NATIONAL UNIVERSITY OF COMPUTER & EMERGING SCIENCE
Computer Networks Lab (CL307)
Lab Session 12

Awais Ahmed || Faizan Yousuf || Munim Ali Khan

awais.ahmed@nu.edu.pk || faizan.yousuf@nu.edu.pk || munim.ali@nu.edu.pk

IP Routing I: Static Routing & Default routing

Routing protocol and Routed protocol

You must understand the difference between a routing protocol and a routed protocol. A routing protocol is used by routers to dynamically find all the networks in the internetwork and to ensure that all routers have the same routing table. Basically, **a routing protocol determines the path of a packet through an internetwork.**

Examples of routing protocols are *RIP*, *RIPv2*, *EIGRP*, and *OSPF*.

Once all routers know about all networks, **a routed protocol can be used to send user data (packets) through the established enterprise**. Routed protocols are assigned to an interface and determine the method of packet delivery.

Examples of routed protocols are *IP* and *IPv6*.

Routing basis

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 do not really care about hosts - they only care about networks and the best path to each network.

The logical network address of the destination host is used to get packets to a network through a routed network, and then the hardware address of the

host is used to deliver the packet from a router to the correct destination host.

If a network is not directly connected to the router, then the router must use one of two ways to learn how to get to the remote network: **static routing**, meaning that someone must hand-type all network locations into the routing table, or something called **dynamic routing**

Static Routing

Static routing occurs when you manually add routes in each router's routing table. There are pros and cons to static routing, but that is true for all routing processes.

Static routing has the following benefits:

- There is no overhead on the router CPU, which means that you could possibly buy a cheaper router than you would use if you were using dynamic routing.
- There is no bandwidth usage between routers, which means you could possibly save money on WAN links.
- It adds security because the administrator can choose to allow routing access to certain networks only.

Static routing has the following disadvantages:

- The administrator must really understand the internetwork and how each router is connected in order to configure routes correctly.
- If a network is added to the internetwork, the administrator has to add a route to it on all routers—by hand.
- It's not feasible in large networks because maintaining it would be a full-time job in itself.

Default Routing

We use default routing to send packets with a remote destination network not in the routing table to the next-hop router. You should only use default routing on stub networks—those with only one exit path out of the network.

Configuring Routes on Cisco Router

Using Cisco Packet Tracer software, we simulate the following network which has 4 networks and 10 subnetworks (VLSM).

And assign each host an IP. Also we have to assign an IP for each interface on the router. We assign an IP for the Router interface and start it up using the following commands:

```
Router(config)#interface fa0/0
Router(config-if)#ip address 192.168.1.129 255.255.255.192
Router(config-if)#no shutdown
```
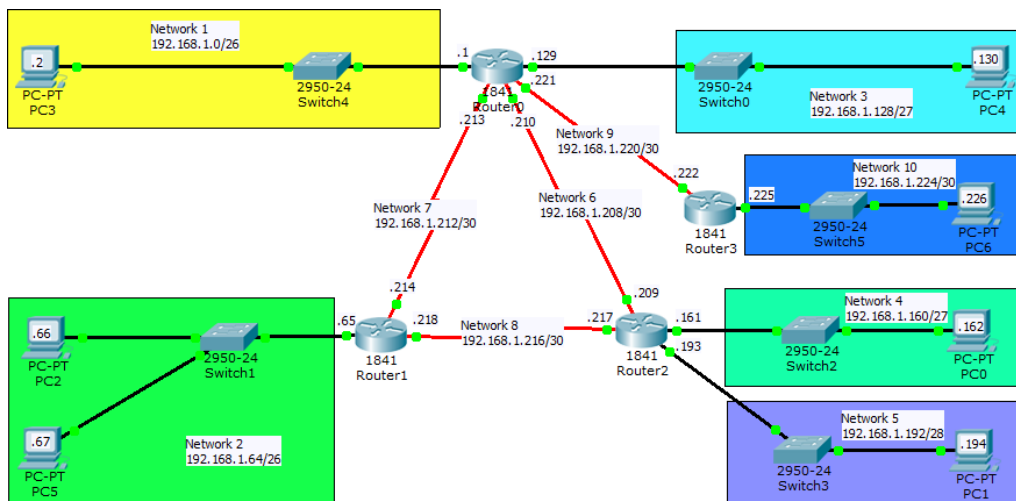
Where:

        fa0/0 is the name of the interface.

        192.168.1.129 is the IP address for interface fa0/0.

        255.255.255.192 is the subnet mask being used on the network that connected directly to the interface.

        no shutdown to start up the interface.

Run the same commands for all routers interfaces and assign each interface an appropriate IP/mask pair.

Now we start routing …

Network 10 is connected directly to **Router 3** and no other subnets is connected to **Router 3**, so we can configure default route on it using the following command:

Router(config)#ip route **0.0.0.0** **0.0.0.0** **192.168.1.221**

Where:

0.0.0.0 is the destination network IP [0.0.0.0 in case of default routing]
0.0.0.0 is the subnet mask being used on the destination network.
192.168.1.221 is the address of the next-hop router that will receive the packet and forward it to the destination network.

For the other routers, we cannot implement default routing since each of them is connected to more than one network. In this case, we use static routing.

We can configure static route on **router0** as follow:

Router(config)#ip route **192.168.1.64** **255.255.255.192** **192.168.1.214**

Where:

192.168.1.64 is the destination network we wants to send packets to it.
255.255.255.192 is the subnet mask being used on the destination network.
192.168.1.214 is the address of the next-hop router that will receive the packet and forward it to the destination network.

