Name : Aditya Somani Roll No: T1851061 PRN NO:71901204L

Assignment No: 4 Using a Network Simulator (e.g. packet tracer) Configure EIGRP – Explore Neighbor-ship Requirements and Conditions, its K Values Metrics Assignment and Calculation, RIPv2 and EIGRP on same network.WLAN with static IP addressing and DHCP with MAC security and filters

---

Title of the Assignment: Using a Network Simulator (e.g. packet tracer) configure EIGRP

Objective of the Assignment: To understand Distance vector routing and how to configure EIGRP protocol .

Prerequisite: Students must have knowledge of Packet tracer simulator.

Theory :

What are IGRP and EIGRP?

- The major disadvantage of RIP is that it is unable to route traffic if the destination is away from 15 hops. More over RIP fail to identify less populated path as it sticking with Hop count metric, only consider less number Hops. RIP doesn't check whether the path is populated or busy.
- (E)IGRP excludes this all the limitations of RIP, It can be used for larger network more than 15 hops! (255 maximum hop count)
- Assure stable routing even in very large or composite networks. No routing loops should happen.
- Quick reaction to variations in network topology.
- Low overhead, means requires small bandwidth to operate.

EIGRP Metric Calculation

Instead of a simple metric, a **combination of metrics** is used to choose best path.

The best path is picked out by on a complex metric using:

$$Metric = \left\{K1 \times Bandwidth + \left[\frac{K2 \times Bandwidth}{256 - Load}\right] + K3 \times Delay\right\} \times \left[\frac{K5}{Reliability + K4}\right]$$

If K5 = 0, the reliability term is not included.

It implies metric is proportional to many factors rather than a single parameter as in RIP. Here the metric derived from **Internetwork delay, Bandwidth,** and **Reliability**.

The default version of IGRP has K1 == K3 == 1, K2 == K4 == K5 == 0

$$Metric = \left\{1 \times Bandwidth + \left[\frac{0 \times Bandwidth}{256 - Load}\right] + 1 \times Delay\right\} \times \left[\frac{0}{Reliability + 0}\right]$$

Excluding the indeterminate forms we end up with:

Metric={Bandwidth+ Delay}

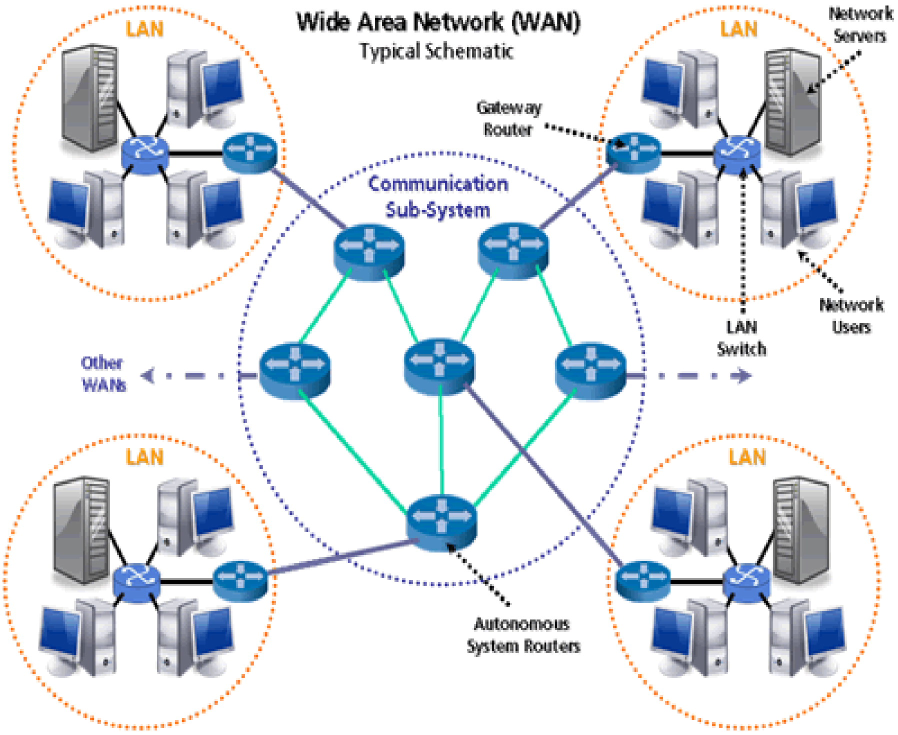
- The terms used in the metric computation are not the raw values gained from the #show interface command. But these values are obtained from **#show ip route** command.
- (E)IGRP capable of perform **<u>Multipath routing</u>**, what is Multipath routing? Unlike RIP, which only recalls a single route to any specified target, **IGRP** can **remember** up to **4 different paths** to any given destination!
- Multipath routing lets IGRP to balance traffic loads over multiple routes, and protecting against the impacts of link failures.
- IGRP uses **port number 9** for communication

Excluding the indeterminate forms we end up with:

Metric={Bandwidth+ Delay}

- The terms used in the metric computation are not the raw values gained from the #show interface command. But these values are obtained from **#show ip route** command.
- (E)IGRP capable of perform **<u>Multipath routing</u>**, what is Multipath routing? Unlike RIP, which only recalls a single route to any specified target, **IGRP** can **remember** up to **4 different paths** to any given destination!
- Multipath routing lets IGRP to balance traffic loads over multiple routes, and protecting against the impacts of link failures.
- IGRP uses **port number 9** for communication

What Autonomous System (AS)

