**Efficiency of Different Routing Protocols**

**Sharda University**

**School of Engineering and Technology**

**Computer Science Engineering**

Prepare by:

Yar Mohammad Hafizy

Roll no: 130101202

Ramin Agha Amin

Roll no: 130101137

08/02/2017

# Overview

IP Routing is a term for the set of protocols that determine the path which data travels across multiple networks from its source to its destination. Data is routed from its source to its destination through a series of routers, and across multiple networks. In this paper we configure RIP, EIGRP, and OSPF. Where RIP is a distance vector routing protocol, OSPF is a link state routing protocol, and EIGRP is a hybrid routing protocol.

We start by setting a network topology, assigning IP addresses to the router’s interfaces, enabling routing protocols to the specific topology, providing different types of authentication to specified routing protocols, and verification of each configuration in the routers.

**Routing information protocol:**

IP RIP (Routing Information Protocol) comes in two different versions: 1 and 2. Version 1 is a distance vector protocol and Version 2 is a hybrid protocol.

Routing Information Protocol Version 1 (RIPv1)

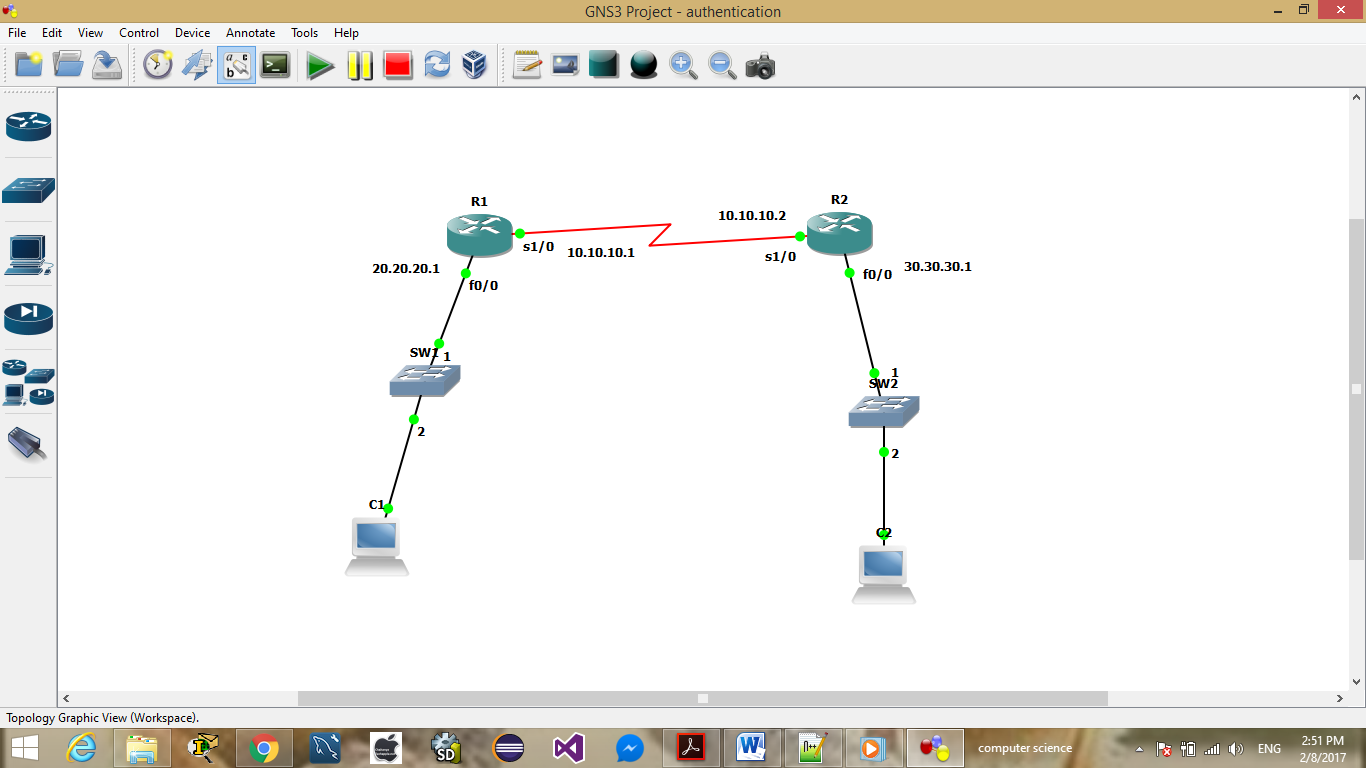
RIPv1 uses local broadcasts to share routing information. These updates are periodic in nature, occurring, by default, every 30 seconds. To prevent packets from circling around a loop forever, both versions of RIP solve counting to infinity by placing a hop count limit of 15 hops on packets. Any packet that reaches the sixteenth hop will be dropped. RIPv1 is a glassful protocol. RIP supports up to six equal-cost paths to a single destination. Equal-cost path are the paths where the metric is same (Hop count).