Configuring all other static routes on router0:

Router(config)#ip route 192.168.1.160 255.255.255.224 192.168.1.209
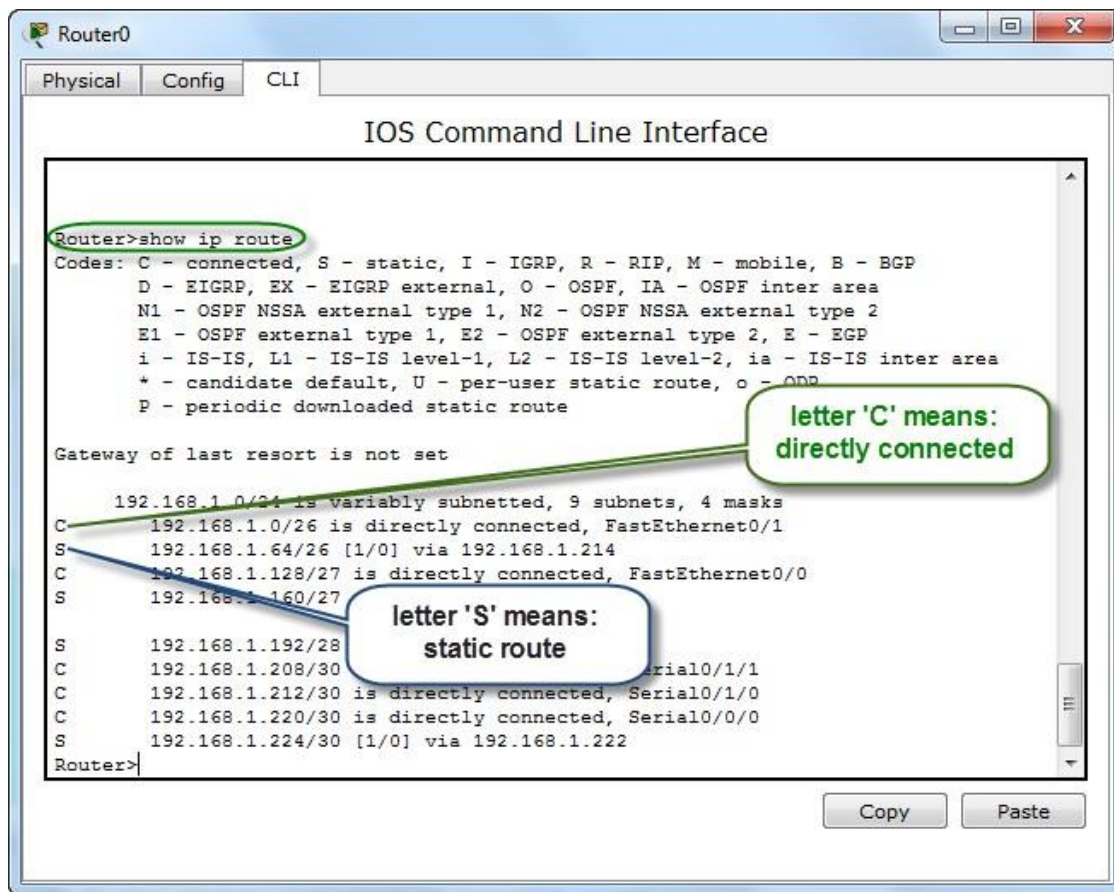Router(config)#ip route 192.168.1.192 255.255.255.240 192.168.1.209
Router(config)#ip route 192.168.1.224 255.255.255.252 192.168.1.222

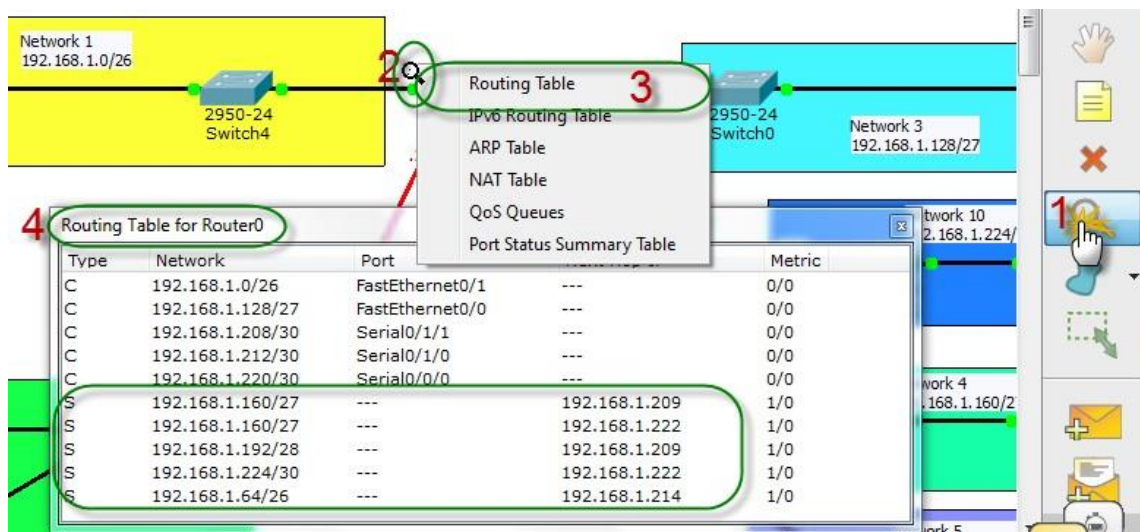And do the same thing for the other routers.