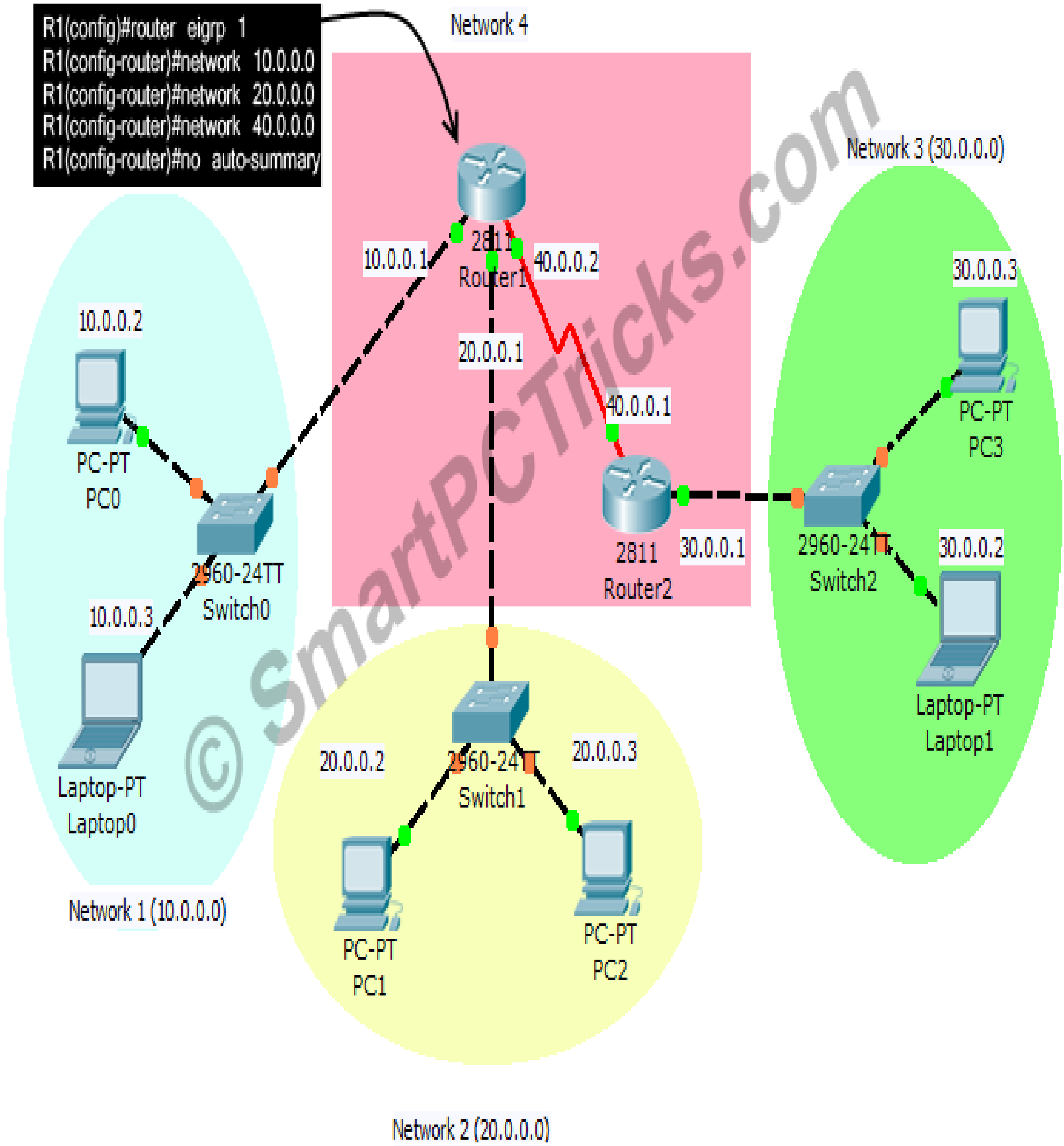


An **Autonomous System** (AS) is a single **network** or a collection of networks that is organized by a **common Network Administrator**. It is also referred as a routing domain. An autonomous system is allotted globally by a unique number called an **Autonomous System Number** (ASN). This number often used in IGRP and EIGRP configuration commands.

EIGRP Example Configuration in Cisco Router

Now I'm going to go to EIGRP configuration example packet tracer. Let's take the same network scenario that we discussed in RIP configuration as our EIGRP configuration topology. To reduce complexity of this article I removed the IP address assignment steps (Assign IP address to all interfaces in Router 1).

EIGRP Configuration Commands: Router 1



R1(config)#router eigrp 1
R1(config-router)#network 10.0.0.0
R1(config-router)#network 20.0.0.0
R1(config-router)#network 40.0.0.0
R1(config-router)#no auto-summary
Network 4
2811
Router1
10.0.0.1
40.0.0.2
20.0.0.1
40.0.0.1
2811
Router2
30.0.0.1
Network 3 (30.0.0.0)
30.0.0.3
PC-PT
PC3
30.0.0.2
Laptop-PT
Laptop1
2960-24TT
Switch2
10.0.0.2
PC-PT
PC0
2960-24TT
Switch0
10.0.0.3
Laptop-PT
Laptop0
Network 1 (10.0.0.0)
2960-24TT
Switch1
20.0.0.2
PC-PT
PC1
20.0.0.3
PC-PT
PC2
Network 2 (20.0.0.0)

If you got basics of EIGRP let’s get in to EIGRP configuration commands. The network topology yields directly connected networks in Router 1 are Network 1 (10.0.0.0), Network 2 (20.0.0.0) and Network 4 (40.0.0.0Cisco EIGRP Example Configuration in Cisco Router

EIGRP Configuration Commands: Router 1

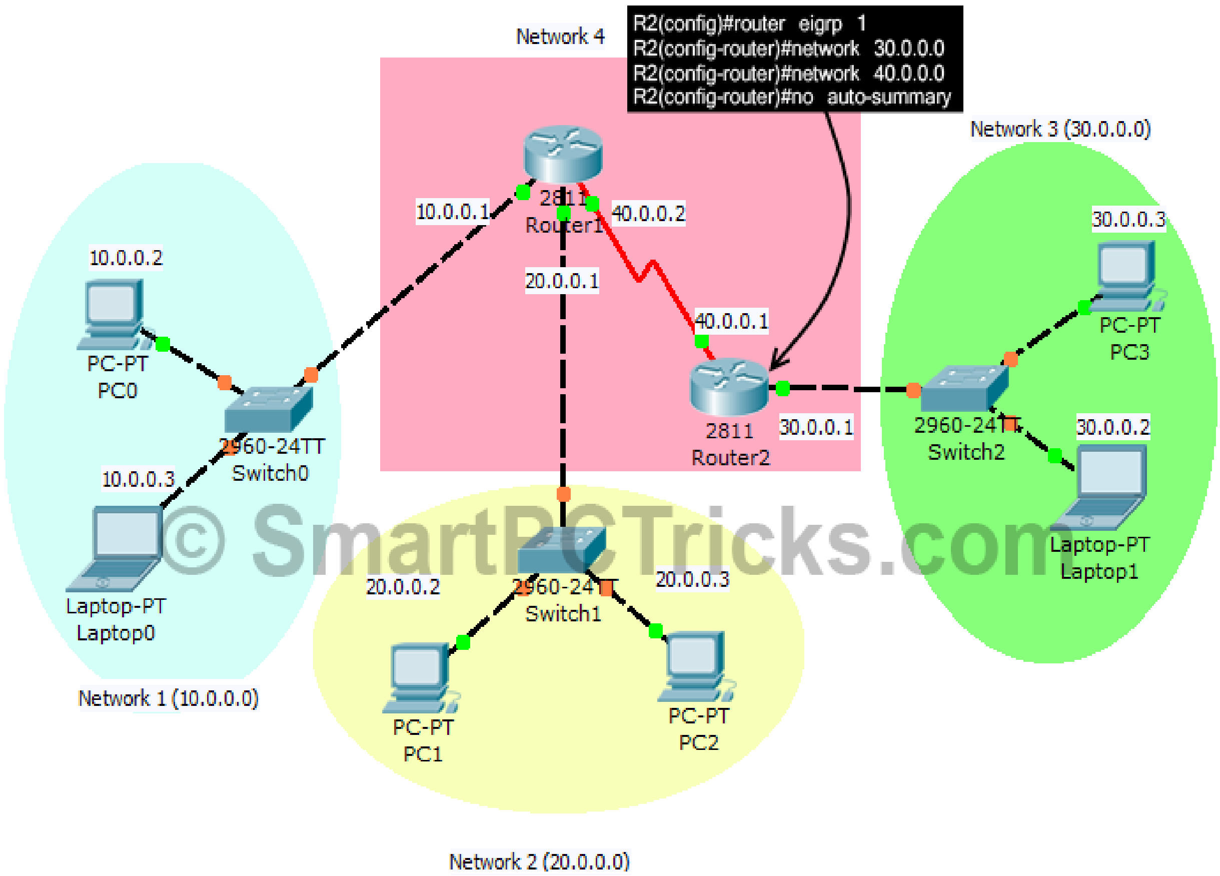
R1>enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router eigrp 1
R1(config-router)#network 10.0.0.0
R1(config-router)#network 20.0.0.0
R1(config-router)#network 40.0.0.0
R1(config-router)#no auto-summary
R1(config-router)#exit
R1(config)#
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#

Where 1 indicates Autonomous System Number.

Next part is configuration of EIGRP in Router 2

The network scenario, directly connected networks are Network 3 (30.0.0.0) and Network 4 (40.0.0.0).



R2>enable
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router eigrp 1
R2(config-router)#network 30.0.0.0
R2(config-router)#network 40.0.0.0
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 40.0.0.2 (Serial0/2/0) is up: new adjacency

R2(config-router)#no auto-summary

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 40.0.0.2 (Serial0/2/0) is up: new adjacency
R2(config-router)#exit
R2(config)#
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#copy running-config startup-config
Destination filename [startup-config]?

Building configuration...
[OK]
R2#

These are the EIGRP configuration commands in packet tracer.

Configure EIGRP Using wildcard masks

- **EIGRP supports VLSM** (Variable Length Subnet Masking). Here I will show you how to configure EIGRP when administering with Subnet masks.

- For EIGRP VLSM routing we should use **Wildcard Mask**, it is nothing but the **inverted version of Subnet mask**. For example Wildcard Mask of 255.0.0.0 is 0.255.255.255.