Routing Information Protocol (RIPv2)

RIPv2 is a distance vector routing protocol with routing enhancements built into it, and it is based on RIPV1. Therefore, it is commonly called as hybrid routing protocol.RIPv2 uses multicasts instead of broadcasts. RIPv2 supports triggered updates. When a change occurs, a RIPv2 router will immediately propagate its routing information to its connected neighbors. RIPv2 is a classless protocol and it supports variable-length subnet masking (VLSM).

Both RIPv1 and RIPv2 uses hop count as the metric.

Note: we do configuration of RIP V2, because this version of routing information protocol supports both types of authentications, and RIPv1 does not support any kind of authentication.



**Objective**: we are going to assign ip address to each interface of the router and configure routing information protocol (RIP) on each router. For accomplishing this task we follow the following steps.

**Step one**: assign IP address to the routers.

Assign IP address to the router one (R1)

R1#configure terminal

R1(config)#interface se1/0

R1(config-if)# ip address 10.10.10.1 255.0.0.0

R1(config-if)#no shut

R1(config)#interface f0/0

R1(config-if)# ip address 20.20.20.1 255.0.0.0

R1(config-if)#no shut

Assign IP address to the router two (R2)

R2#configure terminal

R2(config)#interface se1/0

R2(config-if)# ip address 10.10.10.2 255.0.0.0

R2(config-if)#no shut

R2(config)#interface f0/0

R2(config-if)# ip address 30.30.30.1 255.0.0.0

R2(config-if)#no shut

**Configure terminal:**  by using this command we can go to configuration terminal interface of the router and configure the router, without going to this interface we cannot configure the router.

**Interface fa0/0:** interface is a predefined command and fa0/0 is the interface of the router which is connected to local area network. By using this command we can go into an interface and provide IP address to the interface.

**IP address:** using this command we can define the ip address of the router interface and we can give the subnet mask to the specific IP address. It is (20.20.20.1) the IP address, and it is (255.0.0.0) the subnet mask which specifies the network portion of the IP address.

**No shut:**  this command is used to enable the router’s interface; by default all the interfaces of routers are disabled.

For verifying the configured interfaces we can use:

#show ip interface brief

The above command is used to show details about the each interface of the router.

**Step 2:** configuring routing information protocol

configuring routing information protocol on router one(R1)

R1#configure terminal

R1(config)#router rip

R1(config-router)#version 2

R1(config-router)#network 20.0.0.0 255.0.0.0

R1(config-router)#network 10.0.0.0 255.0.0.0

configuring routing information protocol on router two(R2)

R2#conf t

R2(config)#router rip

R2(config-router)#version 2

R2r(config-router)#network 30.0.0.0 255.0.0.0

R2(config-router)#network 10.0.0.0 255.0.0.0

**Router rip:** this command is used to define the type of routing protocol, which we use for configuration. The routing protocol which is used is RIP routing protocol.

**Version 2:**  this command specifies the version of routing protocol which we want to use for configuration. Here we used the version two of the rip routing protocol, which is better than the version one of the rip routing protocol.

**Network:** this command is used to specify the network address of the interfaces which we already configured. Here the network address (30.0.0.0) is 30 and remaining zeros are for host portion. The subnet mask 255.0.0.0 is used to specify network portion and host portion. 255 shows the network portion and all zeros are used to show the host portion of the IP address.

For verifying RIP protocol

R1#show ip route

**Show ip route:** this command is used to show all the available routes from the flush memory or form nonvolatile RAM (NVRAM).

**RIP authentication**

RIP version one does not support authentication but RIP version two supports authentication, RIP links can require authentication keys (passwords) before they become active. Authentication provides an additional layer of security on the network beyond the other security features. By default, this authentication is disabled.

Authentication keys can be specified in either plain-text or MD5 form. Authentication requires all routers within the RIP network to have the same authentication type and key (password) configured.