To review routing table on a router, use command "***show ip route***":

Router>show ip route

Router0

Physical | Config | CLI

IOS Command Line Interface

```
Router>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

     192.168.1.0/24 is variably subnetted, 9 subnets, 4 masks
C       192.168.1.0/26 is directly connected, FastEthernet0/1
S       192.168.1.64/26 [1/0] via 192.168.1.214
C       192.168.1.128/27 is directly connected, FastEthernet0/0
S       192.168.1.160/27
S       192.168.1.192/28
C       192.168.1.208/30                    rial0/1/1
C       192.168.1.212/30 is directly connected, Serial0/1/0
C       192.168.1.220/30 is directly connected, Serial0/0/0
S       192.168.1.224/30 [1/0] via 192.168.1.222
Router>
```

letter 'C' means: directly connected

letter 'S' means: static route

Copy | Paste

Alternatively, by using the Inspect tool from the right panel, and select "*Routing Table*" from the menu:

Network 1
192.168.1.0/26

2950-24
Switch4

Routing Table
IPv6 Routing Table
ARP Table
NAT Table
QoS Queues
Port Status Summary Table

2950-24
Switch0

Network 3
192.168.1.128/27

Network 10
2.168.1.224/

Routing Table for Router0

Type	Network	Port		Metric
C	192.168.1.0/26	FastEthernet0/1	---	0/0
C	192.168.1.128/27	FastEthernet0/0	---	0/0
C	192.168.1.208/30	Serial0/1/1	---	0/0
C	192.168.1.212/30	Serial0/1/0	---	0/0
C	192.168.1.220/30	Serial0/0/0	---	0/0
S	192.168.1.160/27	---	192.168.1.209	1/0
S	192.168.1.160/27	---	192.168.1.222	1/0
S	192.168.1.192/28	---	192.168.1.209	1/0
S	192.168.1.224/30	---	192.168.1.222	1/0
S	192.168.1.64/26	---	192.168.1.214	1/0

Network 4
.168.1.160/2

Network 5

Now check the connectivity of the network using "*ping*" command, or "*tracert*" command.
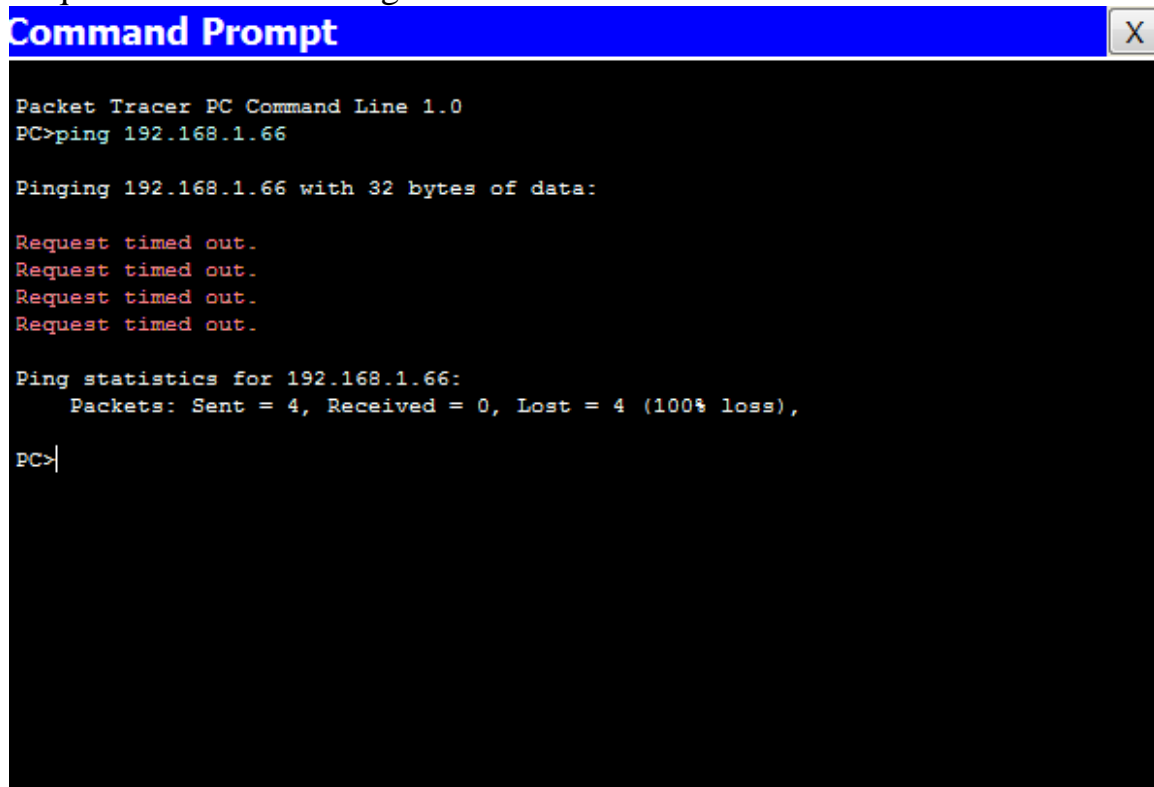
Note: to tell the cisco router to Stops looking for meaning for wrong written words while configuring Cisco router type:
 "Corp(config)#no ip domain-lookup"

Another quick note: to mention that when (if) the packet is lost on the way back to the originating host, you will typically see a "Request timed out" message because it is an unknown error.
If the error occurs because of a known issue, such as if a route is not in the routing table on the way to the destination device, you will see a "Destination host unreachable" message. This should help you determine if the problem occurred on the way to the destination or on the way.