I'm gonna to subnet the 10.0.0.0 network to 4 subnets. For easy calculation use this ***Online Network Calculator tool:*** **http://www.subnetmask.info/**

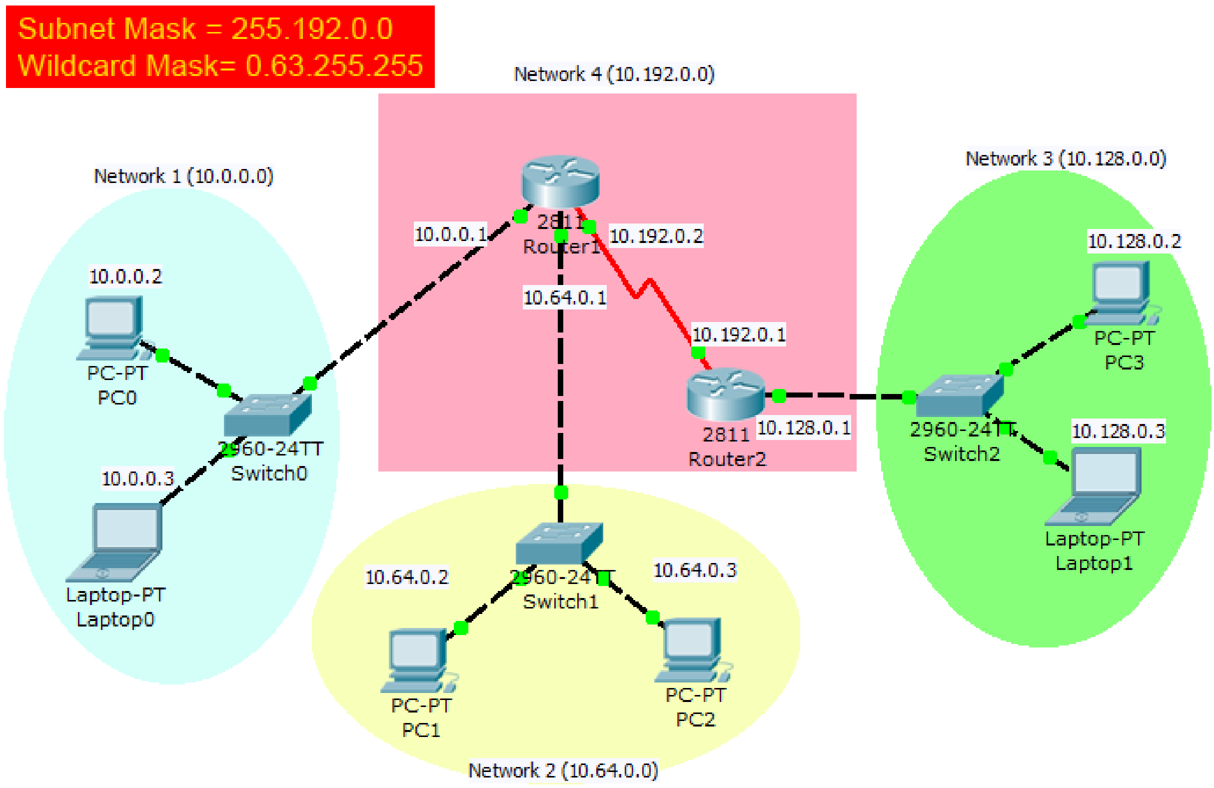
It lets you to calculate sunetting easy.

The networks are 10.0.0.0/10

for the 10.0.0.0 network with the subnet mask 255.192.0.0

Network	Hosts		Broadcast Address
	from	to	
10.0.0.0	10.0.0.1	10.63.255.254	10.63.255.255
10.64.0.0	10.64.0.1	10.127.255.254	10.127.255.255
10.128.0.0	10.128.0.1	10.191.255.254	10.191.255.255
10.192.0.0	10.192.0.1	10.255.255.254	10.255.255.255

Subnet mask = 255.192.0.0, Wildcard Mask is calculated by inverting Subnet mask 255.192.0.0 that is 0.63.255.255



Now let's go to configuration.

<u>Router 1: EIGRP Using wildcard masks</u>

Here we included the 0.63.255.255 Wildcard Mask in the configuration commands.

R1(config)#router eigrp 1
R1(config-router)#network 10.0.0.0 0.63.255.255
R1(config-router)#network 10.64.0.0 0.63.255.255
R1(config-router)#network 10.192.0.0 0.63.255.255
R1(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.192.0.2 (Serial0/2/0) is up: new adjacency

R1(config-router)#exit
R1(config)#
R1#
%SYS-5-CONFIG_I: Configured from console by console

<u>Router 2: EIGRP Using wildcard masks</u>

Router 2 can be configured as the same way

R2(config)#router eigrp 1
R2(config-router)#network 10.128.0.0 0.63.255.255
R2(config-router)#network 10.192.0.0 0.63.255.255
R2(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.192.0.2 (Serial0/2/0) is up: new adjacency
R2(config-router)#exit
R2(config)#

EIGRP Verification and Testing Commands

Now let us familiar some **important commands** that a **Network Admin should know** while dealing with EIGRP.

#show ip eigrp topology

This command shows only feasible successors

R1#show ip eigrp topology

IP-EIGRP Topology Table for AS 1

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,

r - Reply status

P 10.0.0.0/8, 1 successors, FD is 28160

via Connected, FastEthernet0/0

P 20.0.0.0/8, 1 successors, FD is 28160

via Connected, FastEthernet0/1

P 40.0.0.0/8, 1 successors, FD is 20512000

via Connected, Serial0/2/0

P 30.0.0.0/8, 1 successors, FD is 20514560

via 40.0.0.1 (20514560/28160), Serial0/2/**0**

#show ip eigrp topology all-links

This command displays all neighbors, whether feasible successors or not

R1#show ip eigrp topology all-links

IP-EIGRP Topology Table for AS 1

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,

r - Reply status

P 10.0.0.0/8, 1 successors, FD is 28160

via Connected, FastEthernet0/0

P 20.0.0.0/8, 1 successors, FD is 28160

via Connected, FastEthernet0/1

P 40.0.0.0/8, 1 successors, FD is 20512000

via Connected, Serial0/2/0

P 30.0.0.0/8, 1 successors, FD is 20514560

via 40.0.0.1 (20514560/28160), Serial0/2/0

#show ip eigrp topology XX.XX.XX.XX

Gives complete EIGRP details of a specified network path. For example lets verify EIGRP over the network 30.0.0.0 [*where xx.xx.xx.xx is network address*]

R1#show ip eigrp topology 30.0.0.0

IP-EIGRP (AS 1): Topology entry for 30.0.0.0/8

State is Passive, Query origin flag is 1, 1 Successor(s), FD is 20514560

Routing Descriptor Blocks:

40.0.0.1 (Serial0/2/0), from 40.0.0.1, Send flag is 0x0

Composite metric is (20514560/28160), Route is Internal

Vector metric:

Minimum bandwidth is 128 Kbit

Total delay is 20100 microseconds

Reliability is 255/255

Load is 1/255

Minimum MTU is 1500

Hop count is 1

#show ip route

To show updated EIGRP Routing table.

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

C 10.0.0.0/8 is directly connected, FastEthernet0/0
C 20.0.0.0/8 is directly connected, FastEthernet0/1
D 30.0.0.0/8 [90/20514560] via 40.0.0.1, 00:06:01, Serial0/2/0
C 40.0.0.0/8 is directly connected, Serial0/2/0

#show ip route eigrp

Display the route learned through EIGRP only.

R1#show ip route eigrp
D 30.0.0.0/8 [90/20514560] via 40.0.0.1, 00:10:07, Serial0/2/0

#show ip eigrp interfaces

This show command will display all the interfaces participated in the EIGRP process.

R1#show ip eigrp interfaces
IP-EIGRP interfaces for process 1

Xmit Queue Mean Pacing Time Multicast Pending
Interface Peers Un/Reliable SRTT Un/Reliable Flow Timer Routes
Fa0/0 0 0/0 1236 0/10 0 0
Fa0/1 0 0/0 1236 0/10 0 0
Se0/2/0 1 0/0 1236 0/10 0 0

--

#show ip protocols

To show which routing protocol is used in the router.

