CCNA

ROUTING & SWITCHING

PRACTICAL LAB WORKBOOK

DARE TO CHALLENGE YOUR SKILLS

COMPLETE THE TESTS & TAKE YOUR CAREER TO NEXT LEVEL

“ **CONQUER** THE CCNA WORK BOOK CHALLENGES & YOU WILL BE READY FOR **CCNP & CCIE** ”

Yes, this Network Bulls’ CCNA Work Book is full of tough questions and you need to find the solutions.
Solve the workbook, master the challenges and Take Your Career to the Next Level.

Develop a winning attitude by solving it.
We know it’s tough, but **you can do it.**

WHEN GOING IS TOUGH, ONLY TOUGHER GETS GOING

Use every bit of knowledge that you have till date; it’s time to implement what you have learned. This workbook will take you through the hardest questions of CCNA but once you do it; we assure you that your future is

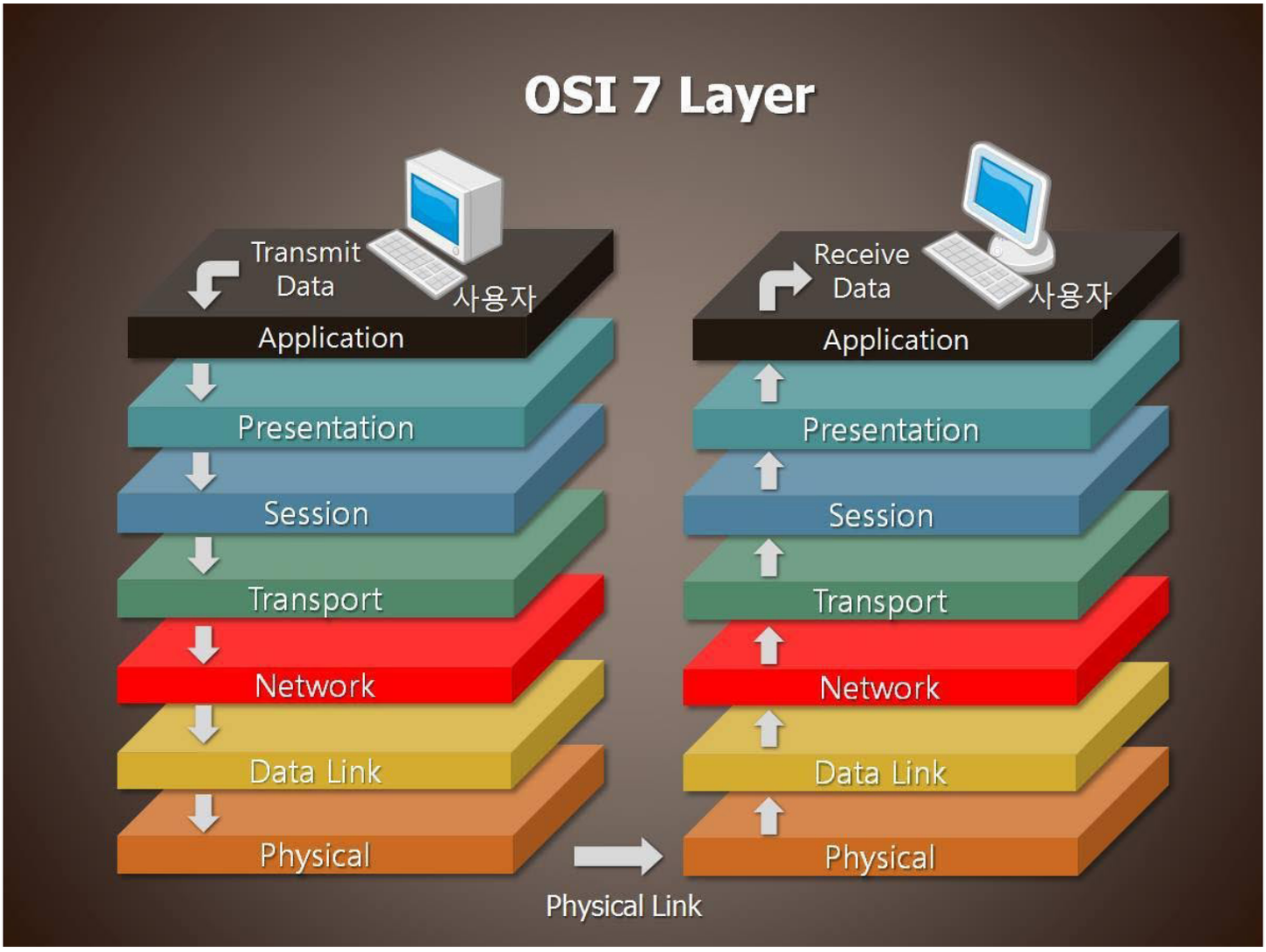
SUPER BRIGHT

“ **START** WITH ZEAL, WORK WITH PASSION & YOU WILL **FINISH** IT WITH EASE ”

DATA ENCAPSULATION AND DECAPSULATION

Data Encapsulation

Sending and receiving of data from a source device to the destination device is possible with the help of networking protocols by using data encapsulation. When a host transmits data to another device across a network, the data is encapsulated with protocol information at each layer of the OSI reference model. Each layer communicates with its neighbor layer on the destination. Each layer uses Protocol Data Units (PDUs) to communicate and exchange information.



