



Discipline

**Routing Protocols, WAN, NAT, PAT & Administrative
Function**

CS5001

Assignment 3

Sheikh Muhammed Tadeeb (AU19B1014)

❖ Problem Statement:

1. Routing Protocols (any two)
2. Short Summary about
 - a. Difference between WAN and WLAN.
 - b. WAN encapsulations.
3. What is meant by NAT and PAT in Computer Networks? Explain with example.
4. Administrative Functions of Cisco Devices. What you will carry out to secure your devices?

❖ Solution:

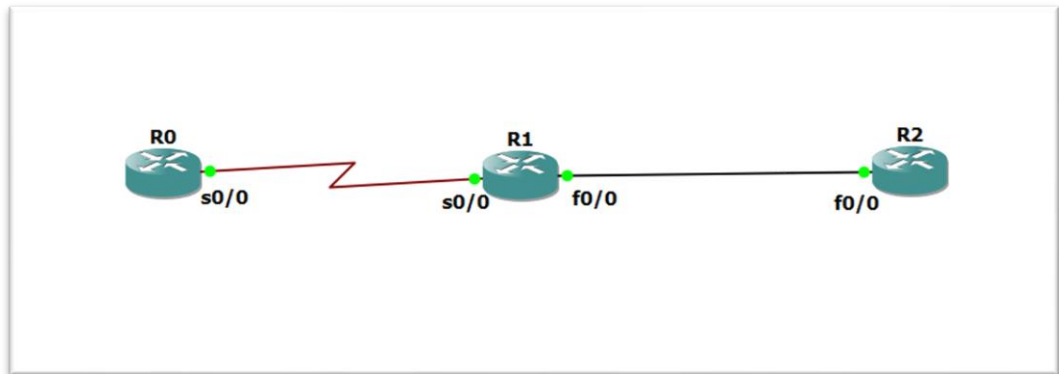
1. Routing Protocols:

1.1 Rip v2 protocol:

- A quick summary of RIPv2:
 - 1) Routing Information Protocol (RIP) is a true distance-vector routing protocol.
 - 2) RIP permits a hop count of up to 15, so anything that requires 16 hops is deemed unreachable.
 - 3) RIP sends the complete routing table out to all active interfaces every 30 seconds(RIP updates occur every 30 seconds).
 - 4) RIP version 2 does send subnet mask information with the route updates. This is called classless routing.
 - 5) RIP only uses hop count to determine the best way to a remote network (a hop is a router).
 - 6) Administrative Distance is 120.

7) Support VLSM & discontinuous networks Below is the topology of this lab.

- Diagram:



- Configuration:

Configuring interfaces for R0:

```
R0(config)# interface s0/0
R0(config-if)# ip address 192.168.1.2 255.255.255.0
R0(config-if)# no shutdown
R0(config-if)# interface lo0
R0(config)# ip address 12.0.0.1 255.0.0.0
```

Configuring interfaces for R1:

```
R1(config)# interface s0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# interface f0/0
R1(config-if)# ip address 192.168.2.1 255.255.255.0
R1(config-if)# no shutdown
```

Configuring interfaces for R2:

```
R2(config)# interface f0/0
```

```
R2(config-if)# ip address 192.168.2.2 255.255.255.0
```

```
R2(config-if)# interface lo0
```

```
R2(config-if)# ip address 200.200.200.1 255.255.255.0
```

Before enable RIP we should check the routing table on these routers to understand what has been changed in these routers.

```
R0#show ip route
Codes: C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, 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    12.0.0.0/8 is directly connected, Loopback0
---
```

```
R1#show ip route
Codes: C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, 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    192.168.2.0/24 is directly connected, FastEthernet0/0
D1#
```

```
R2#show ip route
Codes: C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, 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    200.200.200.0/24 is directly connected, Loopback0
R2#
```

Notice that these 3 routers only see the directly connected routers. Now if you ping from the loopback (or any interface) of R0 to the loopback (or any interface) of R2 then it will not be successful because R0 doesn't know which interface it should send the packets out to reach network 200.200.200.0.

- Rip v2 enabling:

Now we'll enable RIP v2 on three routers, so

Enabling for R0:

```
R0(config)# router rip
R0(config-router) # version 2
R0(config-router) # network 12.0.0.0
R0(config-router)# network 192.168.1.0
```

Enabling for R1:

```
R1(config)# router rip
R1(config-router)# version 2
R1(config-router)# network 192.168.1.0
R1(config-router)# network 192.168.2.0
```

Enabling for R2:

```
R2(config)# router rip
R2(config-router)# version 2
R2(config-router)# network 200.200.200.0
R2(config-router)# network 192.168.2.
```

- Output:

```
R0#show ip route
Codes: C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, 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    12.0.0.0/8 is directly connected, Loopback0
C    192.168.1.0/24 is directly connected, Serial0/0
R    192.168.2.0/24 [120/1] via 192.168.1.1, 00:00:06, Serial0/0
R0#
```

```
R1#show ip route
Codes: C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, 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

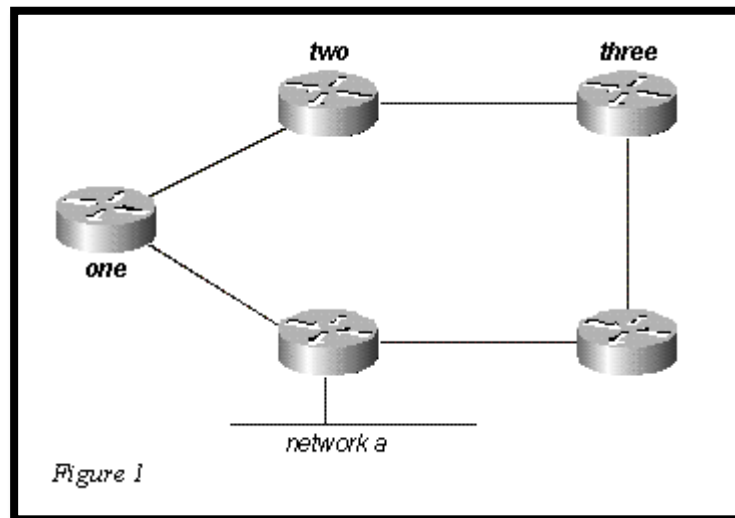
R    12.0.0.0/8 [120/1] via 192.168.1.2, 00:00:01, Serial0/0
C    192.168.1.0/24 is directly connected, Serial0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
R1#
```

Now we can ping from the R0's loopback interface to the R2's loopback interface as the routing table of R0 has a path to R2's loopback interface and vice versa.