**There are two types of authentication**

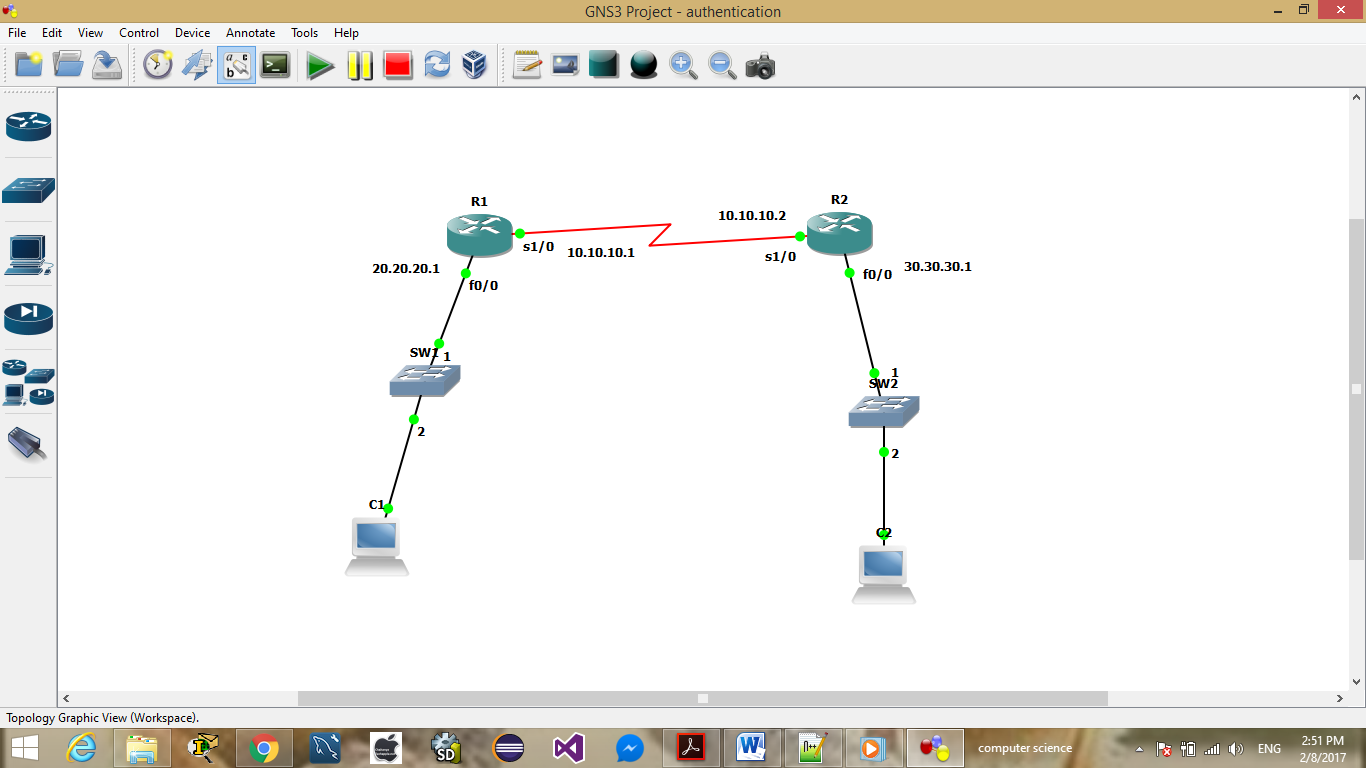
**Simple password authentication**

Routers send packet and key and the other router checks whether the key matches or not, if key does not match the router will not accept. This authentication is not secure because the router sends the key without encryption, hence hackers can easily read the key and hack your router and steal your data. This is mean reason we did not configured this authentication.

**MD5 authentication**

**MD5** stands for message digest five and it is a protocol and used to encrypt your password and key.In this figure a password and key id is configured, router generates a message digest of the key, password and the text we send. Message digest is sent with packet and key is not sent. This authentication is more secure.

Enabling Authentication with MD5 Authentication

for enabling MD5 authentication we need to assign IP address to the routers R1 and R2

step 1: assign IP address to the routers

Assign IP address to the router one (R1)

R1#config t

R1(config)#int se1/0

R1(config-if)# ip add 10.10.10.1 255.0.0.0

R1(config-if)#no shut

R1(config)#int f0/0

R1(config-if)# ip add 20.20.20.1 255.0.0.0

R1(config-if)#no shut

Assign IP address to the router two (R2)

R1#config t

R1(config)#int se1/0

R1(config-if)# ip add 10.10.10.2 255.0.0.0

R1(config-if)#no shut

R1(config)#int f0/0

R1(config-if)# ip add 30.30.30.1 255.0.0.0

R1(config-if)#no shut

**Note:** we explained these command in above for configuring RIP routing protocol

**Step 2:** configure RIP to each router

configuring routing information protocol on router one(R1)

Router#conf t

Router(config)#

Router(config)#router rip

Router(config-router)#version 2

Router(config-router)#network 20.0.0.0 255.0.0.0

Router(config-router)#network 10.0.0.0 255.0.0.0

configuring routing information protocol on router two(R2)

Router#conf t

Router(config)#

Router(config)#router rip

Router(config-router)#version 2

Router(config-router)#network 30.0.0.0 255.0.0.0

Router(config-router)#network 10.0.0.0 255.0.0.0

**Step 3:** provide key chain to each router:

Key chain for router one(R1)

R1# configure terminal

R1(config)# key chain RIP

R1(config-keychain)# key 1

R1(config-keychain-key)# key-string RGjtl5ANYa

R1(config-keychain-key)# end

Key chain for router two (R2)

R1# configure terminal

R1(config)# key chain RIP

R1(config-keychain)# key 2

R1(config-keychain-key)# key-string sharda@123

R1(config-keychain-key)# end

**Key chain**

A key chain is a series of keys that can be created to help ensure secure communication between routers in a network. Authentication occurs whenever neighboring routers exchange information. Plain text authentication sends a plain text key with each message, and plain text is vulnerable to snooping. Key chains allow a rotating series of keys to be used for limited periods of time to decrease the likelihood of a compromise.

