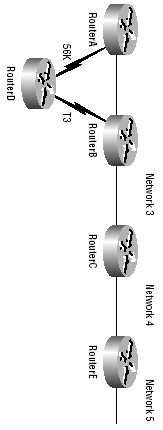
* This works fine, although it takes up CPU process and link bandwidth.
* The slow convergence of Distance-Vector routing protocols can cause inconsistent routing tables and routing loops.







Revision no.: PPT/2K804/04



Revision no.: PPT/2K804/04



# Router Looping Process

* Routing loops can occur because every router is not updated close to the same time. Let’s say that the interface to Network 5 in Figure fails.
* All routers know about Network 5 from Router E. Router A, in its tables, has a path to Network 5 through Routers B, C, and E.



* When Network 5 fails, Router E tells RouterC.
* This causes Router C to stop routing to Network 5 through Router E.
* But Routers A, B, and D don’t know about Network 5 yet, so they keep sending out update information.
* Router C will eventually send out its update and cause B to stop routing to Network 5, but Routers A and D are still not updated.



Revision no.: PPT/2K804/04



**Router Looping Process (contd.)**

## To them, it appears that Network 5 is still available through Router B with a metric of three.

* Router A sends out its regular 30-second “Hello, I’m still here—these are the links I know about” message, which includes reachability for Network 5.



* Routers B and D then receive the wonderful news that Network 5 can be reached from Router A, so they send out the information that Network 5 is available.
* Any packet destined for Network 5 will go to Router A, to Router B, and then back to Router A. This is a routing loop
* How do you stop it?



Revision no.: PPT/2K804/04



# Maximum Hop Count

* The routing loop problem just described is called counting to infinity
* It is caused by gossip and wrong information being communicated and propagated throughout the internetwork.



* Without some form of intervention, the hop count increases indefinitely each time a packet passes through a router.
* One way of solving this problem is to define a maximum hop count.
* Distance vector (RIP) permits a hop count of up to 15, so anything that requires 16 hops is deemed unreachable.



Revision no.: PPT/2K804/04



**Maximum Hop Count (contd.)**

## Hence after a loop of 15 hops, Network 5 will be considered down.

* This means that counting to infinity will keep packets from going around the loop forever.



* Though this is a workable solution, it won’t remove the routing loop itself.
* Packets will still go into the loop, but instead of traveling on unchecked, they’ll whirl around for 16 bounces and die.



Revision no.: PPT/2K804/04



# Split Horizon

* Another solution to the routing loop problem is called split horizon.



* This reduces incorrect routing information and routing overhead in a distance-vector network by enforcing the rule that information cannot be sent back in the direction from which it was received.
* It would have prevented Router A from sending the updated information it received from Router B back to Router B.



Revision no.: PPT/2K804/04



# Route Poisoning

* Another way to avoid problems caused by inconsistent updates is route poisoning.
* when Network 5 goes down, Router E initiates route poisoning by entering a table entry for Network 5 as 16, or unreachable



* By this poisoning of the route to Network 5, Router C is not susceptible to incorrect updates about the route to Network 5.
* When Router C receives a router poisoning from Router E, it sends an update, called a poison reverse, back to Router E.
* This makes sure all routes on the segment have received the poisoned route information.
* Route poisoning, used with hold downs will speed up convergence time because neighboring routers don’t have to wait 30 seconds before advertising the poisoned route.



Revision no.: PPT/2K804/04



# Holddown Timers

## Holddown Timers are used to prevent regular update messages from inappropriately reinstating a route that might have gone bad.

* Holddowns tell router to hold any changes that might affect routes for some period of time.



* The holddown period is usually calculated to be just greater than the period of time necessary to update the entire network with a routing change.



Revision no.: PPT/2K804/04



# How Holddown Timers work

* When a router receives an update from a neighbor indicating that a previously accessible network is now inaccessible, the router marks the route as inaccessible and starts a holddown timer.
* If an update arrives from a neighboring router with a better metric than originally recorded for the network, the router marks the networks as accessible and removes the holddown timer.



* LAN update is received from a neighbor router before the holddown timer expires and it has a lower metric than the previous route, the update is ignored and the holddown timer keeps ticking. This allows more time for the network to converge.