1.2 EIGRP:

- Basic Theory:

A typical distance vector protocol saves the following information when computing the best path to a destination: the distance (total metric or distance, such as hop count) and the vector (the next hop). For instance, all the routers in the network in Figure 1 are running Routing Information Protocol (RIP). Router Two chooses the path to Network A by examining the hop count through each available path.



Since the path through Router Three is three hops, and the path through Router One is two hops, Router Two chooses the path through One and discards the information it learned through Three. If the path between Router One and Network A goes down, Router Two loses all connectivity with this destination until it times out the route of its routing table (three update periods, or 90 seconds), and Router Three re-advertises the route (which occurs every 30 seconds in RIP). Not including any hold-down time, it will take between 90 and 120 seconds for Router Two to switch the path from Router One to Router Three.

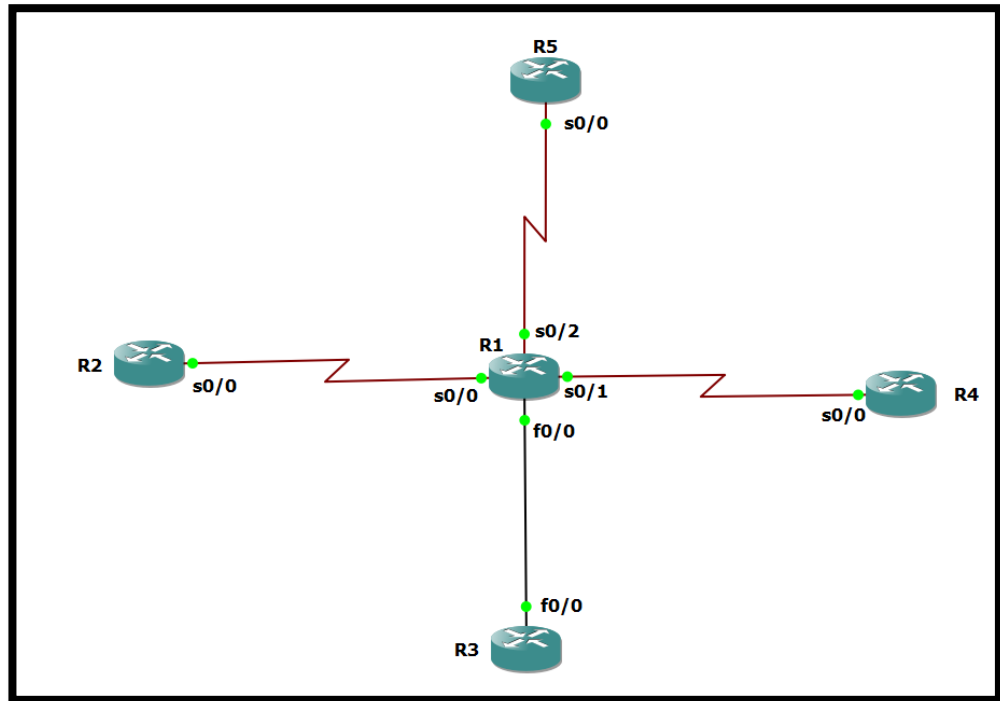
EIGRP, instead of counting on full periodic updates to re-converge, builds a topology table from each of its neighbour's advertisements (rather than discarding the data), and converges by either looking for a likely loop-free route in the topology table, or, if it knows of no other route, by querying its neighbours. Router Two saves the information it received from both Routers One and Three. It chooses the path through One as its best path (the successor) and the path through Three as a loop-free path (a feasible successor). When the path through Router One becomes unavailable, Router Two examines its topology table and, finding a feasible successor, begins using the path through Three immediately.

From this brief explanation, it is apparent that EIGRP must provide:

- A system where it sends only the updates needed at a given time; this is accomplished through neighbour discovery and maintenance
- A way of determining which paths a router has learned are loop-free.
- A process to clear bad routes from the topology tables of all routers on the network.

- A process for querying neighbours to find paths to lost destinations

- Diagram:



This lab consists of 5 routers and we need to configure EIGRP among them. It is done when we can successfully ping among R2, R3, R4 & R5 and the routing tables of these routers show that they are running EIGRP (with letter “D”).

IP addresses of routers:

For R1:

s0/0 – 192.168.30.12/28

s0/1 – 192.168.30.18/28

s0/2 – 192.168.30.35/28

f0/0 – 192.168.60.10/28

For R2:

s0/0 – 192.168.30.13/28

For R3:

f0/0 – 192.168.60.13/28

For R4:

s0/0 – 192.168.30.20/28

For R5:

s0/0 – 192.168.30.40/28

- Configuration:

Configuring interfaces for R1:

```
R1# config t
R1(config)# int s0/0
R1(config-if)# ip address 192.168.30.12 255.255.255.240
R1(config-if)# no shut
R1(config-if)# int s0/1
R1(config-if)# ip address 192.168.30.18 255.255.255.240
R1(config-if)# no shut
R1(config-if)# int s0/2
R1(config-if)# ip address 192.168.30.35 255.255.255.240
R1(config-if)# no shut
R1(config-if)# int f0/0
R1(config-if)# ip address 192.168.60.10 255.255.255.240
R1(config-if)# no shut
```