Request timed out message:

Destination host unreachable message:

```
Command Prompt                                            X

Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.162

Pinging 192.168.1.162 with 32 bytes of data:

Reply from 192.168.1.65: Destination host unreachable.
Reply from 192.168.1.65: Destination host unreachable.
Reply from 192.168.1.65: Destination host unreachable.
Reply from 192.168.1.65: Destination host unreachable.

Ping statistics for 192.168.1.162:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```
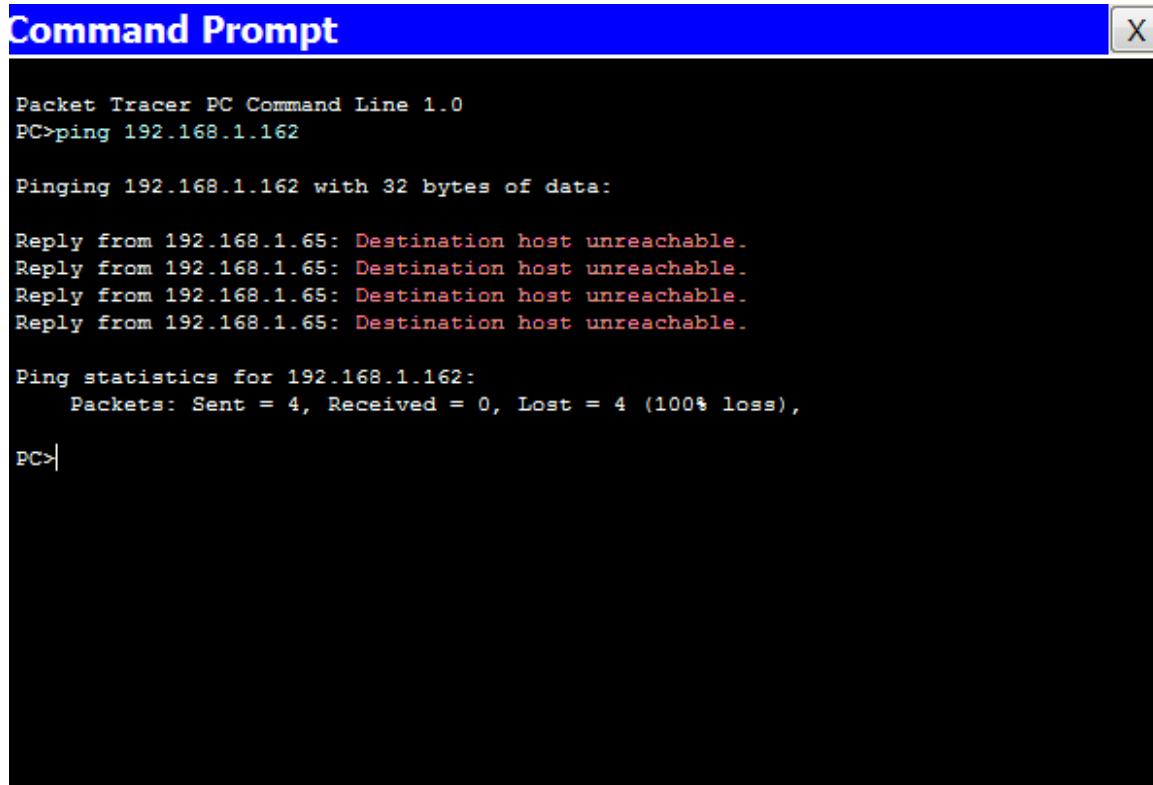
IP Routing II: Dynamic Routing (RIP,OSPF)
Introduction

Dynamic routing is when protocols are used to find networks and update routing tables on routers. True, this is easier than using static or default routing, but **it'll cost you in terms of router CPU processes and bandwidth on the network links**.

A *routing protocol* defines the set of rules used by a router when it communicates routing information between neighbor routers. The routing protocol includes **Routing Information Protocol (RIP) versions 1 and 2**, with a bit of **Interior Gateway Routing Protocol (IGRP)** thrown in.

Two types of routing protocols are used in internetworks: **interior gateway protocols (IGPs) and exterior gateway protocols (EGPs).**

IGPs are used to exchange routing information with routers in the same autonomous system (AS). An AS is a collection of networks under a common administrative domain, which basically means that all routers sharing the same routing table information are in the same AS.

EGPs are used to communicate between ASes. An example of an EGP is **Border Gateway Protocol (BGP), which is beyond the scope of our lab.**

Administrative Distances

The administrative distance (AD) is used to **rate the trustworthiness of routing information received on a router from a neighbor router**. An administrative distance is an integer from 0 to 255, where 0 is the most trusted and 255 means no traffic will be passed via this route.

If a router receives two updates listing the same remote network, the first thing the router checks is the AD.

If one of the advertised routes has a lower AD than the other, then the route with the lowest AD will be placed in the routing table. If both advertised routes to the same network have the same AD, then routing protocol **metrics** (such as hop count or bandwidth of the lines) will be used to find the best path to the remote network. The advertised route with the lowest metric will be placed in the routing table.

But if both advertised routes have the **same AD as well as the same metrics**, then the routing protocol will **load-balance** to the remote network (which means that it sends packets down each link).

Table below shows default AD

Route Source	Default AD
Connected interface	0
Static route	1
EIGRP	90

IGRP	100