R1#show ip protocols

Routing Protocol is "eigrp 1 "
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Default networks flagged in outgoing updates
Default networks accepted from incoming updates
EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
EIGRP maximum hopcount 100
EIGRP maximum metric variance 1
Redistributing: eigrp 1
Automatic network summarization is in effect
Automatic address summarization:
Maximum path: 4
Routing for Networks:
10.0.0.0
20.0.0.0
40.0.0.0
Routing Information Sources:
Gateway Distance Last Update
40.0.0.1 90 96258
Distance: internal 90 external 170

Ooops! Thats all about EIGRP configuration

RIP or (E)IGRP Which one I should use?

Which one is better RIP (Routing Information Protocol) or (E)IGRP (Enhanced- Interior Gateway Routing Protocol)? Which one I should use?

However I cannot tell you which of these two protocols are better, because networks may vary in lots of ways. You must have complete awareness about these Routing Protocols and your network topology while choosing those.

Routing **protocol** strictly **depends** on the **network architecture** which you are dealing with. My recommendation is that if you do have the opportunity to use **EIGRP**, then you have to use it over IGRP or RIP. **EIGRP** is absolutely an **improved routing protocol** than both RIP and IGRP.

Conclusion: Students have successfully implemented EIGRP configuration.

Assignment No: 4(B)

Title of the Assignment: Using a Network Simulator (e.g. packet tracer) configure RIPv2 and EIGRP on same network

---

Objective of the Assignment: To understand multiple protocols on same network

---

Prerequisite: Students must have knowledge of Packet tracer simulator.

Theory :

What is Redistribution between multiple routing protocols?

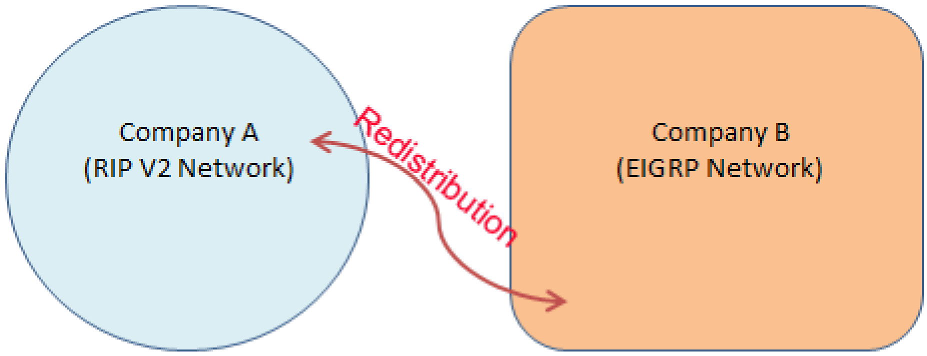
It is the way how routers exchange routing information if two or more different protocols are interconnected. Simply while running multiple routing protocols on same network. For example a company that is running EIGRP and you just bring another company and their network is running OSPF, such conditions are solved by Redistribution. Actually we are going to MIX different protocols by redistribution

What Actually Redistribution means?

- While you redistribute RIP to EIGRP all routes in the **RIP will be inserted into the EIGRP** database and broadcast throughout the autonomous system as an EIGRP External route.
- The same thoughts apply to RIP when you redistribute EIGRP in to RIP, all the routes from **EIGRP will be injected into the RIP** topology table.
- These routes learned by redistribution process will be marked as "**D EX**" routes in the routing table.

Why we Need Redistribution

- Multi-protocol routing is common for many enterprises IP internetworks. They use multi-routing protocol when **company mergers**, several departments managed by various network administrators, and multi-vendor environments etc.
- Organizing different routing protocols is often part of a network design too. In any case, **bearing a multiple protocol** atmosphere **makes redistribution a compulsion**



.

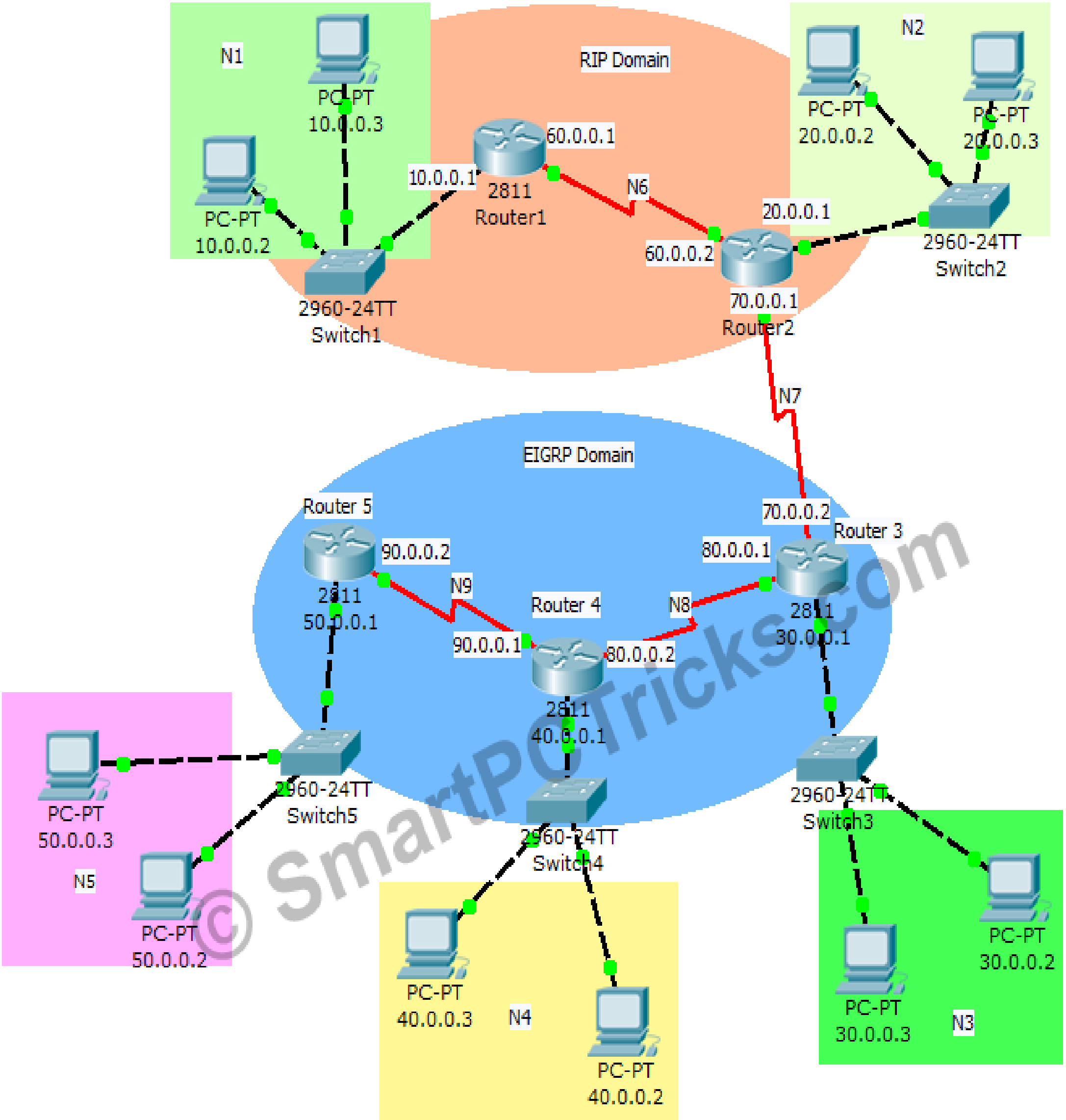
In a nutshell Redistribution required when we are dealing with a **network having different routing protocols**.

We will see How to redistribute RIP to EIGRP and vice versa with Packet Tracer Cisco redistribution example scenario.

Step 1: Initial Configurations

- Listen to the following network scenario and configure each router for IP address assignment (Not shown here). There are two domains called **RIP Domain** and **EIGRP Domain**.

- Once IP assigned, implement RIP V2 on RIP Domain and enforce EIGRP on EIGRP Domain.