Configuring interfaces for R2:

```
R2# config t
R2(config)# int s0/0
R2(config-if)# ip address 192.168.30.13 255.255.255.240
R2(config-if)# no shut
```

Configuring interfaces for R3:

```
R3# config t
R3(config)# int f0/0
R3(config-if)# ip address 192.168.60.13 255.255.255.240
R3(config-if)# no shut
```

Configuring interfaces for R4:

```
R4# config t
R4(config)# int s0/0
R4(config-if)# ip address 192.168.30.20 255.255.255.240
R4(config-if)# no shut
```

Configuring interfaces for R5:

```
R5# config t
R5(config)# int s0/0
R5(config-if)# ip address 192.168.30.40 255.255.255.240
R5(config-if)# no shut
```

We can see all the neighbours of R1 with the “show cdp neighbours” command on R1:

```
R1#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID         Local Intrfce   Holdtme    Capability   Platform   Port ID
R2                Ser 0/0         137        R S I       3745       Ser 0/0
R3                Fas 0/0         167        R S I       3745       Fas 0/0
R4                Ser 0/1         175        R S I       3745       Ser 0/0
R5                Ser 0/2         177        R S I       3745       Ser 0/0
```

At this time we can ping between two directly connected interfaces. For example a ping from s0/0 of R1 to s0/0 of R2 (192.168.30.13) will be successful.

```
R1#ping 192.168.30.13
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.13, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/7/20 ms
R1#
```

But a ping between two far-away interfaces is not successful. For example, a ping from R2 to s0/0 of R4 (192.168.30.20) will be unsuccessful.

```
R2#ping 192.168.30.20
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.20, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R2#
```

If we use the “show ip route” on these routers we will only see directly connected link.

```

R1#show ip route
Codes: C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, 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

192.168.30.0/28 is subnetted, 3 subnets
C    192.168.30.32 is directly connected, Serial0/2
C    192.168.30.16 is directly connected, Serial0/1
C    192.168.30.0 is directly connected, Serial0/0
192.168.60.0/28 is subnetted, 1 subnets
C    192.168.60.0 is directly connected, FastEthernet0/0
R1#

```

- EIGRP Enabling:

Enabling for R1:

```

R1(config)# router eigrp 100
R1(config-router)# network 192.168.30.0
R1(config-router)# network 192.168.60.0
R1(config-router)# no auto-summary

```

Enabling for R2:

```

R2(config)# router eigrp 100
R2(config-router)# network 192.168.30.0
R2(config-router)# no auto-summary

```

Enabling for R3:

```

R3(config)# router eigrp 100
R3(config-router)# network 192.168.60.0
R3(config-router)# no auto-summary

```

Enabling for R4:

```

R4(config)# router eigrp 100
R4(config-router)# network 192.168.30.0
R4(config-router)# no auto-summary

```

Enabling for R5:

```
R5(config)# router eigrp 100
R5(config-router)# network 192.168.30.0
R5(config-router)# no auto-summary
```

Now the EIGRP process is up and we can ping from anywhere. For example, a ping from R2 to s0/0 of R4 (192.168.30.20) will be successful now.

```
R2#ping 192.168.30.20
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.20, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/16 ms
R2#
```

By checking the routing table of R2, R3, R4 & R5 we can confirm EIGRP has been implemented successfully. For example, using the “show ip route” command on R5 we see

```
R5#
R5#show ip route
Codes: C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, 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

    192.168.30.0/28 is subnetted, 3 subnets
C       192.168.30.32 is directly connected, Serial0/0
D       192.168.30.16 [90/2681856] via 192.168.30.35, 00:04:06, Serial0/0
D       192.168.30.0 [90/2681856] via 192.168.30.35, 00:04:06, Serial0/0
    192.168.60.0/28 is subnetted, 1 subnets
D       192.168.60.0 [90/2195456] via 192.168.30.35, 00:02:18, Serial0/0
R5#
R5#
R5#
```

We can check the neighbour relationships on these routers with the “show ip eigrp neighbors” command. Below is an example of R1:

```
R1#
R1#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address                Interface         Hold Uptime   SRTT  RTO  Q  Seq
                               (sec)          (ms)                Cnt Num
2   192.168.30.40           Se0/2             11 00:06:23    17   200  0   7
1   192.168.30.20           Se0/1             11 00:07:38    16   200  0   7
0   192.168.30.13           Se0/0             11 00:09:32    16   200  0  11
R1#
```




To see the topologies of these routers, use the “show ip eigrp topology” command. Below is the output of R4







```
R4#
R4#show ip eigrp topology
IP-EIGRP Topology Table for AS(100)/ID(192.168.30.20)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 192.168.60.0/28, 1 successors, FD is 2195456
   via 192.168.30.18 (2195456/281600), Serial0/0
P 192.168.30.32/28, 1 successors, FD is 2681856
   via 192.168.30.18 (2681856/2169856), Serial0/0
P 192.168.30.16/28, 1 successors, FD is 2169856
   via Connected, Serial0/0
P 192.168.30.0/28, 1 successors, FD is 2681856
   via 192.168.30.18 (2681856/2169856), Serial0/0
R4#
```

2. Short-Summary:

a) Difference between WAN and WLAN:

WLAN	WAN
1. Abbreviation 	
WLAN stands for Wireless Local Area Network, it is also called as LANW i.e., Local Area Wireless Network.	WAN stands for Wide Area Network.
2. Performance 	
The performance of WLAN is usually high compared to other wireless networks	In WAN the WWAN performance is low compared to another wireless network
3. Coverage 	
It is covered within a building, a campus or maybe tech parks	It is established city wise, Countrywide and even Worldwide
4. Standard	