Protocol Data Unit (PDU)

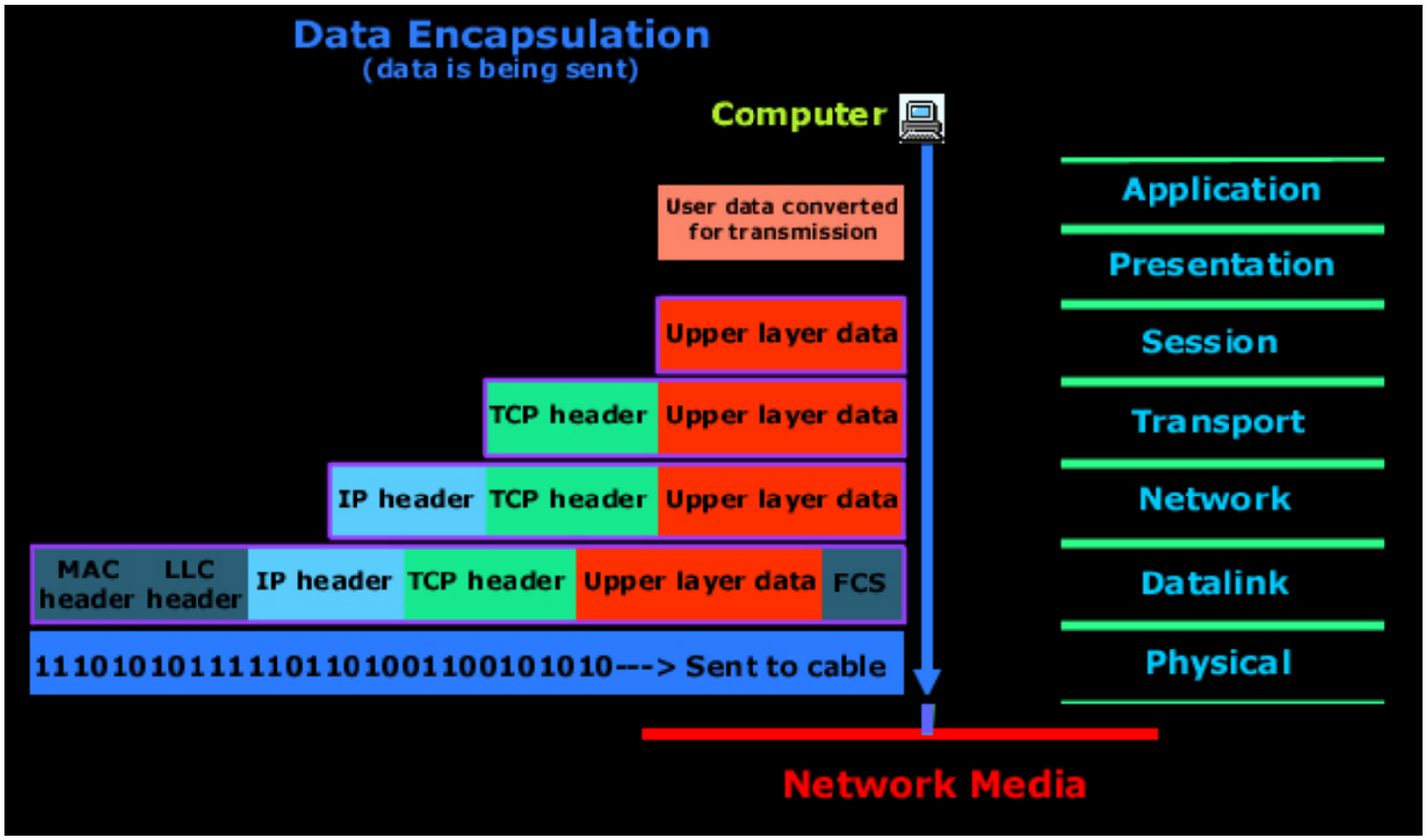
The Protocol Data Units contain the control information attached to the data at each layer. The information is attached to the header of the data field but can also be in end of the data field or trailer. PDUs are encapsulated by attaching them to the data at each layer of the OSI reference model. Each Protocol Data Unit has a name depending on the information each header has. This PDU information is only read by the neighbor layer on the destination and then is stripped off and the data is handed to the next layer.

OSI Layer Model and PDUs

The seven layered Open System Interconnection (OSI) model is basically defined for reducing the complexity of the internetworking. The OSI Model is then divided into two segments for more ease, Upper layers and Data Flow layers. The 7th, 6th and 5th layer of the OSI reference model are application layers also known as upper layers. The upper layers are directly related with user interface while the 4rth, 3rd, 2nd and 1st layer of the OSI model are also called data flow layers because they are related with the flow of the data. Each data flow layer has a Protocol Data Unit.

The Protocol Data Unit of each data flow layers is defined as follows:

Transport Layer: Segment is the PDU of the Transport layer.
Network Layer: Packet is the PDU of the Transport layer.
Data Link Layer: Frame is the PDU of the Transport layer.
Physical Layer: Bit is the PDU of the Transport layer.



Encapsulation and De-Encapsulation Process

The encapsulation and de-encapsulation of header control information on each layer of the OSI reference model is as follows:

TCP Header Encapsulation

The application-layers user data is converted for transmission on the network. The data stream is then handed down to the Transport layer, which sets up a virtual circuit to the destination. The data stream is then broken up, and a Transport layer header is created and called a segment. The header control information is attached to the Transport layer header of the data field. Each segment is sequenced so the data stream can be put back together on the destination exactly as transmitted.

IP Header Encapsulation

Each segment is then handed to the Network layer for logical addressing and routing through a routed protocol, for example IP, IPX, Apple Talk and DECNET etc. The Network-layer protocol adds a header to the segment handed down to the Data Link layer. Remember that the 3rd and 4rth layers work together to rebuild a data stream on a destination host. However, they have no responsibility for placing their Protocol Data Units on a local network segment, which is the only way to get the information to host or router.

MAC Header Encapsulation

The Data Link layer receives the packets from the Network layer and placing them on the network medium such as cable or wireless media. The Data Link layer encapsulates each packet in a frame, and the MAC header carries the source Mac address and destination Mac address. If the device is on a different network, then the frame is sent to a router to be routed through an internetwork.