The key chain name, “RIP”, is user-defined and can be whatever you want it to be. It does not need to be the same on both routers.

The identifier number of the authentication key,“key 1″, does not need to be identical unless you are using MD5 authentication.

The key string, “**key-string sharda@123**”, is the actual password. It does, of course, need to match on both sides.

**Step 4:** configure md5 to each interface

With everything else in place, MD5 authentication is just one command away. In interface configuration mode, we specify the type of authentication being used with the “ip rip authentication mode …” command. It defaults to plain-text, which is why we did not need to specify it above.

Let’s set the authentication mode to MD5 on R1, then we’ll start a debug on R2 before setting MD5 authentication there as well:

For router one (R1)

R1# configure terminal

R1(config)# interface serial 0/0

R1(config-if)# ip rip authentication mode md5

R1(config-if)# end

**For router two (R2)**

R2# configure terminal

R2(config)# interface serial 0/0

R2(config-if)# ip rip authentication mode md5

R2(config-if)# end

**IP authentication mode:** is used to identify the type of authentication we configure. Here the type of authentication is MD5.

For verifying authentication:

R2# debug ip rip.

**EIGRP (Enhanced Interior Gateway Routing Protocol)**

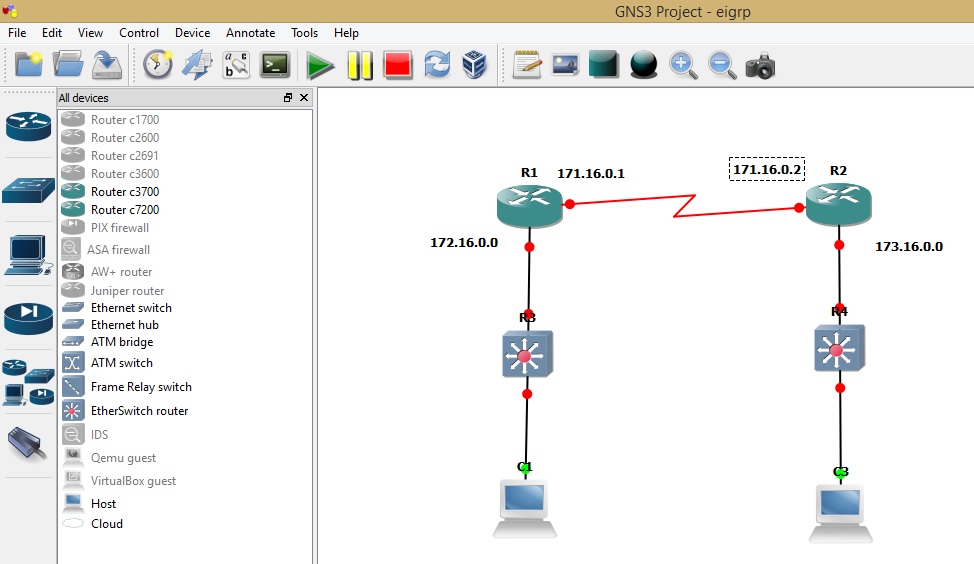
What is EIGRP?

EIGRP is an enhanced version of IGRP. The same distance vector technology found in IGRP is also used in EIGRP, and the underlying distance information remains unchanged. The convergence properties and the operating efficiency of this protocol have improved significantly. This allows for an improved architecture while retaining existing investment in IGRP.

The convergence technology is based on research conducted at SRI International. The Diffusing Update Algorithm (DUAL) is the algorithm used to obtain loop-freedom at every instant throughout a route computation. This allows all routers involved in a topology change to synchronize at the same time. Routers that are not affected by topology changes are not involved in the recompilation. The convergence time with DUAL rivals that of any other existing routing protocol.

EIGRP has been extended to be network-layer-protocol independent, thereby allowing DUAL to support other protocol suites

**Objective:** In this module we are going to configure EIGRP routing protocol on the router R1 and router R2. After configuring EIGRP protocol we provide authentication to each router, manual summarization and load balancing to our network.



**Enabling Eigrp in the following above figure:**

For configuring EIGRP routing protocol, first we have to assign IP address to each interface of the routers, after assigning IP address we should enable the interfaces of the routers.

We did the process of assigning of IP address on each interface RIP configuration.

For R1:

R1(config)# routereigrp42

R1(config-router)# network 172.16.0.0 255.255.0.0

R1(config-router)# network 171.16.0.0 255.255.0.0

R1(config-router)# network 170.16.0.0 255.255.0.0

R1(config-router)# no auto-summary

**For R2:**

R2(config)# routereigrp42

R2(config-router)# network 172.16.0.0 255.255.0.0

R2(config-router)# network 171.16.0.0 255.255.0.0

R2(config-router)# network 170.16.0.0 255.255.0.0

R2(config-router)# no auto-summary

**Router eigrp:**  this command defines the type of internet protocol we are using. Here we use eigrp routing protocol. The number **42** defines the autonomous system number.

**What is an autonomous system number?**

Within the Internet, an autonomous system (AS) is a collection of connected Internet Protocol (IP) routing prefixes under the control of one or more network operators on behalf of a single administrative entity or domain that presents a common, clearly defined routing policy to the Internet.