	
The standards of WLAN are HiperLAN, Wi-fi and IEEE 802.11	The Standard are usually measured in Ethernet, 2G or 3G
5. Services 	
It provides service in Local Area to desktop, Laptop, mobile phones and all the devices that work on internet.	A wide area network (WAN) is a geographically distributed private telecommunications network that interconnects multiple local area networks (LANs)
6. Installation / Set-up 	
WLAN is an affordable method and can be setup in 24 hours or less.	Replacement/Setup is costly and in case of WWAN an ISP contact should be made for Internet service access which is high.
7. Security 	
WLAN is not as secure as WAN	WAN provides better security because of its 128-bit encryption in WWAN and cable connection is always secure than wireless connection.
8. Speed 	
It works faster because of its short-range establishment	It is not as fast as WLAN because of its global range of access.
9. Connecting Links 	
As the name suggest it is a wireless technology	Its ca be both wired as well as wireless

10. Technology

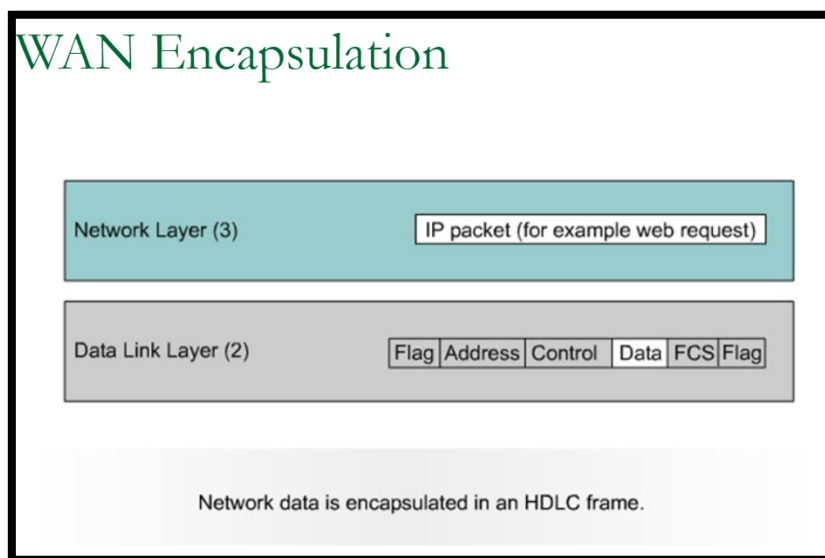


It is a temporary network formed with a limited number of users in short range

It belongs to the family of GSM, CDMA or CDMA 2000. Belong to cellular family to transmit & receive data.

b) WAN Encapsulation:

Network layer passes the data to the data link layer for transmission over the physical layer. The Data Link layer creates frames by adding the necessary checks and controls around the Network layer data. The encapsulation on a router serial interface must be configured to guarantee the correct encapsulation method is used. Different WAN technologies use different encapsulation methods. So, the selection of WAN encapsulation protocol depends on the WAN technology and the communicating equipment.



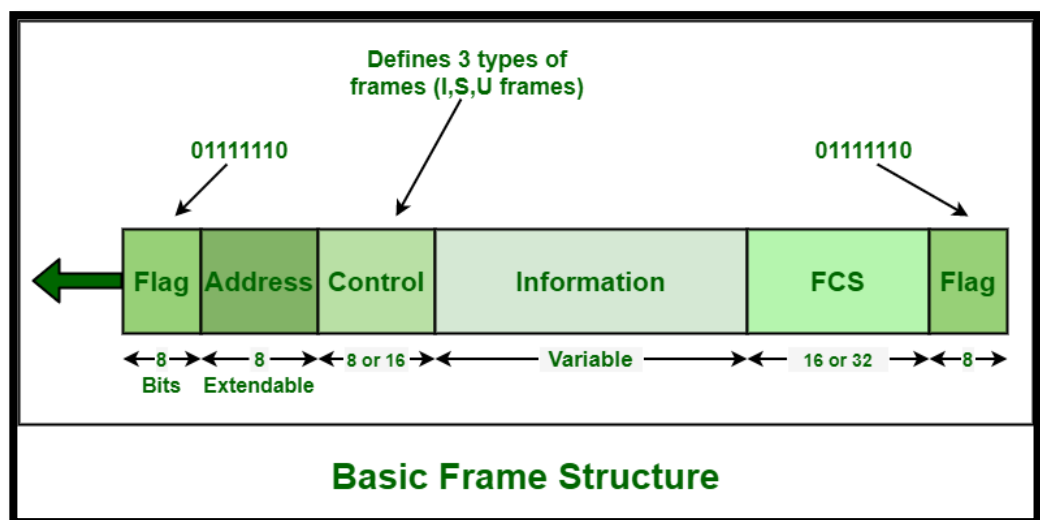
Each WAN encapsulation protocols usually accompany a certain connection type. The important WAN encapsulation protocols are Point-to-Point Protocol (PPP), High-Level Data Link Control (HDLC), Frame Relay, Asynchronous Transfer Mode (ATM), X.25, and Serial Line Internet Protocol (SLIP). HDLC is the most common encapsulation protocol type and most framing protocols are based on it.

- Types

The following are short descriptions of each type of WAN protocol:

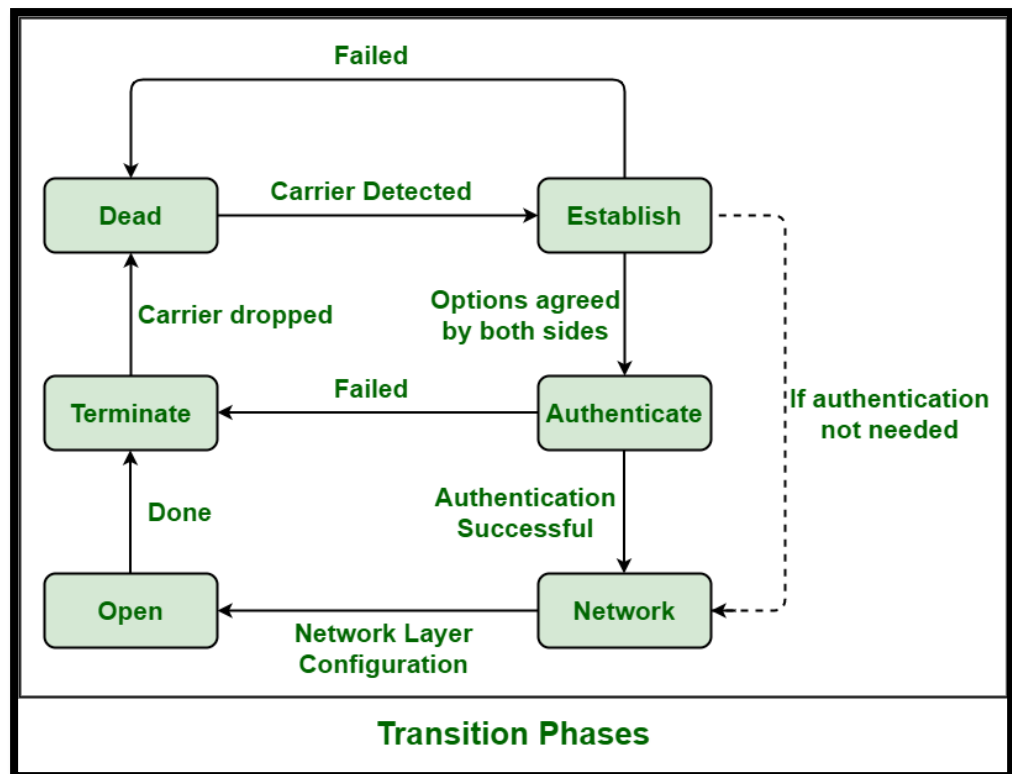
1) *High-Level Data Link Control (HDLC):*

HDLC is the default encapsulation protocol type on point-to-point connections, dedicated links, and circuit-switched links when the link uses two Cisco devices. It is a synchronous Data Link layer bit-oriented protocol originally developed from the Synchronous Data Link Protocol (SDLC) and became standardized by ISO as ISO 13239. It provides both connection-oriented and connectionless service. HDLC also provides flow control and error control by using acknowledgements. Cisco uses a proprietary version of the HDLC protocol known as Cisco HDLC (HDLC).



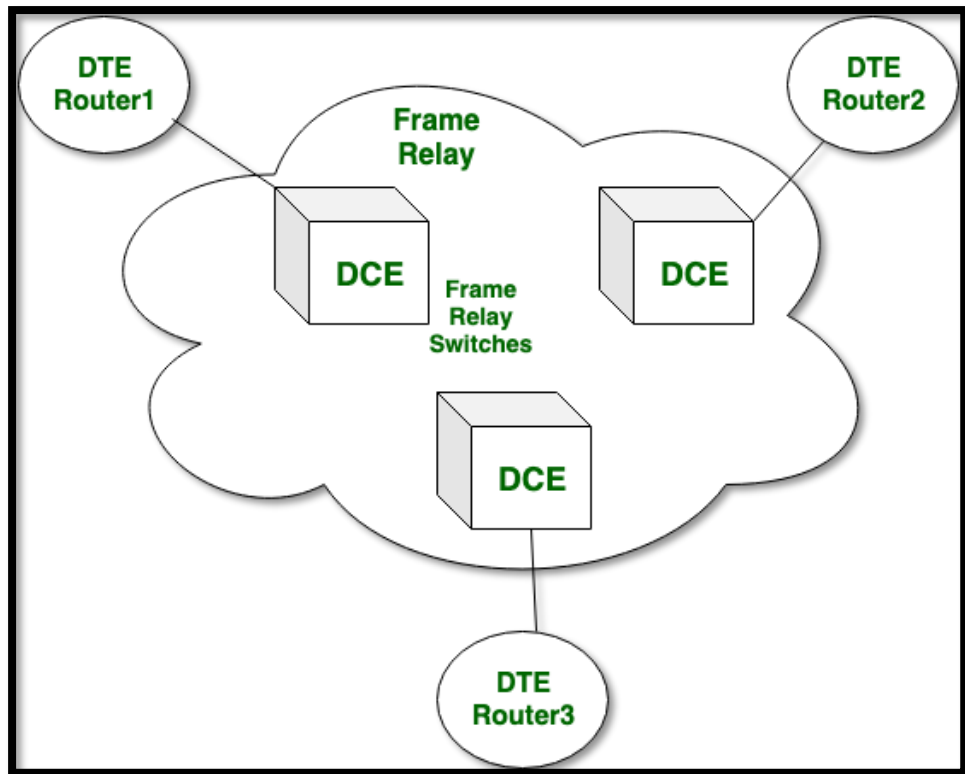
2) *Point-to-Point Protocol (PPP):*

Point-to-Point Protocol (PPP) is another WAN encapsulation protocol of the data link layer that is used to send and receive multiprotocol data between two directly connected computers or network devices. PPP is used between synchronous and asynchronous circuits. It supports several network layer protocols, such as IPv4 and IPv6. It uses HDLC encapsulation protocol, but also has built-in security mechanisms such as PAP and CHAP. PPP is a byte-oriented protocol widely used in broadband network communications. PPP is also known as RFC 1661.