Revision no.: PPT/2K804/04



# HOLD TIMER Expiring

* Hold Timers are run on the router connected to the failed link. It will connected to the failed link.
* It will stop any updation or propagation for the failed Network.



* A Hold Timer will expire under three condition with the help of triggered updates.
  + The Timer expires
  + A tasks proportional to no. of links received.
  + Original Path comes back or alternative path is available.



Revision no.: PPT/2K804/04



# Triggered Updates

## Holddowns use triggered updates, which reset the holddown timer, to alert the neighbor routers of a change in the network.

* Triggered updates create a new routing table that is sent immediately to neighbor routers because a change was detected in the internetwork.



* There are three instances when triggered updates will reset the holddown timer:
  + The holddown timer expires.
  + The router receives a processing task proportional to the number of links in the internetwork.
  + Another update is received indicating the network status has changed.



Revision no.: PPT/2K804/04



# Routing Information Protocol ( R I P )

## Routing Information Protocol (RIP) is a true distance-vector routing protocol.

* It sends the complete routing table out to all active interfaces every 30 seconds.



* RIP only uses hop count to determine the best way to a remote network, but it has a maximum allowable hop count of 15, meaning that 16 is deemed unreachable.
* RIP works well in small networks, but it is inefficient on large networks with slow WAN links or on networks with a large number of routers installed.



Revision no.: PPT/2K804/04



# Routing Information Protocol ( R I P ) (contd.)

## RIP version 1 uses only classful routing, which means that all devices in the network must use the same subnet mask.

* This is because RIP version 1 does not send updates with subnet mask information in tow.



* RIP version 2 provides what is called prefix routing and does send subnet mask information with the route updates.
* This is called classless routing.



Revision no.: PPT/2K804/04



# Configuring RIP Routing

* To configure RIP routing, just turn on the protocol with the *router rip* command and tell the RIP routing protocol which networks to advertise.
* RIP has an administrative distance of 120.



* Example to configure RIP

Lab\_A(config)#**router rip**

Lab\_A(config-router)#**network 192.168.10.0**

Lab\_A(config-router)#**network 192.168.20.0**

Lab\_A(config-router)#**^Z** Lab\_A#



Revision no.: PPT/2K804/04



# Verifying the RIP Routing Tables

Lab\_C#**sh ip route**

*[output cut]*



Gateway of last resort is not set

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| C | 192.168.50.0 | is directly | | connected, FastEthernet0/0 | | |
| C | 192.168.40.0 | is directly | | connected, Serial0/0 | | |
| R | 192.168.30.0 | [120/1] | via | 192.168.40.1, | 00:00:04, | Serial0/0 |
| R | 192.168.20.0 | [120/1] | via | 192.168.40.1, | 00:00:26, | Serial0/ |
| R | 192.168.10.0 | [120/2] | via | 192.168.40.1, | 00:00:04, | Serial0/0 |

Lab\_C#



Revision no.: PPT/2K804/04



# Holding Down RIP Propagations

## There are a few different ways to stop unwanted RIP updates from propagating across your LANs and WANs.

* The easiest one is through the *passive-interface* command. This command prevents RIP update broadcasts from being sent out a defined interface, but that same interface can still receive RIP updates.



Lab\_A#**config t**

Lab\_A(config)#**router rip**

Lab\_A(config-router)#**network 192.168.10.0**

Lab\_A(config-router)#**passive-interface serial 0/0**

****

Revision no.: PPT/2K804/04



# RIP Version 2 (RIPv2) RIPv1 vs. RIPv2

|  |  |
| --- | --- |
| **RIPv1** | **RIPv2** |
| Distance vector | Distance vector |
| Maximum hop count of 15 | Maximum hop count of 15 |
| Classful | Classless |
| Broadcast based | Uses multicast 224.0.0.9 |
| No support for VLSM | Supports VLSM networks |
| No authentication | Allows for MD5 authentication |
| No support for discontiguous networks | Supports discontiguous networks |

**Configuring RIPv2**



Lab\_C(config)#router rip

Lab\_C(config-router)#network 192.168.40.0

Lab\_C(config-router)#network 192.168.50.0

Lab\_C(config-router)#version 2

**Note :** We can configure Rip through sdm.



Revision no.: PPT/2K804/04



# Interior Gateway Routing Protocol (IGRP)

* Interior Gateway Routing Protocol (IGRP) is a Cisco proprietary distance-vector routing protocol.
* This means that all your routers must be Cisco routers to use IGRP in your network.