**No auto-summary**: By default routing protocol like RIP and EIGRP summarize subnets into major class full network at class full boundary. In other word, these protocols perform an auto-summarization each time they crosses a border between two different major networks. To disable this behavior and advertise subnets, 'no auto-summary' command is used. Let's say router has two subnets 172.16.8.0/24 and 172.16.4.0/24 of Class B network and one subnet 10.2.0.0/16 of Class A. When auto-summary is enabled, router will advertise only summarized major class full network 172.16.0.0/16 for class B addresses into its Class A interface but you can change this default behavior and advertise both subnets using this 'no auto-summary'.

**Note:** Above section of this paper has been prepared by Ramin Agha Amin from this part onward has been prepare by Yar Mohammad Hafizy.

**EIGRP Authentication:**

Two routers, R1 and R2, directly connected via their serial 0/0 interfaces. In the previous lab, we were using RIP. This time we’ll use EIGRP and authenticate our routing updates.

The following example enables MD5 authentication on EIGRP packets in autonomous system 42.

For configuring EIGRP authentication we first should assign IP address and configure EIGRP routing protocol on each router, then configure EIGRP authentication.

In EIGRP all steps for providing key chains are same as RIP v2 routing protocol except key chains in EIGRP should be different, not same as RIP authentication.

**R1 Configuration:**

R1# configure terminal

R1(config)# key chain EIGRP

R1(config-keychain)# key 2

R1(config-keychain-key)# key-string sharda@123

R1(config-keychain-key)# end

**R2 Configuration:**

R2# configure terminal

R2(config)# key chain EIGRP

R2(config-keychain)# key 1

R2(config-keychain-key)# key-string sharda@123

R2(config-keychain-key)# end

**R1 Configuration:**

R1# configure terminal

R1(config)# interface serial 0/0

R1(config-if)# ip authentication key-chain eigrp 42 EIGRP

R1(config-if)# ip authentication mode eigrp 42 md5

R1(config-if)# end

**R2 configuration:**

R2# configure terminal

R2(config)# interface serial 0/0

R2(config-if)# ip authentication key-chain eigrp 42 EIGRP

R2(config-if)# ip authentication mode eigrp 42 md5

R2(config-if)# end

**IP authentication mode eigrp 42 md5:** this command is used to provide MD5 authentication in EIGRP routing protocol configured routers. Here **ip authentication mode**  is predefined keywords, and used for specification of kind of authentication, **eigrp**  defines the type of protocol which we use. **42** is autonomous system number, and **md5**  defines the type of authentication we implement.

**Summarization in EIGRP**

Summarization is a process of combing multiple smaller networks into a single large sub network (combining the contagious address into one and send the neighbors). It helps in reducing the size of routing table.

**Types of summarization**

**Auto summarization**

This summarization is done by default via routers itself. All kinds of internet routing protocols support auto summarization. It creates loops and ambiguity in the network, this is why we do not configure it here.

**Manual summarization**

Manual summarization is done to a specific network manually by administrations. It is supported by all classless routing protocols

**Manual summarization configuration**

We do it on router one and it is done on interface level of eigrp, so, we should identify the exact interface where we do summarization.

Example: we do summarization of following IP address

13.0.0.1/24

13.0.1.1/24

13.0.2.1/24

13.0.3.1/24

The summarized IP address is 13.0.0.0/22

Let’s configure manual summarization on serial interface 1/0 , on router one

R1(config)#interface se1/0

R1(config-inter)#ip summary-address eigrp 100 13.0.0.0 255.255.252.0

R1(config-inter)#end

**Ip summary-address eigrp 100:**  **ip summary-address** is predefined command and used for manual summarization in eigrp, **eigrp 100** eigrp is routing protocol and 100 is autonomous system number.