Router 1 RIP V2:

R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 10.0.0.0
R1(config-router)#network 60.0.0.0
R1(config-router)#no auto-summary
R1(config-router)#exit
R1(config)#

Since R2 and R3 are the end points of these domains (RIP Domain and EIGRP Domain) implement both protocols on either R2 or R3. In my example I configured R2 with RIP V2 and EIGRP.

Router 2 RIP V2:

R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 20.0.0.0
R2(config-router)#network 60.0.0.0
R2(config-router)#network 70.0.0.0
R2(config-router)#no auto-summary
R2(config-router)#exit

Router 2 EIGRP1:

R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router eigrp 1
R2(config-router)#network 20.0.0.0
R2(config-router)#network 60.0.0.0
R2(config-router)#network 70.0.0.0
R2(config-router)#no auto-summary
R2(config-router)#exit
R2(config)#

Router 3 EIGRP1:
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router eigrp 1
R3(config-router)#network 30.0.0.0
R3(config-router)#network 70.0.0.0
R3(config-router)#network 80.0.0.0
R3(config-router)#no auto-summary
R3(config-router)#exit

Router 4 EIGRP1:

R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R4(config)#router eigrp 1
R4(config-router)#network 40.0.0.0
R4(config-router)#network 80.0.0.0
R4(config-router)#network 90.0.0.0
R4(config-router)#no auto-summary
R4(config-router)#exit
R4(config)#
R4#

Router 5 EIGRP1:

R5#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R5(config)#router eigrp 1
R5(config-router)#network 50.0.0.0
R5(config-router)#network 90.0.0.0
R5(config-router)#no auto-summary
R5(config-router)#exit
R5(config)#

Step 2: Routing Table verification

Now check the routing tables of each router, reveals that R1 don't have information regarding N3, N4, N5, N8 and N9. That indicates only RIP routes are present in the routing table of R1.

Router 1

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

C 10.0.0.0/8 is directly connected, FastEthernet0/0
R 20.0.0.0/8 [120/1] via 60.0.0.2, 00:00:09, Serial0/2/0
C 60.0.0.0/8 is directly connected, Serial0/2/0
R 70.0.0.0/8 [120/1] via 60.0.0.2, 00:00:09, Serial0/2/0
R1#

Router 2

Router 2 has idea about all networks since it is configured with RIP and EIGRP. We may observe the routes leaned by RIP and EIGRP.

R2#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

R 10.0.0.0/8 [120/1] via 60.0.0.1, 00:00:12, Serial0/0/0
C 20.0.0.0/8 is directly connected, FastEthernet0/0
D 30.0.0.0/8 [90/20514560] via 70.0.0.2, 00:03:13, Serial0/2/0
D 40.0.0.0/8 [90/21026560] via 70.0.0.2, 00:03:13, Serial0/2/0
D 50.0.0.0/8 [90/21538560] via 70.0.0.2, 00:03:13, Serial0/2/0
C 60.0.0.0/8 is directly connected, Serial0/0/0
C 70.0.0.0/8 is directly connected, Serial0/2/0
D 80.0.0.0/8 [90/21024000] via 70.0.0.2, 00:03:13, Serial0/2/0
D 90.0.0.0/8 [90/21536000] via 70.0.0.2, 00:03:13, Serial0/2/0
R2#

Router 3, 4 and 5 have only EIGRP routing updates in their routing table.

Router 3

R3#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

D 20.0.0.0/8 [90/20514560] via 70.0.0.1, 00:04:20, Serial0/0/0
C 30.0.0.0/8 is directly connected, FastEthernet0/0
D 40.0.0.0/8 [90/20514560] via 80.0.0.2, 00:04:20, Serial0/2/0
D 50.0.0.0/8 [90/21026560] via 80.0.0.2, 00:04:20, Serial0/2/0
D 60.0.0.0/8 [90/21024000] via 70.0.0.1, 00:04:20, Serial0/0/0
C 70.0.0.0/8 is directly connected, Serial0/0/0
C 80.0.0.0/8 is directly connected, Serial0/2/0

D 90.0.0.0/8 [90/21024000] via 80.0.0.2, 00:04:20, Serial0/2/0
R3#

Router 4

R4#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

D 20.0.0.0/8 [90/21026560] via 80.0.0.1, 00:04:51, Serial0/0/0
D 30.0.0.0/8 [90/20514560] via 80.0.0.1, 00:04:51, Serial0/0/0
C 40.0.0.0/8 is directly connected, FastEthernet0/0
D 50.0.0.0/8 [90/20514560] via 90.0.0.2, 00:04:53, Serial0/2/0
D 60.0.0.0/8 [90/21536000] via 80.0.0.1, 00:04:51, Serial0/0/0
D 70.0.0.0/8 [90/21024000] via 80.0.0.1, 00:04:51, Serial0/0/0
C 80.0.0.0/8 is directly connected, Serial0/0/0
C 90.0.0.0/8 is directly connected, Serial0/2/0
R4#