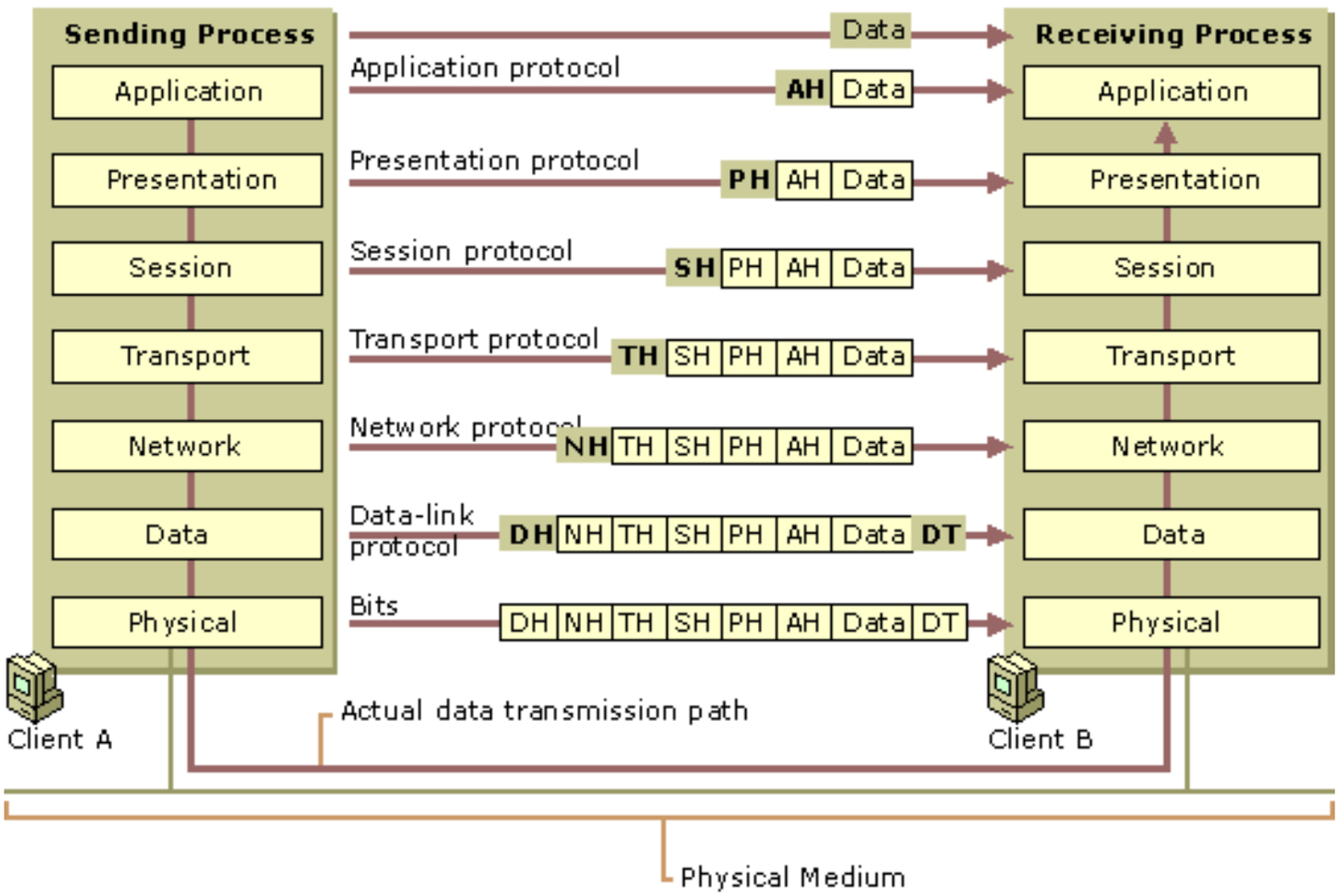
Physical Layer Encapsulation

Once the frame gets to the destination network, a new frame is used to get the packet to the destination host. To put this frame on the network, it must first be put into a digital signal. Since a frame is really a logical group of 1s and 0s, the Physical layer of the OSI model is responsible for encapsulating these digits into a digital signal, which is read by devices on the same local network.

Data encapsulation flow

At a transmitting device, the data encapsulation method works as follows:

User information is converted into data for transmission on the network. Data is converted into segments and a reliable or unreliable connection is set up between the source and destination devices using connection oriented and connectionless protocols. Segments are converted into packets using a logical address such as IP datagram using an IP address. Packets are converted into frames for transmission on the local network. Media Access Control (MAC) addresses or Ethernet addresses are commonly used to uniquely identify hosts on a local network segment. Frames are converted into bytes and bits, and a digital encoding and clocking or signaling method is used.



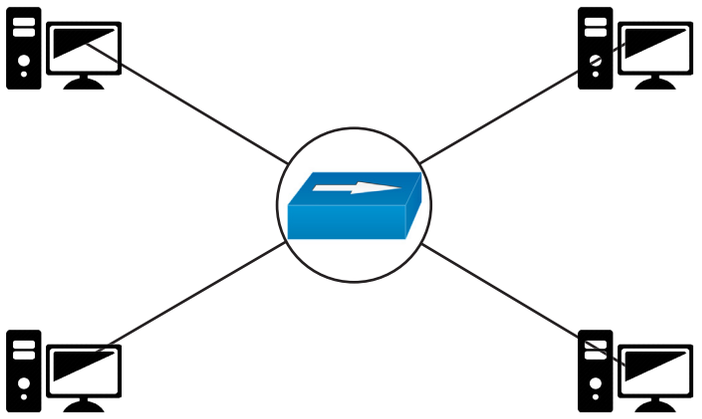
De-Encapsulation

On destination side, the receiving devices will synchronize on the digital signal and extract the 1s and 0s from the digital signal. At this point the devices build the frames, run a Cyclic Redundancy Check (CRC), and then check their output against the output in the Frame Check Sequence (FCS) field of the data frame. If the information matches then the packet is pulled from the frame, and the frame is discarded. This process is known as de-encapsulation. The packet then transfers to the Network layer, where the IP address is checked. If the IP address matches then the segment is pulled from the packet, and the packet is discarded. The data is processed at the Transport layer that rebuilds the data stream and acknowledges to the transmitting station that it received each piece of segment. It then happily transfers the data stream to the upper layer application.