OSPF	110
RIP 1	120
External EIGRP	170
Unknown	266

The smaller the AD is, the more preferable to route is.

Classes of routing protocols

Distance vector

The distance-vector protocols find the best path to a remote network by judging distance. Each time a packet goes through a router, that's called a hop. **The route with the least number of hops to the network is determined to be the best route.** The vector indicates the direction to the remote network. Both RIP and IGRP are distance-vector routing protocols. **They send the entire routing table to directly connected neighbors.**

Link state

In link-state protocols, also called **shortest-path-first protocols**. Link-state routers know more about the internetwork than any distance vector routing protocol. OSPF is an IP routing protocol that is completely link state. Link-state protocols send updates containing the state of their own links to all other routers on the network.

Hybrid

Hybrid protocols use aspects of both distance vector and link state—for example, EIGRP. There's no set way of configuring routing protocols for use with every business. This is something you really have to do on a case-by-case basis. If you understand how the different routing protocols work, you can make good, solid decisions that truly meet the individual needs of any business.
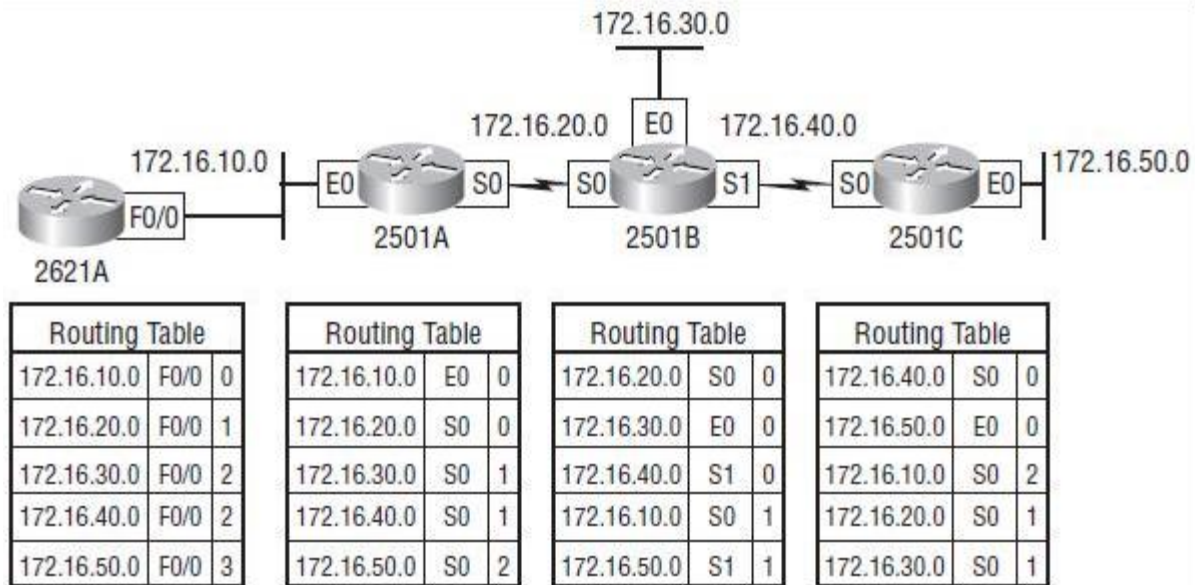
Distance vector routing protocols

The distance-vector routing algorithm passes complete routing table contents to neighboring routers, which then combine the received routing table entries with their own routing tables to complete the router's routing table. 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.
Example:
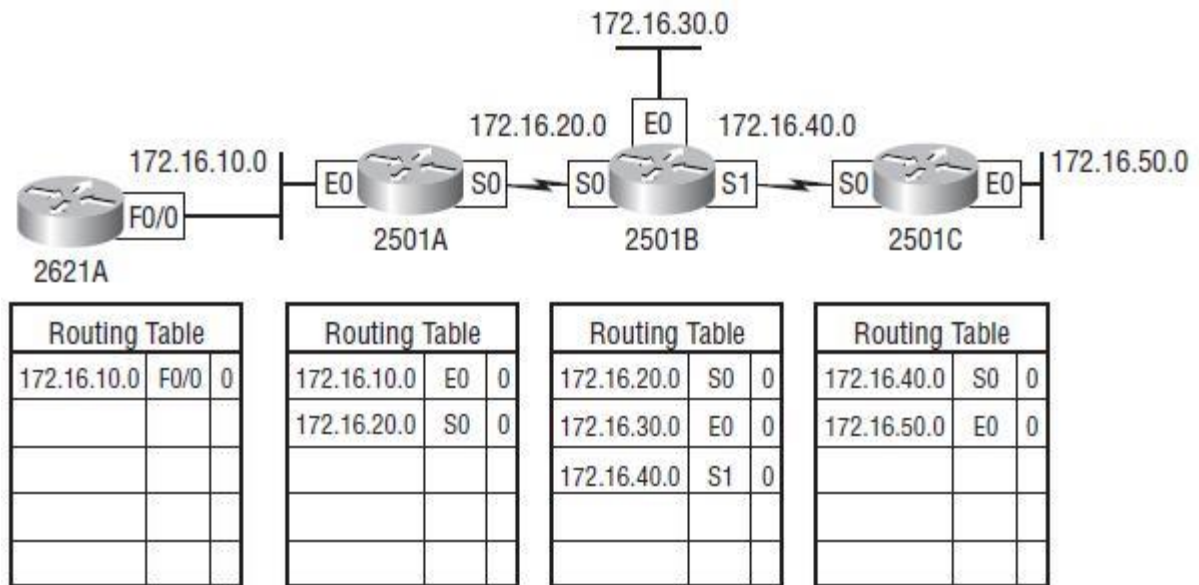
The four routers start off with only their directly connected networks in their routing tables. After a distance-vector routing protocol is started on each router, the routing tables are updated with all route information gathered from neighbor routers.

After convergence, the routing tables will look like this:

Routing Table		
172.16.10.0	F0/0	0
172.16.20.0	F0/0	1
172.16.30.0	F0/0	2
172.16.40.0	F0/0	2
172.16.50.0	F0/0	3

Routing Table		
172.16.10.0	E0	0
172.16.20.0	S0	0
172.16.30.0	S0	1
172.16.40.0	S0	1
172.16.50.0	S0	2

Routing Table		
172.16.20.0	S0	0
172.16.30.0	E0	0
172.16.40.0	S1	0
172.16.10.0	S0	1
172.16.50.0	S1	1

Routing Table		
172.16.40.0	S0	0
172.16.50.0	E0	0
172.16.10.0	S0	2
172.16.20.0	S0	1
172.16.30.0	S0	1

Routing loops in DV and how to solve it?

Routing loops can occur because every router isn't updated simultaneously, or even close to it. Here's an example assume network 10.4.0.0 goes down (figure a), and before R3 advertises that **(by sending routing poisoning message: hope count > 15 = infinity)**, it receives an update form R2 which contains information about network 10.4.0.0 (see figure b)