Router 5

R5#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

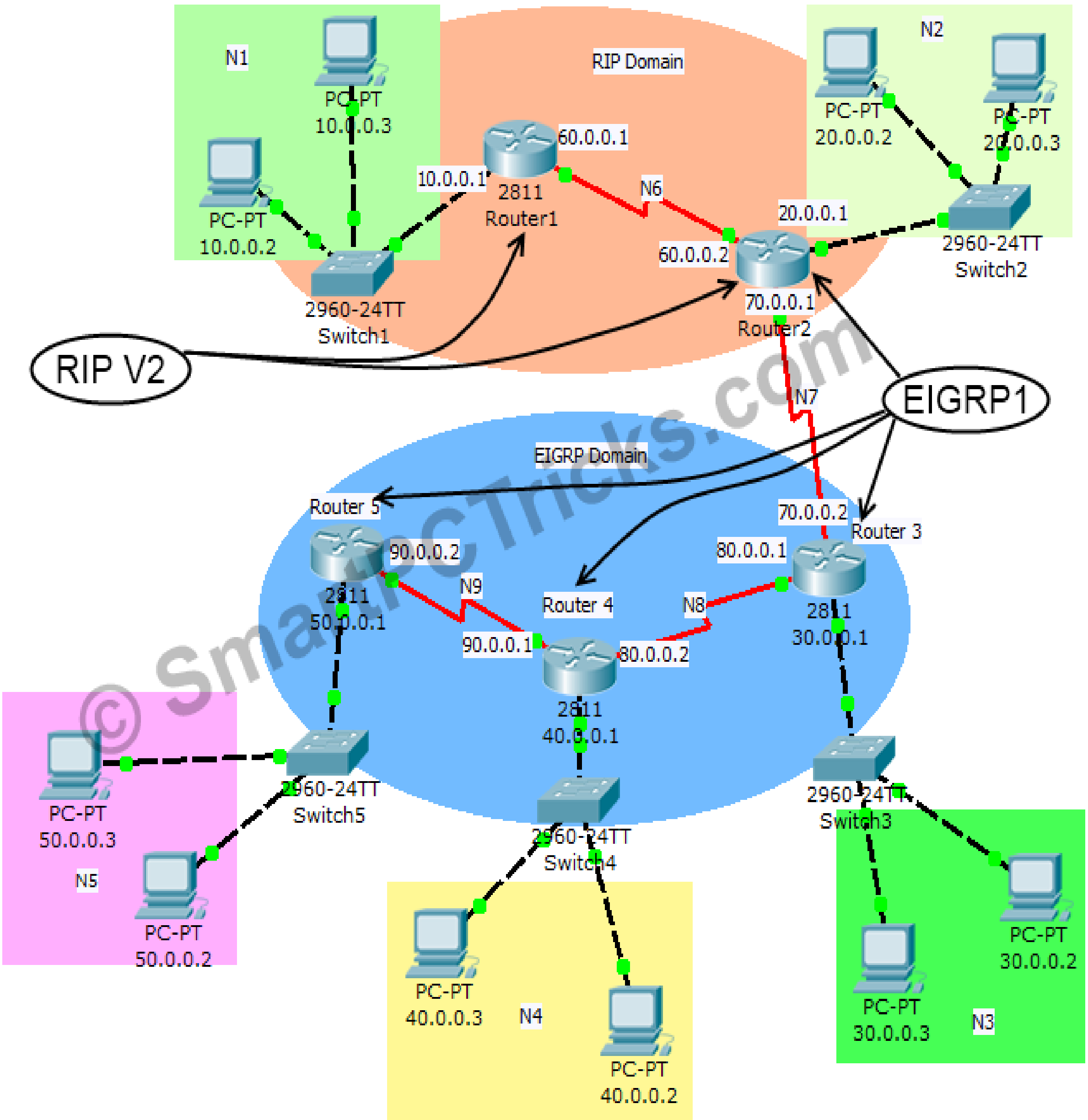
Gateway of last resort is not set

D 20.0.0.0/8 [90/21538560] via 90.0.0.1, 00:05:16, Serial0/2/0
D 30.0.0.0/8 [90/21026560] via 90.0.0.1, 00:05:16, Serial0/2/0
D 40.0.0.0/8 [90/20514560] via 90.0.0.1, 00:05:18, Serial0/2/0
C 50.0.0.0/8 is directly connected, FastEthernet0/0
D 60.0.0.0/8 [90/22048000] via 90.0.0.1, 00:05:16, Serial0/2/0
D 70.0.0.0/8 [90/21536000] via 90.0.0.1, 00:05:16, Serial0/2/0
D 80.0.0.0/8 [90/21024000] via 90.0.0.1, 00:05:18, Serial0/2/0
C 90.0.0.0/8 is directly connected, Serial0/2/0
R5#

<u>So Router 2 running with RIP V2 and EIGRP1, Hence it is aware about all the networks in this topology but other routers not</u>.

Step 3: Redistribution between RIP and EIGRP Protocols

Following figure shows the current configurations structure in each router. Router 2 has RIP V2 and EIGRP1 so **redistribution done in Router 2**. (*Instead of Router 2 we can also use Router 3 if you configured RIP and EIGRP in R3)*



Now we are gonna to **Inject EIGRP in to RIP V2** using Cisco redistribute EIGRP command **#redistribute eigrp <eigrp number> metric <hope count>**

Redistribute EIGRP to RIP

R2(config)#router rip
R2(config-router)#redistribute eigrp 1 metric 5
R2(config-router)#exit
R2(config)#

Here we should enter manually a metric (Hope count) which I entered here is **5**.

Redistribute RIP V2 to EIGRP

R2(config)#router eigrp 1
R2(config-router)#redistribute rip ?
metric Metric for redistributed routes

R2(config-router)#redistribute rip metric ?
Bandwidth metric in Kbits per second
R2(config-router)#redistribute rip metric 10000 ?
EIGRP delay metric, in 10 microsecond units
R2(config-router)#redistribute rip metric 10000 10 ?
EIGRP reliability metric where 255 is 100% reliable
R2(config-router)#redistribute rip metric 10000 10 255 ?
EIGRP Effective bandwidth metric (Loading) where 255 is 100% loaded
R2(config-router)#redistribute rip metric 10000 10 255 100 ?
EIGRP MTU of the path
R2(config-router)#redistribute rip metric 10000 10 255 100 1000

As we know **EIGRP metric** is influenced by **Bandwidth, Delay and Reliability**, hence we should specify those parameters for redistribution. Enter '**?**' if you don't know the syntax, Cisco IOS will **suggest** you the **possible values and its meaning**.

If you check the updated routing table of R3 or R4 or R5, you may see **D EX 10.0.0.0/8 [170/21026560] via 80.0.0.1** which means the <u>**network 10.0.0.0 (N1) is learned via External EIGRP (Redistributed from RIP V2)**</u>.

That's all, Redistribution between RIP and EIGR completed!

Conclusion: Students have successfully implemented RIPv2 and EIGRP on same network

----

Assignment No: 4C

Title of the Assignment: Using a Network Simulator (e.g. packet tracer) configure WLAN protocol WLAN with static IP addressing and DHCP with MAC security and filters

---.--

Objective of the Assignment: To understand WLAN configuration with MAC security

----

Prerequisite: Students must have knowledge of Packet tracer simulator.

Theory :

What is WLAN ?

A wireless local area network (**WLAN**) is a wireless computer network that links two or more devices using a wireless distribution method (often spread-spectrum or OFDM radio) within a limited area such as a home, school, computer laboratory, or office building

WLAN typically extends an existing wired local area network. WLANs are built by attaching a device called the access point (AP) to the edge of the wired network. Clients communicate with the AP using a wireless networkadapter similar in function to a traditional Ethernet adapter.

Network security remains an important issue for WLANs. Random wireless clients must usually be prohibited from joining the WLAN. Technologies like WEP raise the level of security on wireless networks to rival that of traditional wired networks.

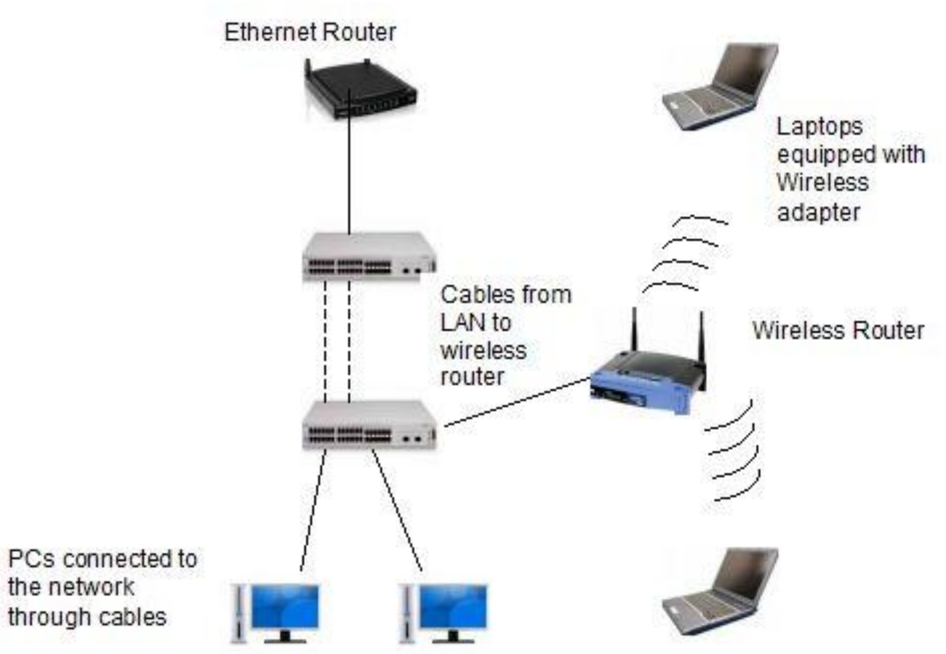


Fig : Access Point connection in WLAN

What is WAP ?

Wireless **access points** (APs or WAPs) are special-purpose communication devices on wireless local area networks (WLANs). Access points act as a central transmitter and receiver of wireless radio signals. Mainstream wireless APs support Wi-Fi and are most commonly used to support public Internet hotspots and other business networks where larger buildings and spaces need wireless coverage.

Access points are small hardware devices closely resembling home broadband routers. (Home routers actually integrate an access point into the rest of the device.) AP hardware consists of radio transceivers, antennas and device firmware.

Access points enable so-called Wi-Fi infrastructure mode networking

Although Wi-Fi connections do not technically require the use of access points, APs enable Wi-Fi networks to scale to larger distances and numbers of clients. Modern access points support up to 255 clients (while very old ones supported only about 20). APs also provide *bridging* capability that enables a Wi-Fi network to connect to other wired networks.

What is WEP ?

Wired Equivalent Privacy, a security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. WEP is designed to provide the same level of security as that of a wired LAN. LANs are inherently more secure than WLANs because LANs are somewhat protected by the physicalities of their structure, having some or all part of the network inside a building that can be protected from unauthorized access. WLANs, which are over radio waves, do not have the same physical structure and therefore are more vulnerable to tampering.

WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another. However, it has been found that WEP is not as secure as once believed. WEP is used at the two lowest layers of the OSI model - the data link and physical layers; it therefore does not offer end-to-end security.

Weakness of WEP ?

WEP's Disadvantage :

WEP's major **weakness is its use of static encryption keys.** When you set up a router with a WEP encryption key, that one key is used by every device on your network to encrypt every packet that's transmitted. But the fact that packets are encrypted doesn't prevent them from being intercepted, and due to some esoteric technical flaws it's entirely possible for an eavesdropper to intercept enough WEP-encrypted packets to eventually deduce what the key is.

What is SSID ?

An Service Set Identifier is the name of a wireless local area network (WLAN). All wireless devices on a WLAN must employ the same SSID in order to communicate with each other.

The SSID on wireless clients can be set either manually, by entering the SSID into the client network settings, or automatically, by leaving the SSID unspecified or blank. A network administrator often uses a public SSID, that is set on the access point and broadcast to all wireless devices in range. Some newer wireless access points disable the automatic SSID broadcast feature in an attempt to improve network security.

SSIDs are case sensitive text strings. The SSID is a sequence of alphanumeric characters (letters or numbers).SSIDs have a maximum length of 32 characters

Introduction to MAC Address:-

The Media Access Control (MAC) address is a binary number used to uniquely identify computer network adapters. These numbers (sometimes called "hardware addresses") are physically burned into the network hardware during the manufacturing process, or stored in firmware, and designed to not be modified.

Some refer to them as "Ethernet addresses" for historical reasons, but most popular types of networks utilize MAC addressing including Ethernet, Wi-Fi and Bluetooth.

Format of MAC address :

- Format of a MAC Address

MAC addresses are 12-digit (48-bit) hexadecimal numbers. By convention, they are usually written in one of the following three formats:

- MM:MM:MM:SS:SS:SS
- MM-MM-MM-SS-SS-SS
- MMM.MMM.SSS.SSS

The leftmost 6 digits (24 bits) called a "prefix" is associated with the adapter manufacturer.

MAC vs. IP Address Relationship

TCP/IP networks use both MAC addresses and IP addresses but for separate purposes. A MAC address remains fixed to the device's hardware while the IP address for that same device can be changed depending on its TCP/IP network configuration. Media Access Control operates at Layer 2 of the OSI model while Internet Protocol operates at Layer 3. This allows MAC addressing to support other kinds of networks besides TCP/IP.

IP networks manage the conversion between IP and MAC addresses using Address Resolution Protocol (ARP). The Dynamic Host Configuration Protocol (DHCP) relies on ARP to manage the unique assignment of IP addresses to devices.

How to Enable MAC Address Filtering on Wireless Access Points and Routers **?**

- Most Wi-Fi access points and routers ship with a feature called hardware or MAC address filtering. This feature is normally turned "off" by the manufacturer, because it requires a bit of effort to set up properly. However, to improve the security of your Wi-Fi LAN (WLAN), strongly consider enabling and using MAC address filtering.

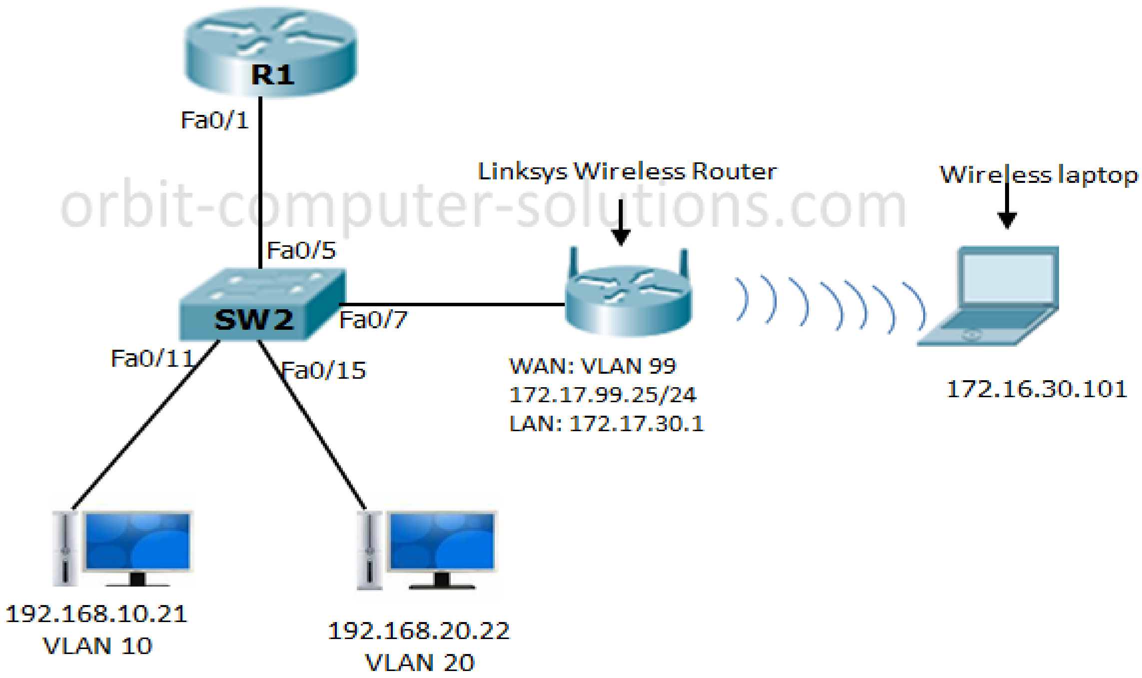
- Without MAC address filtering, any wireless client can join (authenticate with) a Wi-Fi network if they know the network name (also called the SSID) and perhaps a few other security parameters like encryption keys. When MAC address filtering is enabled, however, the access point or router performs an additional check on a different parameter. Obviously the more checks that are made, the greater the likelihood of preventing network break-ins.
- To set up MAC address filtering, you as a WLAN administrator must configure a list of clients that will be allowed to join the network. First, obtain the MAC addresses of each client from its operating system or configuration utility. Then, they enter those addresses into a configuration screen of the wireless access point or router. Finally, switch on the filtering option.
- Once enabled, whenever the wireless access point or router receives a request to join with the WLAN, it compares the MAC address of that client against the administrator's list. Clients on the list authenticate as normal; clients not on the list are denied any access to the WLAN.
- MAC addresses on wireless clients can't be changed as they are burned into the hardware. However, some wireless clients allow their MAC address to be "impersonated" or "spoofed" in software. It's certainly possible for a determined hacker to break into your WLAN by configuring their client to spoof one of your MAC addresses. Although MAC address filtering isn't bulletproof, still it remains a helpful additional layer of defence that improves overall Wi-Fi network security.

WLAN CONFIGURAION TOPOLOGY

How to add and Configure a Wireless Router to a LAN.

On this page, we will look at how to configure a Linksys wireless router, allowing for remote access from PCs as well as wireless connectivity with WEP security. We will use the topology diagram below as sample.

The router **R1** and switch **SW2** had been configured with the appropriate configurations with the LAN and VLAN



R1's configuration:

```
R1(config)#
R1(config)#interface fa0/0
R1(config-if)#IP address 172.17.40.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
!
R1(config) #interface fa0/1
R1(config-if)#no shutdown
Router(config-if)#exit
!
R1(config)#interface fa0/1.10
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#ip address 192.168.10.1 255.255.255.0
R1(config-subif)#exit
!
R1(config)#interface FA0/1.20
R1(config-subif)#encapsulation dot1Q 20
R1(config-subif)#ip address 192.168.20.1 255.255.255.0
R1(config-subif)#end
R1#
!
R1(config)#interface FA0/1.99
R1(config-subif)#encapsulation dot1Q 99
R1(config-subif)#ip address 172.17.99.1 255.255.255.0
R1(config-subif)#end
R1#
```

SW2's Configuration:

```
Sw2#
!
SW2(config)#interface fa0/5
SW2(config-if)#switchport mode trunk
SW2(config-if)#no shutdown
SW2(config-if)#exit
!
SW2(config)#interface fa0/7
SW2(config-if)#switchport access vlan 99
SW2(config-if)#switchport mode access
SW2(config-if)#no shutdown
!
SW2(config-if)#interface fa0/11
SW2(config-if)#switchport access vlan 10
SW2(config-if)#switchport mode access
SW2(config-if)#no shutdown
!
SW2(config-if)#interface fa0/15
SW2(config-if)#switchport access vlan 20
SW2(config-if)#switchport mode access
SW2(config-if)#no shutdown
SW2(config-if)#exit
SW2(config)#
```

Before you begin, you might like to do a reset on the wireless router. In order to clear any previous configurations, do a hard reset. Look for the reset button on the back of the router. Using a pen or other thin instrument, hold down the reset button for 5 - 7 seconds. The router should now be restored to its factory default settings.