Collision Domain:

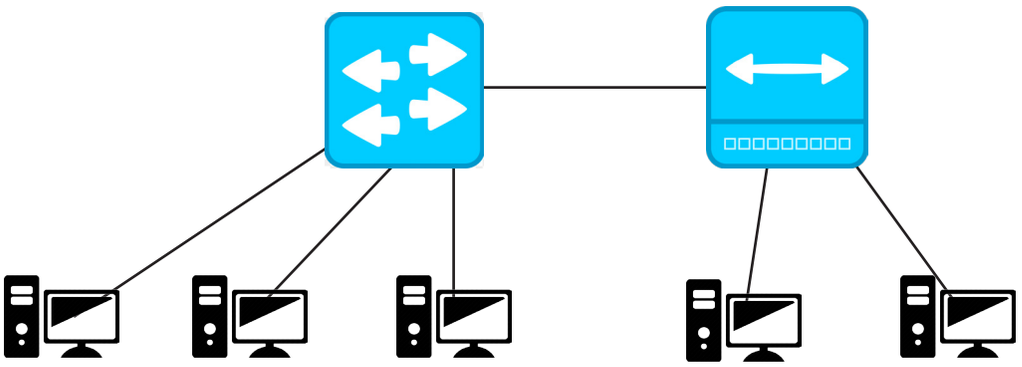
Collision domain is a set of LAN devices whose frames could collide with one another. This happens with hubs, bridges, repeaters and wireless access points as only one device can send and receive at a time. If more than one device tries sending or receiving, the information is lost and irrecoverable and it will need to be resent. This can slow down network performance along with making it a security threat.

A hub is considered a layer one device of the OSI model; all it does is send packets out on all ports including the port in which the packet was received on. This causes a collision because only one device can transmit at time. This also shares the bandwidth of all devices connected to that collision domain



All the devices are connected to a hub in this diagram. When two pcs send data at the same time, there can be a collision so the number of collision domain of hub is one.

Question.



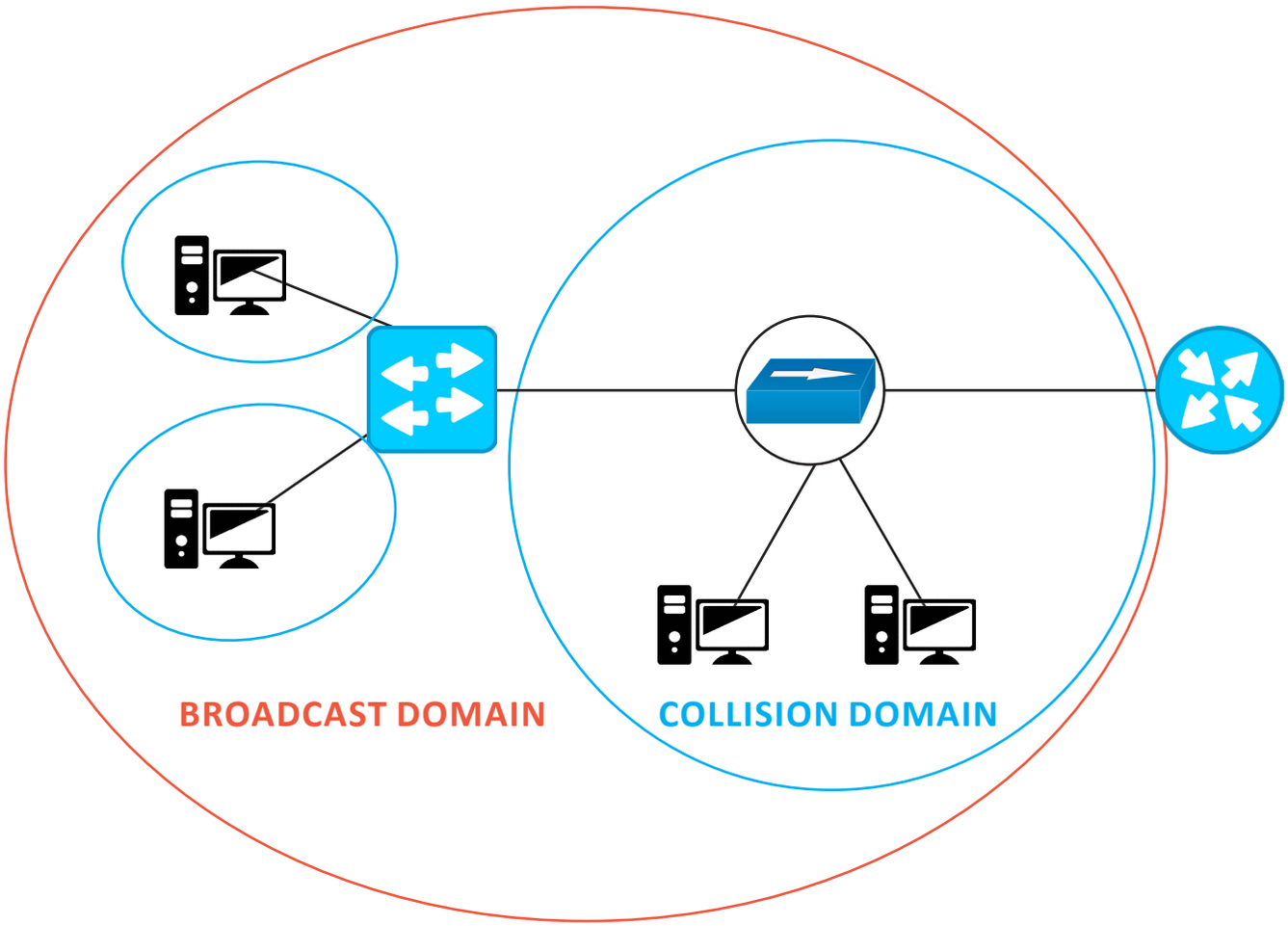
Find the number of collision domain of the network.

Answer : Number of Collision domain is 4

Description:
Here our network has a Switch and a Hub. A switch uses layer two of the OSI model, so the switch uses MAC addresses to send the packet to the correct device. Rather than sending it to all ports, a switch only sends the packet out one port, if it has the MAC address in its MAC address table. If not the switch will send the packet on all ports except for the port in which the packet was received on. Switches provide separate collision domains on each port. This provides dedicated bandwidth to that device. This also allows simultaneous conversations between devices on different ports. Each port can be operated at full-duplex so the device can send and receive information at the same time. Switch has collision domain per-port.
The 3 directly connected pc to the switch will have their own collision domain and the port with which the pc is connected to the hub is shared with hub, as hub will entertain the switch as an end device and put the switch with the other two pc in the same collision so the total number of collision domains is 4. 3 pc's and 1 shared with hub.