3) Frame Relay:

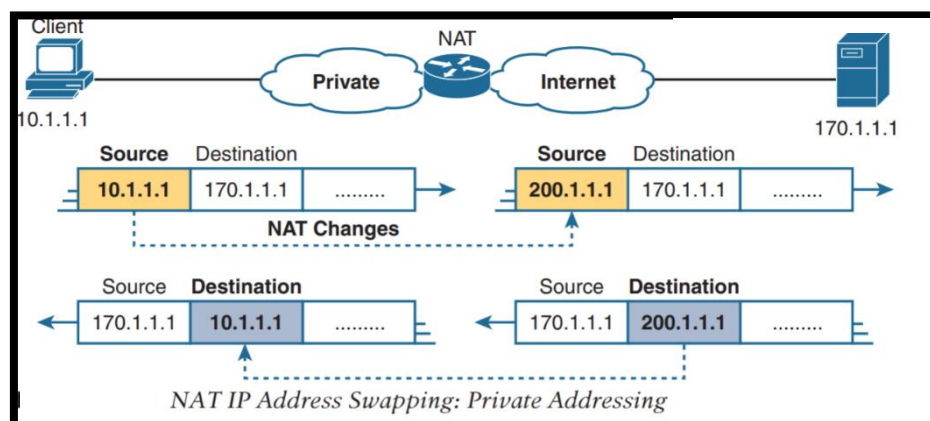
Frame Relay is a high-performance WAN encapsulation protocol working at the physical layer and data link layers of the OSI reference model. It was originally designed for use across Integrated Services Digital Network (ISDN) interfaces. It is an industry-standard, packet-switched protocol that handles multiple virtual circuits simultaneously. Frame Relay overcomes the time-consuming processes (such as error correction and flow control) employed in previous X.25 protocol. Today, it is used over a variety of network interfaces.



3) NAT & PAT:

- *NAT (Network Address Translation):*

NAT, defined in RFC 3022, allows a host that does not have a valid, registered, globally unique IP address to communicate with other hosts through the Internet. The hosts might be using private addresses or addresses assigned to another organization. In either case, NAT allows these addresses that are not Internet ready to continue to be used and still allows communication with hosts across the Internet. NAT achieves its goal by using a valid registered IP address to represent the private address to the rest of the Internet. The NAT function changes the private IP addresses to publicly registered IP addresses inside each IP packet, as shown in Figure below.



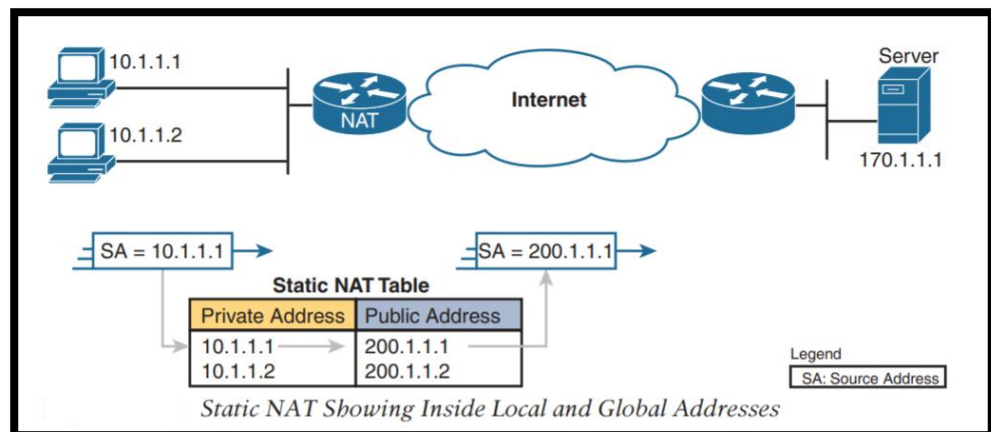
Notice that the router, performing NAT, changes the packet's source IP address when the packet leaves the private organization. The router performing NAT also changes the destination address in each packet that is forwarded back into the private network. (Network 200.1.1.0 is a registered network in above Figure. The NAT feature, configured in the router labeled NAT, performs the translation.

- *Types:*

- Static NAT: -

Static NAT works just like the example shown in Figure below, but with the IP addresses statically mapped to each other.

- Static NAT Example:



First, the concepts:

The company's ISP has assigned it registered network 200.1.1.0. Therefore, the NAT router must make the private IP addresses look like they are in network 200.1.1.0. To do so, the NAT router changes the source IP addresses in the packets going from left to right in the figure. In this example, the NAT router changes the source address (SA in the figure) of 10.1.1.1 to 200.1.1.1. With static NAT, the NAT router simply configures a one-to-one mapping between the private address and the registered address that is used on its behalf. The NAT router has statically configured a mapping between private address 10.1.1.1 and public, registered address 200.1.1.1. Supporting a second IP host with static NAT requires a second static one-to-one mapping using a second IP address in

the public address range. For example, to support 10.1.1.2, the router statically maps 10.1.1.2 to 200.1.1.2. Because the enterprise has a single registered Class C network, it can support at most 254 private IP addresses with NAT, with the usual two reserved numbers (the network number and network broadcast address). The terminology used with NAT, particularly with configuration, can be a little confusing. Notice in Figure 10-3 that the NAT table lists the private IP addresses as “private” and the public, registered addresses from network 200.1.1.0 as “public.” Cisco uses the term inside local for the private IP addresses in this example and inside global for the public IP addresses.

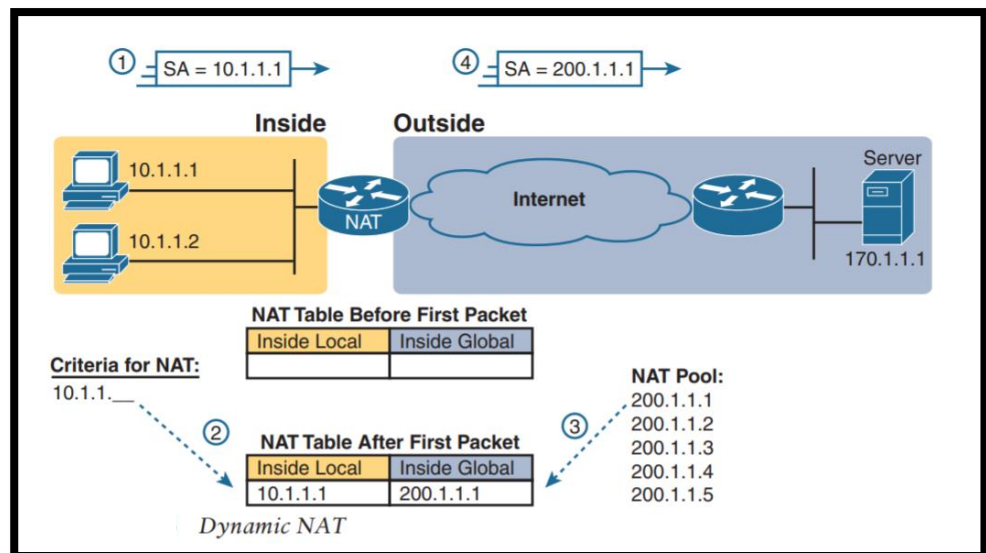
ptg31460660 10 Chapter 10: Network Address Translation 209 Using NAT terminology, the enterprise network that uses private addresses, and therefore needs NAT, is the “inside” part of the network. The Internet side of the NAT function is the “outside” part of the network. A host that needs NAT (such as 10.1.1.1 in the example) has the IP address it uses inside the network, and it needs an IP address to represent it in the outside network. So, because the host essentially needs two different addresses to represent it, you need two terms. Cisco calls the private IP address used in the inside network the inside local address and the address used to represent the host to the rest of the Internet the inside global address.