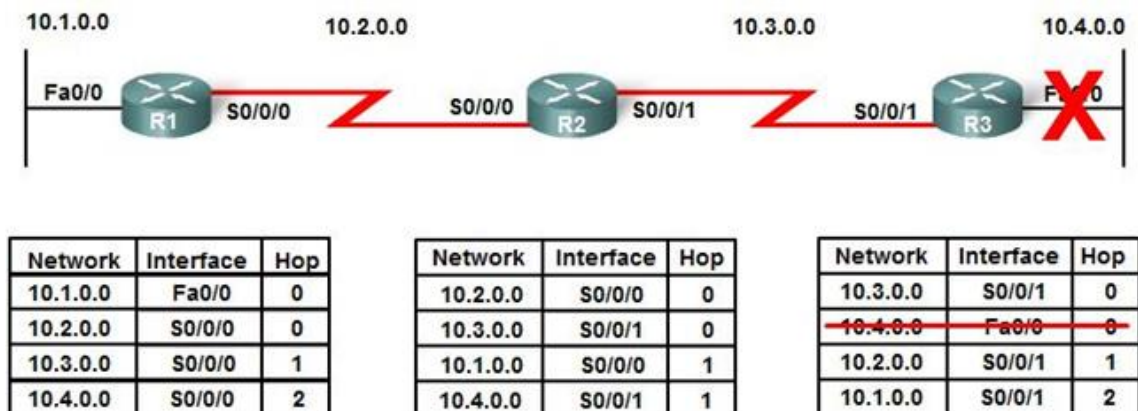

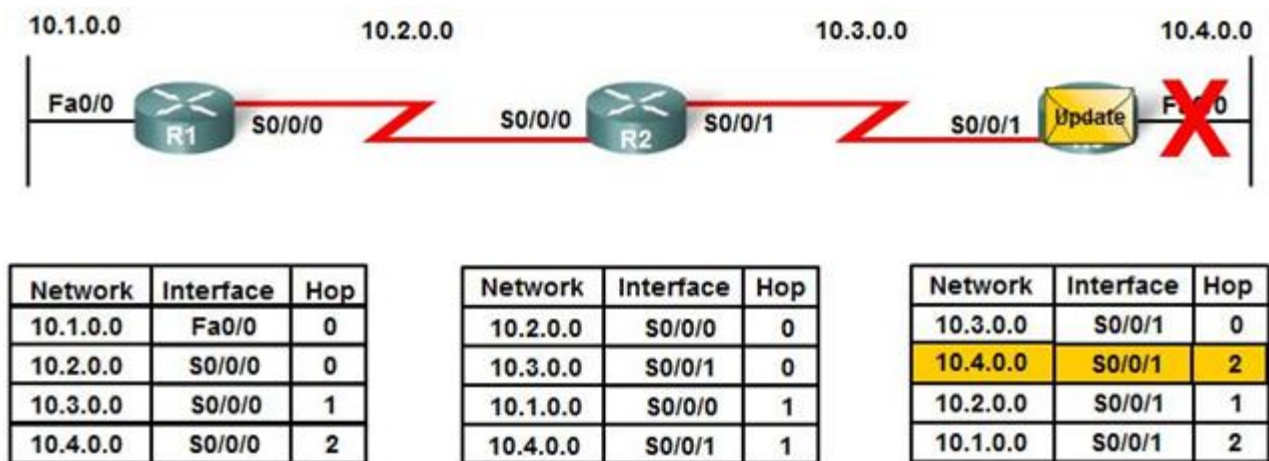| Network	Interface	Hop
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1
10.4.0.0	S0/0/0	2

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

Figure a

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	2
10.2.0.0	S0/0/1	1
10.1.0.0	S0/0/1	2

Figure b

Now assume a PC in network 10.1.0.0 tries to send data to a PC in network 10.4.0.0? What will happen?!

Another example —let's say that the interface to Network 5 fails. All routers know about Network 5 from RouterE. RouterA, in its tables, has a path to Network 5 through RouterB.
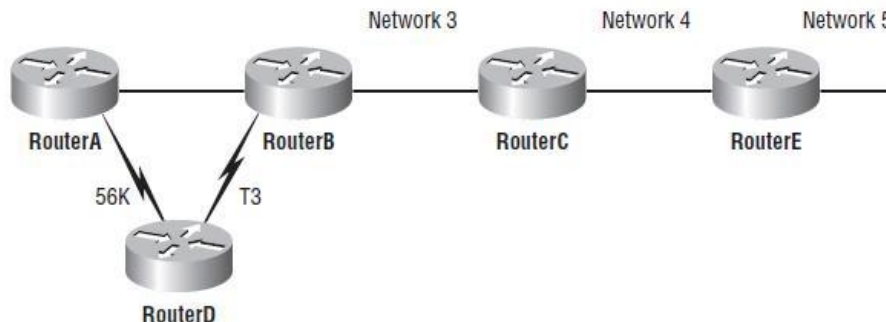
When Network 5 fails, RouterE tells RouterC **(by sending routing poisoning message: hope count > 15 = infinity).** This causes RouterC to stop routing to Network 5 through RouterE. But routers A, B, and D don't know about Network 5 yet, so they keep sending out update information. RouterC will eventually send out its update and cause B to stop routing to Network 5, but routers A and D are still not updated. To them, it appears that Network 5 is still available through RouterB with a metric of 3. **The problem occurs** when RouterA sends out its regular 30-second "Hello, I'm still here— these are the links I know about" message, which includes the ability to reach Network 5, and now routers B and D receive the wonderful news

that Network 5 can be reached from RouterA.

Loops?

Router A thinks he knows how to reach Network 5 form network B by 3 hops and B thinks he know it form A by 4 hops. When B advertise, A will receive that B knows Network 5 by 4 now! Then he alters his table and advertise. Same thing when B receives it. And so on.

Solution:

Maximum hope count, Split horizon >>> HOW?

Routing Information Protocol (RIP)

Routing Information Protocol (RIP) is a true distance-vector routing protocol. RIP 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** by default, meaning that 16 is deemed unreachable. RIP works well in small networks, but it's inefficient on large networks with slow WAN links or on networks with a large number of routers installed.

What will happen using RIP?
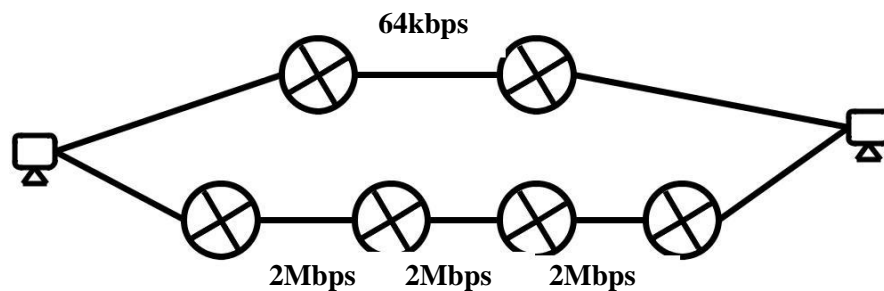
RIP Timers

RIP uses four different kinds of timers to regulate its performance:

Route update timer

Sets the interval (typically 30 seconds) between periodic routing updates in which the router sends a complete copy of its routing table out to all neighbors.

Route 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.

Hold down timer

This sets the amount of time during which routing information is suppressed. Routes will enter into the hold-down state when an update packet is received that indicated the route is unreachable. This continues either until an update packet is received with a better metric or until the hold-down timer expires. The default is 180 seconds.