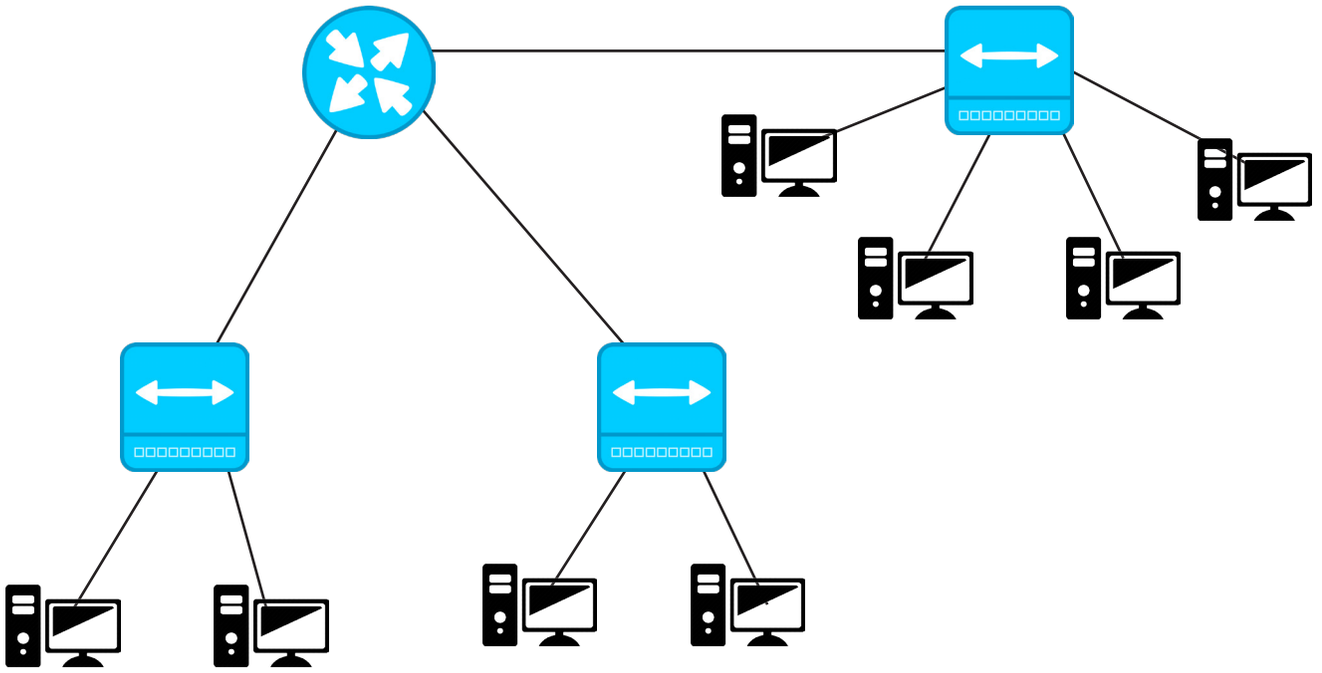
BROADCAST DOMAIN

The definition of a broadcast domain is a set of devices that if one device sends a broadcast frame, all other devices will receive that frame in the same broadcast domain. So if devices are in the same IP network, they will be able to receive a broadcast message. Having a smaller broadcast domain can improve network performance and improve against security attacks. The more PCs and network devices connected to a single broadcast domain, the more broadcast messages you will have. Remember a broadcast message goes to every PC and network device.



Switch by default has single broadcast domain and per-port collision domain.
Router has per-port collision and broadcast domain.
Hub has single broadcast and collision domain.

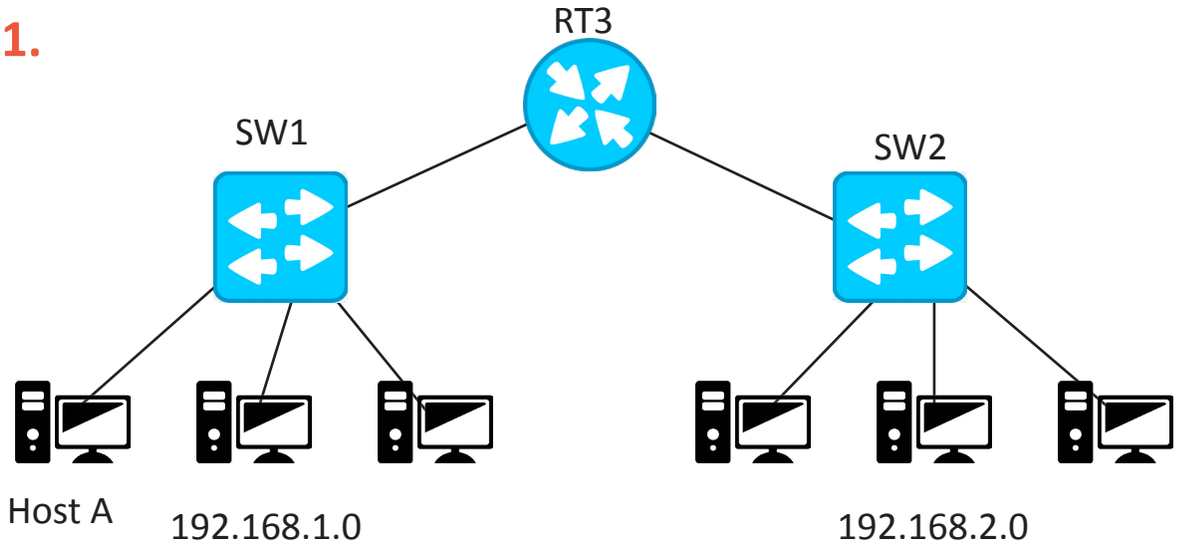
Question: Find the number of collision domains and broadcast domains.