➤ **Dynamic NAT:**

Dynamic NAT has some similarities and differences compared to static NAT. Like static NAT, the NAT router creates a one-to-one mapping between an inside local and inside global address, and changes the IP addresses in packets as they exit and enter the inside network. However, the mapping of an inside local address to an inside global address happens dynamically. Dynamic NAT sets up a pool of possible inside global addresses and defines matching criteria to determine which inside local IP addresses should be translated with NAT.

➤ *Dynamic NAT Example:*

In Figure below, a pool of five inside global IP addresses has been established: 200.1.1.1 through 200.1.1.5. NAT has also been configured to translate any inside local addresses that start with 10.1.1.



The numbers 1, 2, 3, and 4 in the figure refer to the following sequence of events:

1. Host 10.1.1.1 sends its first packet to the server at 170.1.1.1.
2. As the packet enters the NAT router, the router applies some matching logic to decide whether the packet should have NAT applied. Because the logic has been configured to match source IP addresses that begin with 10.1.1, the router adds an entry in the NAT table for 10.1.1.1 as an inside local address.
3. The NAT router needs to allocate an IP address from the pool of valid inside global addresses. It picks the first one available (200.1.1.1, in this case) and adds it to the NAT table to complete the entry.
4. The NAT router translates the source IP address and forwards the packet.

The dynamic entry stays in the table as long as traffic flows occasionally. You can configure a timeout value that defines how long the router should wait, having not translated any packets with that address, before removing the dynamic entry. You can also manually clear the dynamic entries from the table using the “*clear ip nat translation*” command. NAT can be configured with more IP addresses in the inside local address list than in the inside global address pool. The router allocates addresses from the pool until all are allocated. If a

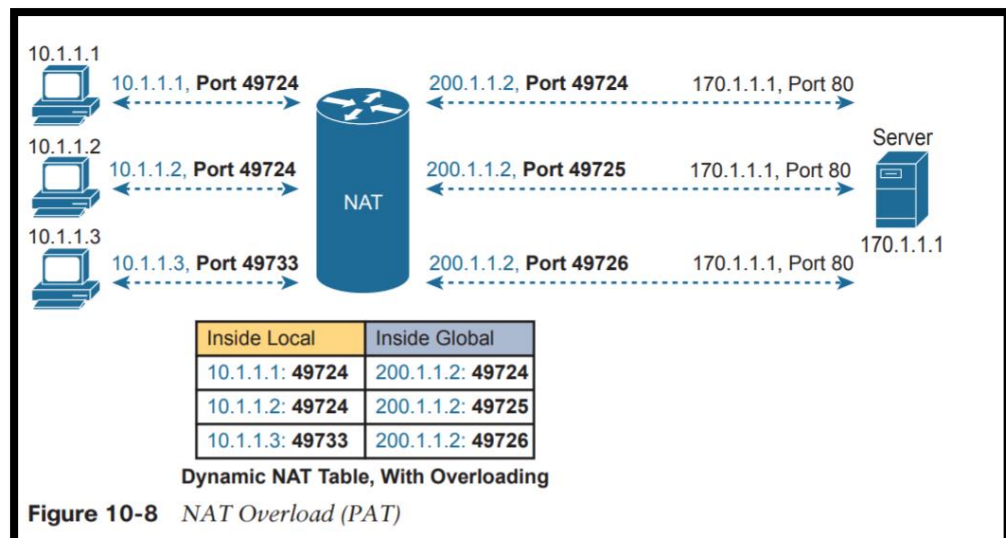
new packet arrives from yet another inside host, and it needs a NAT entry, but all the pooled IP addresses are in use, the router simply discards the packet. The user must try again until a NAT entry times out, at which point the NAT function works for the next host that sends a packet.

- *Port Address Translation (PAT):*

Some networks need to have most, if not all, IP hosts reach the Internet. If that network uses private IP addresses, the NAT router needs a very large set of registered IP addresses. With static NAT, for each private IP host that needs Internet access, you need a publicly registered IP address, completely defeating the goal of reducing the number of public. Dynamic NAT lessens the problem to some degree, because every single host in an internetwork should seldom need to communicate with the Internet at the same time. However, if a large percentage of the IP hosts in a network will need Internet access throughout that company's normal business hours, NAT still requires a large number of registered IP addresses, again failing to reduce IPv4 address consumption. The NAT Overload feature, also called Port Address Translation (PAT), solves this problem. Overloading allows NAT to scale to support many clients with only a few public IP addresses.

➤ *PAT Example:*

NAT takes advantage of the fact that, from a transport layer perspective, the server doesn't care whether it has one connection each to three different hosts or three connections to a single host IP address. NAT overload (PAT) translates not only the address, but the port number when necessary, making what looks like many TCP or UDP flows from different hosts look like the same number of flows from one host.