* Cisco created this routing protocol to overcome the problems associated with RIP.
* IGRP has a maximum hop count of 255 with a default of 100.
* This is helpful in larger networks and solves the problem of there being only 15 hops maximum possible in a RIP network. IGRP also uses a different metric from RIP.



Revision no.: PPT/2K804/04



# Interior Gateway Routing Protocol (IGRP) (contd.)

## IGRP uses bandwidth and delay of the line by default as a metric for determining the best route to an internetwork.



* This is called a composite metric.
* Reliability, load, and Maximum Transmission Unit (MTU) can also be used, although they are not used by default.



Revision no.: PPT/2K804/04



# IGRP Timers

## To control performance, IGRP includes the following timers with default settings:

* + Update timers :-These specify how frequently routing-update messages should be sent. The default is 90 seconds.



* + Invalid timers:- These specify how long a router should wait before declaring a route invalid if it doesn’t receive a specific update about it. The default is three times the update period.
  + Holddown timers:- These specify the holddown period. The default is three times the update timer period plus 10 seconds.
  + Flush timers:-These indicate how much time should pass before a route should be flushed from the routing table. The default is seven times the routing update period.



Revision no.: PPT/2K804/04



# Configuring IGRP Routing

* The command used to configure IGRP is the same as the one used to configure RIP routing with one important difference:
  + you use an autonomous system (AS) number.



* + All routers within an autonomous system must use the same AS number, or they will not communicate with routing information.

Lab\_A#**config t**

Enter configuration commands, one per line. End with CNTL/Z. Lab\_A(config)#**router igrp ?**

<1-65535> Autonomous system number Lab\_A(config)#**router igrp 10**

Lab\_A(config-router)#**network 192.168.10.0**

Lab\_A(config-router)#**network 192.168.20.0**

Lab\_A(config-router)#**^Z** Lab\_A#



Revision no.: PPT/2K804/04



**Configuring IGRP Routing (contd.)**

## Command is as simple as in RIP routing except that IGRP uses an AS number.

* This number advertises only to routers you want to share routing information with.



* IGRP can load balance up to six unequal links
* RIP networks must have the same hop count to load balance, whereas IGRP uses bandwidth to determine how to load balance.
* To load balance over unequal-cost links, the variance command controls the load balancing between the best metric and the worst acceptable metric.



Revision no.: PPT/2K804/04



# Controlling Traffic Distribution

## There are two more commands that are used to help control traffic distribution among IGRP load-sharing routes: traffic-share balanced and traffic-share min .

* The router output below shows the options available under the router igrp as command prompt.



Router(config-router)#variance *multiplier*

## Controls IGRP load balancing

Router(config-router)#traffic-share {balanced | min}

## Controls how load-balanced traffic is distributed



Revision no.: PPT/2K804/04



# Verifying you configurations

## show ip route

* + privilege mode command, shows the routing table.



## show protocols

* + Privilege mode command, shows the network layer address configured on each interface

## show ip protocol

* + Privilege mode command, shows the routing protocol that are configured on your router.

## debug ip rip

* + privilege mode command, sends routing updates as they are sent and received, to the console session.



Revision no.: PPT/2K804/04



**Verifying you configurations (contd.)**

## debug ip igrp events

* + privilege mode command, it is a summary of the IGRP routing running on the router.



## debug ip igrp transactions

* + privilege mode command shows message request from neighbor routers asking for an update and the broadcasts sent from your router towards that neighbor router.



Revision no.: PPT/2K804/04

permission.

prior the

without

emailed or

stored d,

reproduce be

may

material

this of

part No

reserved.

rights All

.

**2004**

**INSTITUTE, CMS**

**©**



**Design & Published by:**