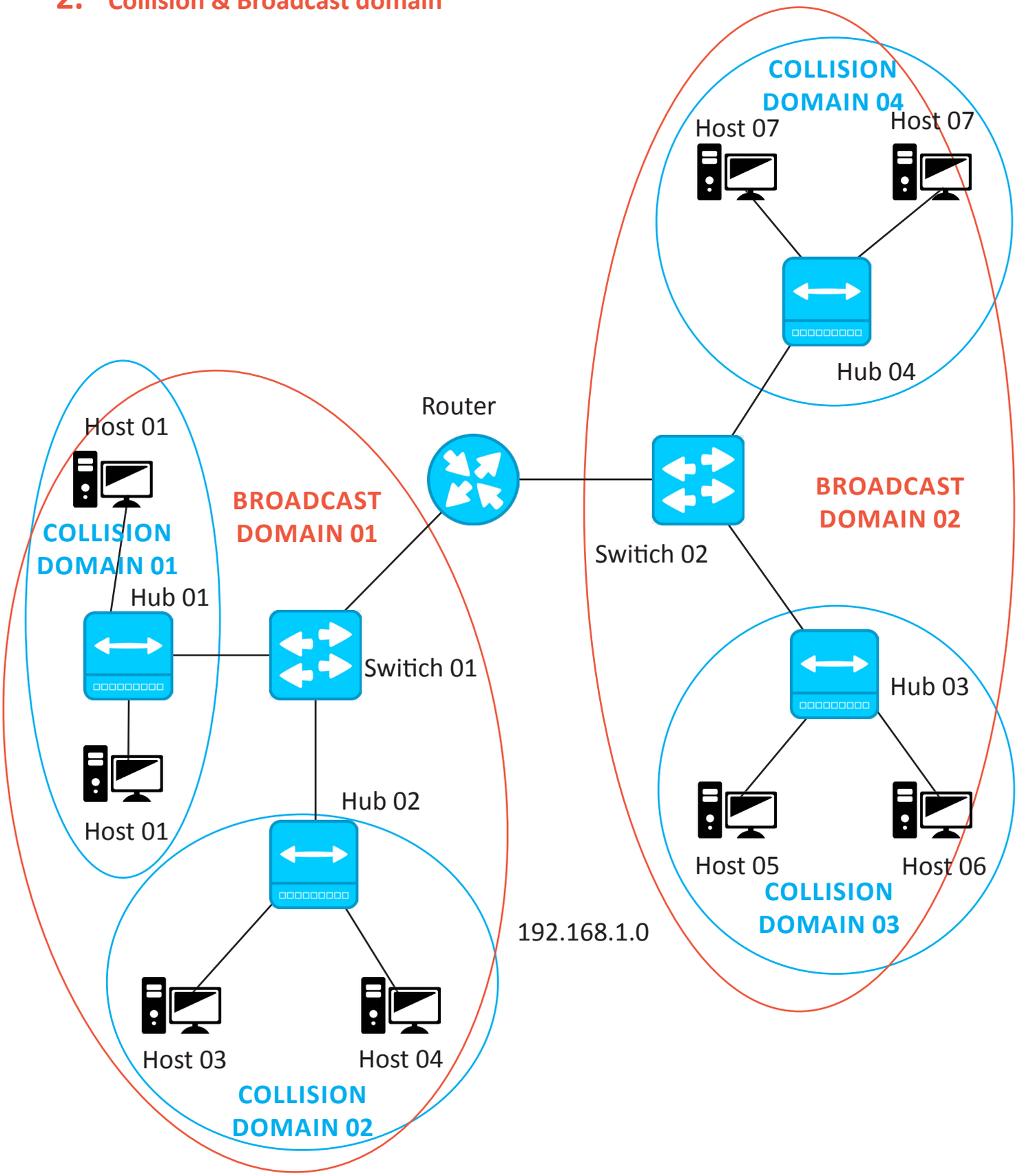
The number of collision domain is 11
And the broadcast domain is 3

Question: Find the collision and broadcast domain.

1.



2. Collision & Broadcast domain



“

Congrats,

you have completed the first Milestone Successfully.

ROAD AHEAD IS TOUGHER BUT WE KNOW YOU CAN DO IT. KEEP MARCHING ON… ALL THE BEST!

”

SUBNETTING

Subnetting is the process of making small networks (subnets) from a large network.

Basic Procedure to make Subnets

Suppose you have a network 192.168.10.0/24, it means you have a network of 256 addresses (0-255) or you can say you have a network of block size 256. You normally use it as a class C Address. What will happen if you ON one more bit. Let's try this out-

Network - 192.168.10.0/25

Now you have 25 ON bits, so subnet mask will be 255.255.255.128
Network Address- 192.168.10.0
Subnet Mask- 255.255.255.128

Now you have to find out what will be block size of your network
192.168.10.0/25.
Block size = 256 – (a value from subnet mask).

Always choose a nonzero value from subnet mask and start reading the subnet mask from right to left. In the above case, your value is 128.

If you have a subnet mask 255.255.192.0, then your value will be 192.
(Don't consider the zero.) Now put the value in above formula.
So the block size of your network 192.168.10.0/25 is
Block size=256 – 128= 128
No. of Subnets= 2x, here x is equal to the number of extra ON bits (except default ones).
In our case, you have one extra ON bit, don't consider the default 24 bits of class C.
No. of subnets = 2x = 21= 2
No of hosts per subnet = 2y -2, here y is number the OFF bits. In our case we have (32-25) 7 OFF bits.
So number of subnets = 27-2=128-2=126.

Block size	128
No. of subnets	2
No. of hosts per subnet	126

Now find the Network addresses of your subnets-

Start from the IP address 192.168.10.0 which is a Network address for your first subnet. To get the Network address of your 2nd subnet, add the block size in fourth octet of your 1st network address. Remember, you are adding the block size in 4th octet, because you use the value of 4th octet to find the block size. If you are using the value of 3rd octet to get the block size, you have to add the block size in the 3rd octet of your Network address.

	Network address	Broadcast address
First subnet	192.168.10.0	?
Second subnet	192.168.10.128	?

Broadcast address of 1st subnet will be the ip address before 192.168.10.128 and that is 192.168.10.127 or you can count from 0 to 127 and that will give you a block size of 128.

Broadcast address of 2nd subnet will be 192.168.10.255

	Network address	Broadcast address
First subnet	192.168.10.0	192.168.10.127
Second subnet	192.168.10.128	192.168.10.255

Host addresses will be the addresses between Network address and Broadcast address. Host addresses are those addresses that you can assign to your devices.