When PAT creates the dynamic mapping, it selects not only an inside global IP address but also a unique port number to use with that address. The NAT router keeps a NAT table entry for every unique combination of inside local IP address and port, with translation to the inside global address and a unique port number associated with the inside global address. And because the port number field has 16 bits, NAT overload can use more than 65,000 port numbers, allowing it to scale well without needing many registered IP addresses—in many cases, needing only one inside global IP address. Of the three types of NAT covered in this chapter so far, PAT is by far the most popular option. Static NAT and Dynamic NAT both require a one-to-one mapping from the inside local to the inside global address. PAT significantly reduces the number of required registered IP addresses compared to these other NAT alternatives.

4) Administrative Functions of Cisco Device:

4.1) *Brief about Administrative Function:*

The administrative functions that we can configure on a router and switch are:

- Hostnames
- Banners
- Password
- Interface descriptions

➤ **Hostname:**

The hostname is used to distinguish devices within a local network.

➤ **Banner:**

A banner is a message presented to a user who is using the Cisco switch.

➤ **Password:**

A password is a way to add security by giving rights to authorised user.

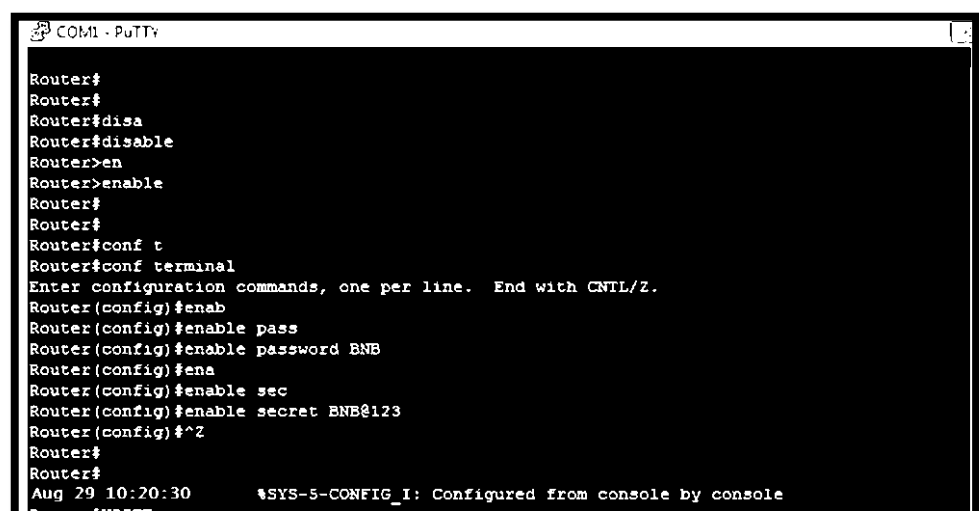
➤ **Interface description:**

The description command is a helpful way to keep track of circuit numbers.

4.2) *Commands for Securing our devices:*

1. enable secret password

Cisco Enable secret password is used for restricting access to enable mode and to the global configuration mode of a router. Enable secret password is stored in encrypted form in the router's configurations and is also called encrypted privileged exec password, therefore hard to break for an intruder and cannot be seen or guessed by displaying router configuration.



```
COM1 - PuTTY
Router#
Router#
Router#disa
Router#disable
Router>en
Router>enable
Router#
Router#
Router#conf t
Router#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#enab
Router(config)#enable pass
Router(config)#enable password BNB
Router(config)#ena
Router(config)#enable sec
Router(config)#enable secret BNB@123
Router(config)#^Z
Router#
Router#
Aug 29 10:20:30      %SYS-5-CONFIG_I: Configured from console by console
```


2. *line vty 0 4*

The term “vty” stands for Virtual teletype. VTY is a virtual port and used to get Telnet or SSH access to the device. The abstract “0 – 4” means that the device can allow 5 simultaneous virtual connections which may be Telnet or SSH. In a way, we may say that 5 (0 – 4) are connection ports to the Router or Switch.

```
R6#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R6(config)#line vty 0 4
R6(config-line)#login local
R6(config-line)#end
R6#
```

3. *service password-encryption*

Console and VTY passwords are displayed in clear-text. To encrypt them, we can use the service password-encryption global configuration command.

```
HQ_Router(config)#service password-encryption
HQ_Router(config)#
```

Notice how passwords are now stored in encrypted form:

```
ip flow-export version 9
!
!
!
!
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line aux 0
!
line vty 0 4
 password 7 0822455D0A16
 login
line vty 5 15
 password 7 0822455D0A16
 login
!
!
!
end
```

4. *crypto key generate rsa*

The `crypto key generate rsa` Global Configuration mode command generates RSA key pairs. RSA keys are generated in pairs - one public RSA key and one private RSA key. If the device already has RSA keys, a warning is displayed with a prompt to replace the existing keys with new keys. For example:

```
R1(config)#!  
R1(config)#crypto key generate rsa  
The name for the keys will be: R1.cisco.com  
Choose the size of the key modulus in the range of 360 to 2048 for your  
General Purpose Keys. Choosing a key modulus greater than 512 may take  
a few minutes.  
  
How many bits in the modulus [512]: 1024  
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]  
R1(config)#
```

5. *switchport port-security mac-address <mac-address / sticky [mac address]>*

Force a specific mac-address to the interface. Also use the “sticky” option to make the interface remember the first mac-address connected to the interface.

```
SW1(config-if)#switchport port-security maximum ?  
<1-132> Maximum addresses  
  
SW1(config-if)#switchport port-security maximum 2  
SW1(config-if)#switchport port-security mac-address aaaa.aaaa.aaaa  
SW1(config-if)#^Z  
SW1#wr  
Building configuration...  
[OK]  
SW1#  
03:21:32: %SYS-5-CONFIG_I: Configured from console by console  
SW1#  
BRYANT_ADV_1#2  
[Resuming connection 2 to r2 ... ]  
  
R2#  
R2#ping 172.23.23.3
```