Establish physically connectivity.

1. Connect a straight through cable from the Laptop PC to one of the wireless router's LAN ports, labelled Ethernet 1 - 4. By default, the wireless router will provide an IP address to the laptop using default DHCP configurations.

Open a web browser.

2. **Navigate to the wireless router's Web Utility.** You can use **t**he WEB GUI will be used to configure the settings on the wireless router. The GUI can be accessed by navigating to the router's LAN/Wireless IP address with a web browser. The factory default address is **192.168.1.1**.

3. Leave the username blank and set the password to: **admin**.

4. Configure Options in the Linksys Setup Tab.

By default the start-up page is the **Setup** screen. Here, you will need to set the Internet connection type to static IP. In the menus at the top notice you are in the Setup section and under the **Basic Setup** tab.

5. • In the Setup screen for the Linksys router, locate the **Internet Connection Type** option in the **Internet Setup** section of this page. Click the drop-down menu and select **Static IP** from the list.

6. Configure the VLAN 99 IP address, subnet mask, and default gateway for the Linksys Wireless Router**.**

• Set the **Internet IP address** to 172.17.99.25.

• Set the **Subnet Mask** to 255.255.255.0.

• Set the **Default Gateway** to 172.17.99.1.

Note: Typically in a home or small business network, this Internet IP address is assigned by the ISP through DHCP or PPPoE.

7. Configure the router R1 IP parameters.

• Still on the Basic Setup page, scroll down to **Network Setup**. For the **Router IP** fields do the following:

* Set the IP address to **172.17.30.1** and the subnet mask to **255.255.255.0**.

Under the **DHCP Server Setting**, ensure that the DHCP server is **Enabled**.

Click the **Save Settings** button at the bottom of the **Setup** screen.

At this stage, you will notice that the IP address range for the DHCP pool adjusts to a range of addresses to match the Router IP parameters. These addresses are used for any wireless clients that connect to the router's internal switch. Clients receive an IP address and mask, and are given the router IP to use as a gateway.

8. **Set the network name (SSID).**

• Click the **Wireless** tab.

• Under **Network Name (SSID)**, rename the network from **Linksys** to any name of your choice, example orbitcisco1.

• Click **Save Settings**.

9. Set the security mode.

• Click **Wireless Security**. It is located next to **Basic Wireless Settings** in the main **Wireless**tab.

• Change **Security Mode** from **Disabled** to **WEP**.

• Using the default Encryption of 40/64-Bit, set **Key1** to **1234567890 or** any combination of hex digit only,

• Click **Save Settings**.

10. **Set the router password.**

• Click the **Administration** tab.

• Under **Management** in the **Router Access** section, change the router password to **orbit123** or any password of your choosing. Re-enter the same password to confirm.

11. **Enable remote management.**

• In the **Remote Access** section, set **Remote Management** to **Enabled**.

• Click **Save Settings**.

• You may be prompted to log in again. Use the new password of **cisco123** and still keep the username blank

12. **Enable remote management.**

• In the **Remote Access** section, set **Remote Management** to **Enabled**.

• Click **Save Settings**.

• You may be prompted to log in again. Use the new password and still keep the username blank.

13. Add Wireless Connectivity to a laptop PC

i. Disconnect the Ethernet connection from the laptop to Wireless Router.

ii: Use Windows XP to connect to the wireless router.

Below is on how to use Windows XP's built in Wireless Network Connection Utility. Depending on the model of NIC you use, this might be disabled, and you will need to use the utility provided by the NIC manufacturer.

• click **Start > Control Panel > Network Connections**.

• Select the **Wireless Network Connection**.

• Navigate to the **File** menu and select **Status**.

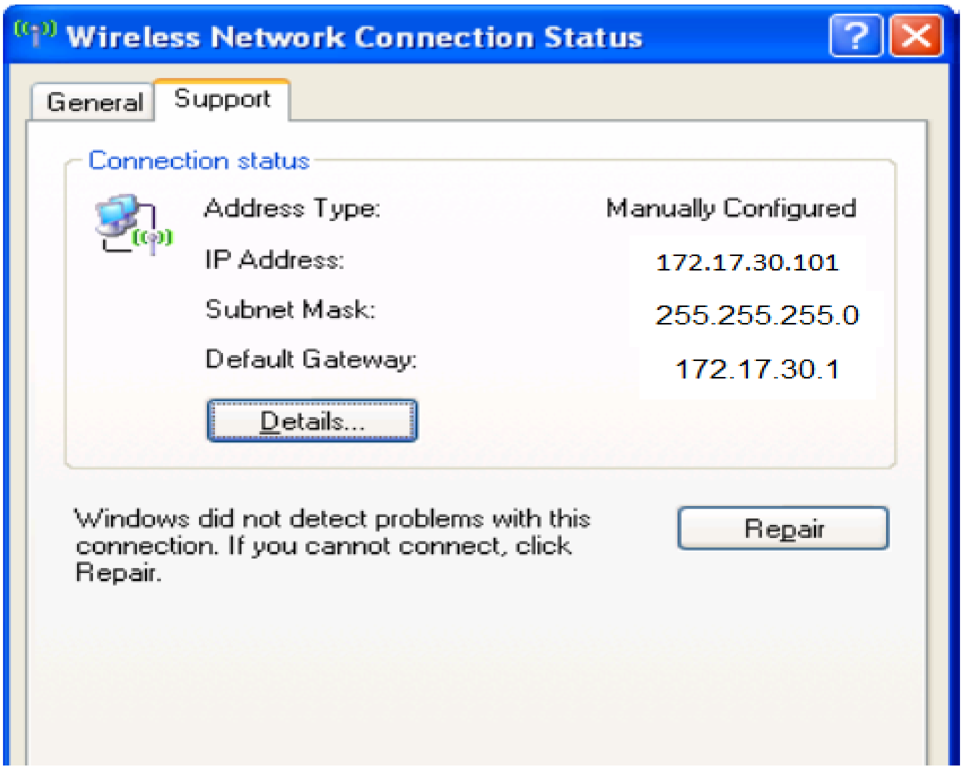
• Click **View Wireless Networks**.

• Locate the '**orbitcisco1** or whatever names you gave to your network **SSID** in the list of available networks and connect to it.

• When prompted for the **WEP** key enter it as above, **1234567890 or** whatever key you used and click **Connect**.

ii. Verify your Connection.

• In the **Status** window, select the **Support** tab. Verify that the Laptop has received an IP address from the Wireless router's DHCP address pool or has been manually configured.



Test your Connection

iv. Ping Wireless router's LAN/Wireless interface.

• On Laptop PC, navigate to the command prompt or click **Start->Run**

• Type **cmd**and select open. This will open the command prompt

• In the command prompt type **ping 172.17.30.1**

v. Ping R1's Fa0/1.99 Interface.

• In the command prompt type **ping 172.17.99.1**

vi. Ping VLAN 10 and VLAN 20 from Laptop PC.

• In the command prompt type **ping 192.168.10.21** to ping VLAN 10.

• Repeat on VLAN 20's address, 192.168.20.22.

The pings should work. If not check or troubleshoot configuration.

Conclusion: Students have successfully understood the concept of WLAN configuration with applying MAC security and filters.