	Range of Host addresses
First subnet	192.168.10.1 - 192.168.10.126
Second subnet	192.168.10.129 - 192.168.10.254

From above table, you can see that the 1st host address and last host address of your first subnet and second subnet.

Class C subnetting examples

Example: 1

Network address = 192.168.10.0
CIDR = 26
26 bits are ON, so subnet mask =255.255.255.192
Block size =256-192 =64
No. of subnets= 22= 4
No. of hosts per subnet= 26-2 =64-2 =62

	Network address	Broadcast address
1st subnet	192.168.10.0	192.168.10.63
2nd subnet	192.168.10.64	192.168.10.127
3rd subnet	192.168.10.128	192.168.10.191
4th subnet	192.168.10.192	192.168.10.255

	Range of Host addresses
1st subnet	192.168.10.1 - 192.168.10.62
2nd subnet	192.168.10.65 - 192.168.10.126
3rd subnet	192.168.10.129-192.168.10.190
4th subnet	192.168.10.193-192.168.10.254

Class B Subnetting examples

Example: 1

Network address = 172.16.0.0
CIDR = 17
17 bits are ON, so subnet mask =255.255.128.0
Block size =256-128 =128
No. of subnets= 21= 2
No. of hosts per subnet= 215-2

	Network address	Broadcast address
1st subnet	172.16.0.0	172.16.127.255
2nd subnet	172.16.128.0	172.16.255.255

	Range of Host addresses
1st subnet	172.16.0.1 -172.16.127.254
2nd subnet	172.16.128.1 -172.16.255.254

Example: 2

Network address = 172.16.0.0
CIDR = 24
24 bits are ON, so subnet mask =255.255.255.0
Block size =256-255 =1
No. of subnets= 28= 256
No. of hosts per subnet= 28-2 =256-2 =254

	Network address	Broadcast address
1st subnet	172.16.0.0	172.16.0.255
2nd subnet	172.16.1.0	172.16.1.255
------	-----	-------
256th subnet	172.16.255.0	172.16.255.255

	Range of Host addresses
1st subnet	172.16.0.1 -172.16.0.254
2nd subnet	172.16.1.1 -172.16.1.254
--------	-------
256th subnet	172.16.255.1 -172.16.255.254

Example: 3

Network address = 172.16.0.0
CIDR = 25
25 bits are ON, so subnet mask =255.255.255.128
Block size =256-128 =128
No. of subnets= 29= 512
No. of hosts per subnet= 27-2 =126

	Network address	Broadcast address
1st subnet	172.16.0.0	172.16.0.127
2nd subnet	172.16.0.128	172.16.0.255
3rd subnet	172.16.1.0	172.16.1.127
4th subnet	172.16.1.128	172.16.1.255
------	-----	-------
Last subnet	172.16.255.128	172.16.255.255

	Range of Host addresses
1st subnet	172.16.0.1 -172.16.0.126
2nd subnet	172.16.0.129 -172.16.0.254
3rd subnet	172.16.1.1 -172.16.1.126
4th subnet	172.16.1.129 -172.16.1.254
--------	-------
last subnet	172.16.255.129-172.16.255.254

Class B Subnetting Examples

Example: 1

Network address = 10.0.0.0
CIDR = 9
9 bits are ON, so subnet mask =255.128.0.0
Block size =256-128 =128
No. of subnets= 21= 2
No. of hosts per subnet= 223-2

	Network address	Broadcast address
1st subnet	10.0.0.0	10.127.255.255
2nd subnet	10.128.0.0	10.255.255.255

	Range of Host addresses
1st subnet	10.0.0.1 – 10.127.255.254
2nd subnet	10.128.0.1 – 10.255.255.254

Example: 2

Network address = 10.0.0.0

CIDR = 16

16 bits are ON, so subnet mask =255.255.0.0

Block size =256-255 =1

No. of subnets= 28=256

No. of hosts per subnet= 216-2 =65534

	Network address	Broadcast address
1st subnet	10.0.0.0	10.0.255.255
2nd subnet	10.1.0.0	10.1.255.255
------	-----	-------
Last subnet	10.255.0.0	10.255.255.255

	Range of Host addresses
1st subnet	10.0.0.1 -10.0.255.254
2nd subnet	10.1.0.1 – 10.1.255.254
--------	-------
Last subnet	10.255.0.1 -10.255.255.254

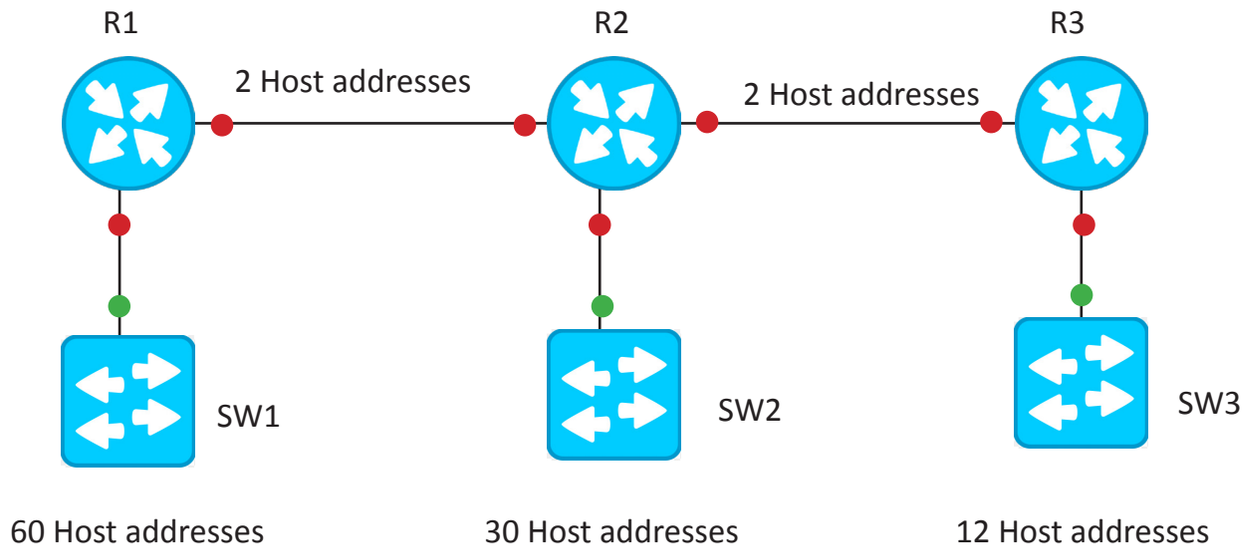
VARIABLE LENGTH SUBNET MASK (VLSM)

In subnetting, you divided one large network into small networks (subnets) with subnet mask of same length. But using VLSM, you can divide one large network into subnets with subnet mask of different lengths and you can choose the length of mask according to the number of hosts required on your network.