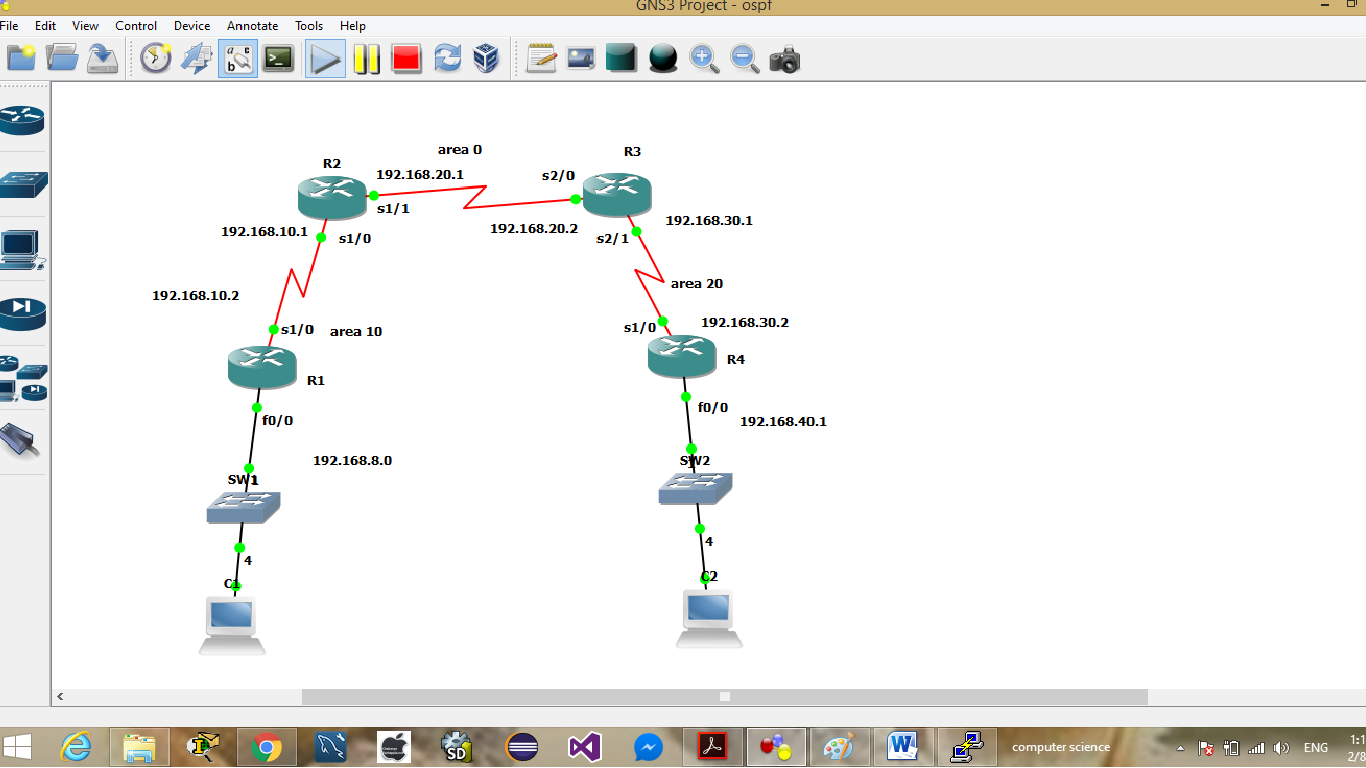
**Open shortest path first (OSPF)**

The Open Shortest Path First (OSPF) protocol is a link state protocol that handles routing for IP traffic. Its newest implementation, version 2, which is explained in RFC 2328, is an open standard. Open Shortest Path First (OSPF) is an open standard (not proprietary) and it will run on most routers independent of make. Open Shortest Path First (OSPF) uses the Shortest Path First (SPF) algorithm, developed by Dijkstra, to provide a loop-free topology. Open Shortest Path First (OSPF) provides fast convergence with triggered, incremental updates via Link State Advertisements (LSAs). Open Shortest Path First (OSPF) is a classless protocol and allows for a hierarchical design with VLSM and route summarization.

**Objective:** our aim is to configure OSPF routing protocol using multiple area, and provide authentication on interfaces of router.

For configuring multiple area OSPF, we should have area zero, and it should act as transaction between other areas. Data packet should be transferred between different other areas through area zero.

**OSPF Configuring Multi-Area:**

****

**Objective**

In this lab we show how to configure OSPF routing protocol with multi area.

**Step 1:** assign IP address to the interfaces of routers.

For assigning ip address we follow same process as we did in RIP V2

Assign IP address to router one (R1)

R1#configure terminal

R1(config)#interface fa0/0

R1(config-if)#ip add 192.168.8.1 255.255.255.0

R1(config-if)#no shut

R1(config-if)#exit

R1(config)#int s1/0

R1(config-if)#ip add 192.168.10.2 255.255.255.0

R1(config-if)#no shut

R1(config-if)#exit

**Assign IP address to the router 2 (R2)**

R2#conf t

R2(config)#interface s1/0

R2(config-if)#ip address 192.168.10.1 255.255.255.0

R2(config-if)#no shut

R2(config-if)#exit

R2(config)#interface s1/1

R2(config-if)#ip add 192.168.20.1 255.255.255.0

R2(config-if)#no shut

R2(config-if)#exit

**Assign IP address to the router 3 (R3)**

R2#configure terminal

R3(config)#interface s2/0

R3 (config-if)#ip address 192.168.20.2 255.255.255.0

R3 (config-if)#no shut

R3 (config-if)#exit

R3 (config)#interface s2/1

R3 (config-if)#ip add 192.168.30.1 255.255.255.0

R3 (config-if)#no shut

R3 (config-if)#exit

**Assign IP address to the router 4 (R4)**

R4#conf t

R4(config)#int fa0/0

R4(config-if)#ip add 192.168.40.1 255.255.255.0

R4(config-if)#no shut

R4(config-if)#exit

R4(config)#int s1/0

R4(config-if)#ip add 192.168.30.2 255.255.255.0

R4(config-if)#no shut

R4(config-if)#exit

**Exit:** this command is used for going one step back to the previous interface.

**Step 2: configuring OSPF routing protocol on router one**

Assign router one’s interfaces in area 10

R1#conf t

R1(config)#router ospf 10

R1(config-router)#network 192.168.8.0 0.0.0.255 area 10

R1(config-router)#network 192.168.10.0 0.0.0.255 area 10

R1(config-router)#exit

**Router ospf 10:** this command is used to specify the type of dynamic routing protocol is use and the autonomous system number (10).