Route flush timer

Sets the time between a route becoming invalid and its removal from the routing table (240 seconds). Before it's removed from the table, the router notifies its neighbors of that route's impending demise. The value of the route invalid timer must be less than that of the route flush timer. This gives the router enough time to tell its neighbors about the invalid route before the local routing table is updated.

RIP Versions

	RTP V1	RIP V2
AD	120	120
Metric	Hope count	Hope count
Max hope count	15	15
Sending update every	30 sec	30 sec
Sending updates using	Broadcast	multicast
VLSM\CIDR	Not supported	Supported

RIP practical part

RIPV1

Lab_A#**config t**
Lab_A(config)#**router rip**
Lab_A(config-router)#**network 192.168.10.0 (only net without mask)**

Lab_A(config-router)#**passive-interface serial 0/0** (This command prevents RIP update broadcasts from being sent out a specified interface, yet that same interface can still receive RIP updates.)

RIPV2

RIPv2 is considered classless because subnet information is sent with each route update

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**

Interior Gateway Routing Protocol (IGRP)

No longer supported by CISCO so we won't waste our time learning it ☺.

Open Shortest Path First (OSPF)

OSPF works by using the **Dijkstra algorithm**. First, a shortest path tree is constructed, and then the routing table is populated with the resulting best paths. OSPF converges quickly, although perhaps not as quickly as EIGRP, and it supports multiple, equal-cost routes to the same destination. Like EIGRP, it does support both IP and IPv6 routed protocols.

OSPF provides the following features:

- Consists of areas and autonomous systems

- Minimizes routing update traffic
- Allows scalability
- Supports VLSM/CIDR
- Has unlimited hop count
- Allows multi-vendor deployment (open standard)

OSPF Terminology

Router ID

The Router ID (RID) is an IP address used to identify the router. Cisco chooses the Router ID by using the highest IP address of all configured interfaces.

Neighbor

Neighbors are two or more routers that have an interface on a common network, such as two routers connected on a point-to-point serial link.

Adjacency

An adjacency is a relationship between two OSPF routers that permits the direct exchange of route updates. OSPF shares routes only with neighbors that have also established adjacencies.

Hello protocol

The OSPF Hello protocol provides dynamic neighbor discovery and maintains neighbor relationships.

Neighborship database

The neighborship database is a list of all OSPF routers for which Hello packets have been seen.

Link State Advertisement

A Link State Advertisement (LSA) is an OSPF data packet containing link-state and routing information that's shared among OSPF routers. (Contains directly connected interface, cost, type and between whom? Eg:

R1-R2 Serial network 10.4.0.0 cost 40).

Topological database

The topological database contains information from all of the Link State Advertisement packets that have been received for an area.

Designated router

A Designated Router (DR) is elected whenever OSPF routers are connected to the same **multi-access network** (later). DR is chosen (elected) to disseminate/receive routing information to/from the remaining routers. This ensures that their topology tables are synchronized.

The **DR** is the one with the highest router ID.

Backup designated router

A Backup Designated Router (BDR) is a hot standby for the DR on BDR receives all routing updates from OSPF adjacent routers but doesn't flood LSA updates.

OSPF areas

An OSPF area is a grouping of contiguous networks and routers. All routers in the same area share a common Area ID. Areas also play a role in establishing a hierarchical network organization—something that really enhances the scalability of OSPF!

Loopback Address

If the OSPF router-id command is not used and loopback interfaces are configured, OSPF will choose highest IP address of any of its loopback interfaces. A loopback address is a virtual interface and is automatically in the up state when configured. You already know the commands to configure a loopback interface:

Router(config)#interface loopback 0 Router(config-if)#ip address 10.3.0.0 255.255.255.255

Link costs

Simply by dividing 10^8 on every interface bandwidth see table below:

Interface Type	10^8/bps = Cost
Fast Ethernet and faster	10^8/100,000,000 bps = 1
Ethernet	10^8/10,000,000 bps = 10
E1	10^8/2,048,000 bps = 48
T1	10^8/1,544,000 bps = 64
128 kbps	10^8/128,000 bps = 781
64 kbps	10^8/64,000 bps = 1562
56 kbps	10^8/56,000 bps = 1785

Hint: When the serial interface is not actually operating at the default speed, the interface requires manual modification. Both sides of the link should be configured to have the same value.
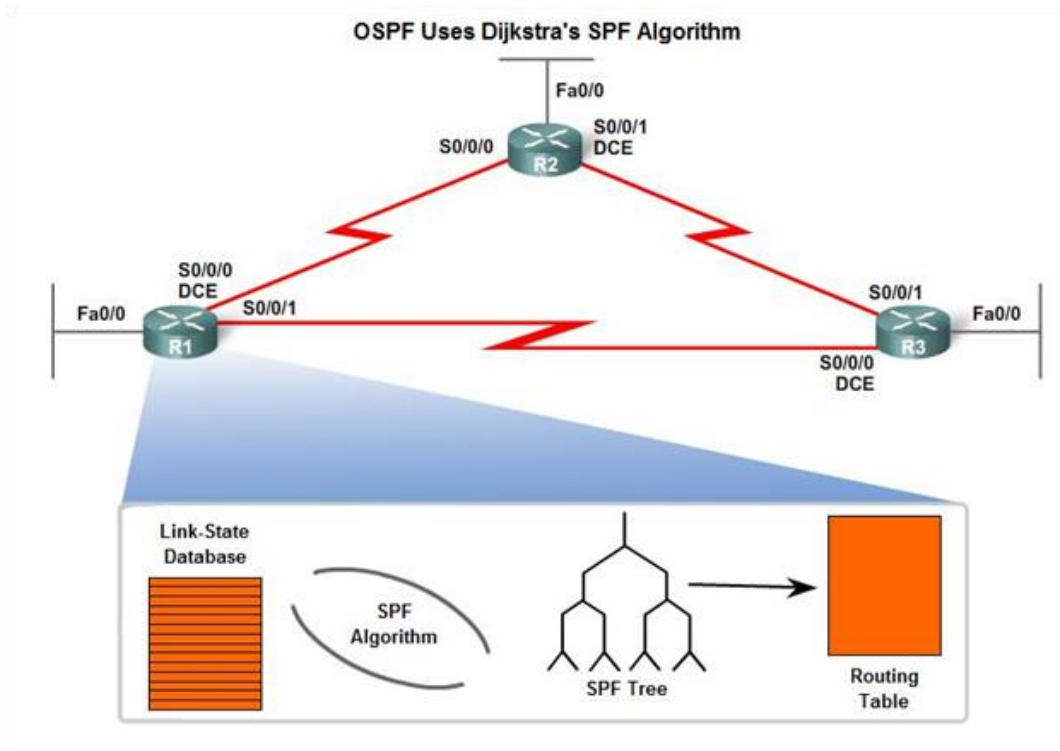
Router(config)#interface s0/0
Router(config-if)# Bandwidth 64
Then the interface cost will be 1562 or simply

R1(config)#interface serial 0/0/0
R1(config-if)#ip ospf cost 1562

Everything ready? Start *shortest path first (SPF)* algorithm

OSPF PRACTICAL PART

Lab_A#**config t**
Lab_A(config)#**router ospf 1**

1: is OSPF process number: out of scope for CCNA, range: <1-65535>
Lab_A(config-router)#**network 10.0.0.0 0.255.255.255 area 0**

0.255.255.255 : an example of wildcard

Wildcard:
 The wildcard mask can be configured as the inverse of a subnet mask. For example, IP 172.16.1.16/28 network. The subnet mask for this interface is /28 or 255.255.255.240. The inverse of the subnet mask results in the wildcard mask .

```
   255.255.255.255
-  255.255.255.240 (Subtract the subnet mask)
-----------------------------
   0. 0. 0. 15            Wildcard mask
```