**What is area?**

An OSPF network can be divided into sub-domains called areas. An area is a logical collection of OSPF networks, routers, and links that have the same area identification. A router within an area must maintain a topological database for the area to which it belongs.

**network 192.168.8.0 0.0.0.255 area 10:** this command is used to identify the network address and subnet mask. It also provide the area, it tells the current network is in part of area 10.

**configuring OSPF routing protocol on router two(R2)**

assign the router interfaces s1/0 network (192.168.10.0) to area 10 and assign the router interface se1/1 to area zero

R2#conf t

R2(config)#router ospf 20

R2(config-router)#net

R2(config-router)#network 192.168.2.0 0.0.0.255 area 0

R2(config-router)#network 192.168.10.0 0.0.0.255 area 10

R2(config-router)#exit

**configuring OSPF routing protocol on router three(R3)**

assign the router interfaces s2/0 network (192.168.20.0) to area zero and assign the router interface se2/1 to area 20

R3#conf t

R3(config)#router ospf 30

R3(config-router)#net

R3(config-router)#network 192.168.2.0 0.0.0.255 area 0

R3(config-router)#network 192.168.30.0 0.0.0.255 area 10

R3(config-router)#exit

**configuring OSPF routing protocol on router four(R4)**

Assign router one’s interfaces in area 20

R4#conf t

R4(config)#router ospf 40

R4(config-router)#net

R4(config-router)#network 192.168.3.0 0.0.0.255 area 20

R4(config-router)#network 192.168.40.0 0.0.0.255 area 20

R4(config-router)#exit

**For verifying OSPF routes**

R1# show ip route

Or

**R1#show ip protocol**

This command is used to show the type of configured routing protocol from flush memory

**R1#show ip ospf database**

This command is used to show the complete database of router about the networks, it gives the complete routes which exist in the network.

**R1#show ip ospf neighbor**

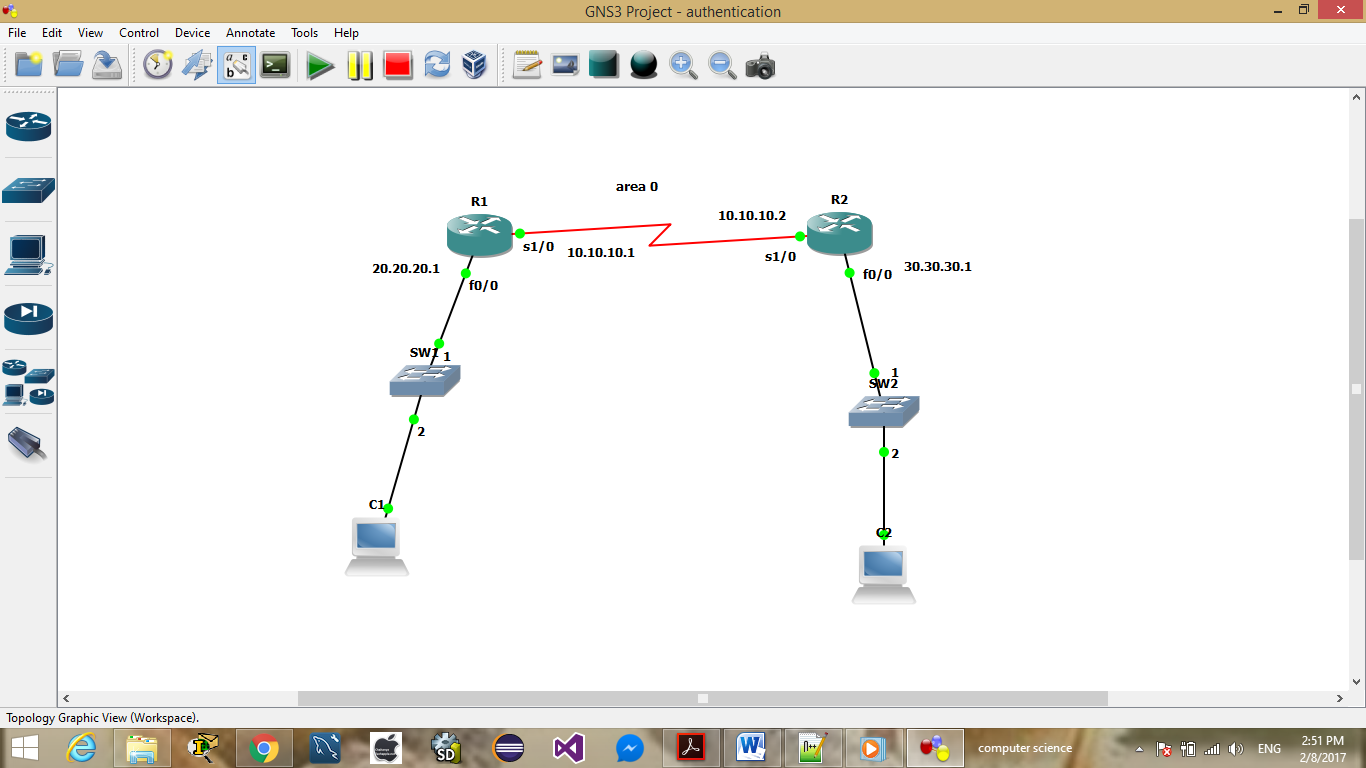
This command is used to show the directly connected neighbors from flush memory.

**Note:** area zero should be backbone it means all other areas should be connected to area zero and area 0 should be as transit.

**Configuring OSPF Authentication**

OSPF authentication comes in two forms: plain-text and MD5. Because a secure method was specified, we have to use MD5 authentication in our environment (plain-text is not secure).

We configure clear text authentication and message digest five on this topology:



**Configurations for Plain Text Authentication**

Plain text authentication is used when devices within an area cannot support the more secure MD5 authentication. Plain text authentication leaves the internetwork vulnerable to a "sniffer attack," in which packets are captured by a protocol analyzer and the passwords can be read. However, it is useful when you perform OSPF reconfiguration, rather than for security. For example, separate passwords can be used on older and newer OSPF routers that share a common broadcast network to prevent them from talking to each other. Plain text authentication passwords do not have to be the same throughout an area, but they must be the same between neighbors.

**For configuring plain text authentication we should follow the following process:**

**Step 1:** assign IP address to the interfaces of routers

**Step 2:** configure OSPF routing protocol on each router

**Step3:** configure clear text authentication

**Step 1:** assign IP address to the interfaces of router one (R1)

R1(config)#interface se1/0

R1(config-if)# ip address 10.10.10.1 255.0.0.0

R1(config-if)#no shut

R1(config)#interface f0/0

R1(config-if)# ip address 20.20.20.1 255.0.0.0

R1(config-if)#no shut

**Step 2: configure OSPF routing protocol on each router**

R1(config)#router ospf 10

R1(config-router)#network 10.0.0.0 0.255.255.255 a 0

R1(config-router)#network 20.0.0.0 0.255.255.255 a 0

R1(config-router)#exit

**Step3: configure clear text authentication**

R1(config)#interface se1/0

R1(config-if)#ip ospf authentication

R1(config-if)#ip ospf authentication-key cisco123

R1(config-router)#exit

**Authentication on router two (R2)**

**Step 1:** assign IP address to the interfaces of routers

R2(config)#int se1/0

R2(config-if)# ip add 10.10.10.2 255.0.0.0

R2(config-if)#no shut

R2(config)#interface f0/0

R2(config-if)# ip add 30.30.30.1 255.0.0.0

R2(config-if)#no shut

**Step 2:** configure OSPF routing protocol on R2

R2(config)#router ospf 10

R2(config-router)#network 10.0.0.0 0.255.255.255 a 0

R2(config-router)#network 30.0.0.0 0.255.255.255 a 0

R2(config-router)#exit

**Step3:** configure clear text authentication

R2(config)#interface se1/0

R2(config-if)#ip ospf authentication

R2(config-if)#ip ospf authentication-key cisco123

R2(config-router)#exit

**Exit:** it is used to go one step back to the configuration

**ip ospf authentication-key cisco123:** in this command, **ip ospf**  is used to say that, it is using ospf routing protocol for authentication, **authentication-key** it is a predetermined command and used for configure authentication in ospf routing protocol, and **cisco123**  is the actual password for authentication, it is user defined password, it means you can give any kind of password according to your wish.

**Message digest 5 authentication**

When you use MD5 OSPF authentication, a key and a key id must be configured on routers. From this key and key id a hash is generated, which is added to OSPF packet header.

This authentication does encrypts the password, so, hackers cannot easily hack the password.it is very secure as compare to plain text authentication.

We work on the same topology which we did for clear text authentication

**Step 1**: assign IP address to each interfaces of router

**Step 2:** configure OSPF on each router

We did these two steps in above clear text authentication. We need to configure MD5 only on each interface of routers

**Now configure MD5 on router one (R1)**

R1(config)#int se1/0

R1(config-if)#ip ospf ip ospf authentication message-digest

R1(config-if)#ip ospf message-digest-key 2 md5 cisco123

R1(config-router)#exit

**Now configure MD5 on router two (R2)**

R1(config)#interface se1/0

R1(config-if)#ip ospf authentication message-digest

R1(config-if)#ip ospf message-digest-key 2 md5 cisco123

R1(config-router)#exit

**ip ospf ip ospf authentication message-digest:** this command is used to configure MD5 authentication on the interface. Here we specify the type of routing protocol which is OSPF and the mode of authentication, which is message-digest (MD5).