Before starting the VLSM, first understand the below table. This table says that if you want to get a block size of 128, then you have to ON one extra bit, and to get a block size of 64, you have to ON two extra bits and so on.

Block size	Extra ON bits
128	1
64	2
32	3
16	4
8	5
4	6

Basic Procedure for VLSM



Consider the above diagram; here you need a network having capability of at least 60 host addresses between R1 and SW1 and also need a different network having at least 30 host addresses between R2 and SW2. Similar for networks b/w R3 and SW3, R1 and R2, R2 and R3.

Now suppose ISP gave you a network 192.168.10.0/24 and you have to use IP addresses of this network for your topology. You cannot use the subnetting, because subnetting will divide the network into subnets with subnet mask of same length so you will get blocks of same size. But in the above topology, you want a network with block size 64 b/w R1 and SW1 and network of block size 32 b/w R2 and SW2 and so on. So there is only option is left, that is VLSM.

192.168.10.0 192.168.10.1 192.168.10.2 192.168.10.3 192.168.10.4 - - 192.168.10.63	B/w R1 and SW1, you need 60 host addresses. To get 60 host addresses, you need at least block size of 64 and to get a block size of 64, you have to ON 2 extra bits. So total bits will be 26 (24bits of first three octets +2 extra bits to get a block size of 64). So network b/w R1 and SW1 will be 192.168.10.0/26
192.168.10.64 192.168.10.65 192.168.10.66 - - 192.168.10.95	B/w R2 and SW2, you need 30 host addresses, so block of size 32 will be enough. To get a block size of 32, you have to ON 3 extra bits. So total ON bits will be 27(24+3). Network will be 192.168.10.64/27
192.168.10.96 192.168.10.97 192.168.10.98 - - 192.168.10.111	B/w R3 and SW3, you need 12 host addresses, so block size =16 will be enough. So to get a block size of 16, you have to ON 4 extra bits. So total ON bits =28. Network will be 192.168.10.96/28
192.168.10.112 192.168.10.113 192.168.10.114 192.168.10.115	B/w R1 and R2, you need 2 host addresses, so block size =4 is enough. So to get a block size of 4, you have to ON 6 extra bits. so total ON bits =30. Network will be
192.168.10.116 192.168.10.117 192.168.10.118 192.168.10.119	B/w R2 and R3 Network will be 192.168.10.116/30

SUMMARIZATION/SUPERNETTING

Summarization is reverse process of subnetting. In subnetting, you divided one large network into subnets but in summarization, you will combine small subnets to make large network

Purpose of using summarization:

- Reduce the size of routing table. So that router can analyze the routing table faster.
- It will be easy for router to send a summary route rather than individual subnets.

Basic procedure for Summarization

Suppose you have four subnets like –

192.168.10.0/30
192.168.10.4/30
192.168.10.8/30
192.168.10.12/30

And you want to make a summarization of above subnets. First you have to understand the subnets. These subnets are representing the IP addresses from 192.168.10.0 to 192.168.10.15. Now you have total 16 IP addresses, so block size of 16 is enough and to get a block size of 16, you have to ON 4 extra bits. So you will get a subnet mask of length 28(24+4). And your network address will be 192.168.10.0

So summarization of above subnets will be 192.168.10.0/28

Example: 1

Summarize the below subnets-

10.0.0.0/24
10.0.1.0/24
10.0.2.0/24
10.0.3.0/24

Solution: 3rd octet is changing (0-3), so block size of 4 is enough. To get a block size of 4 , you have to ON 6 extra bits. So total ON bits are 22(16 bits of 1st and 2nd octet+6). Network address will be 10.0.0.0

Summary route = 10.0.0.0/22

Example: 2
Summarize the below subnets-

10.0.1.0/24
10.0.2.0/24
10.0.3.0/24
10.0.4.0/24

Solution: 3rd octet is changing (1-4), in this case, block size of 4 is not enough. In block size of 4, you have numbers from 0 to 3. So here you will choose a bigger block size than 4, and that will be 8. To get a block size of 8, you have to ON 5 extra bits. So total ON bits are 21(16 bits of 1st and 2nd octet+5). Network address will be 10.0.0.0 because when you use subnet mask length 21, then it will give you subnets like 10.0.0.0/21, 10.0.8.0/21, 10.0.16.0/21

Summary route = 10.0.0.0/21

QUESTIONS

1. Summarize the below subnets-
   10.0.0.0/24
   10.0.1.0/24
   10.0.2.0/24
   10.0.3.0/24

2. Summarize the below subnets-
   10.0.1.0/24
   10.0.2.0/24
   10.0.3.0/24
   10.0.4.0/24

3. Do the subnetting of 192.168.10.0 using CIDR value 29.

4. Do the subnetting of 172.168.0.0 using CIDR value 19.

5. Do the subnetting of 155.165.0.0 using CIDR value 25.

6. Do the subnetting of 20.0.0.0 using CIDR value 11.

7. Do the subnetting of 35.0.0.0 using CIDR value 24.

8. Do the subnetting of 37.0.0.0 using CIDR value 27.

9. You are working in a data center environment and are assigned the addressing plan to allow the maximum number of subnets with as many as 30 hosts each. Which IP address range meets these requirements?
   A. 10.188.31.0/27
   B. 10.188.31.0/26
   C. 10.188.31.0/29
   D. 10.188.31.0/28
   E. 10.188.31.0/25

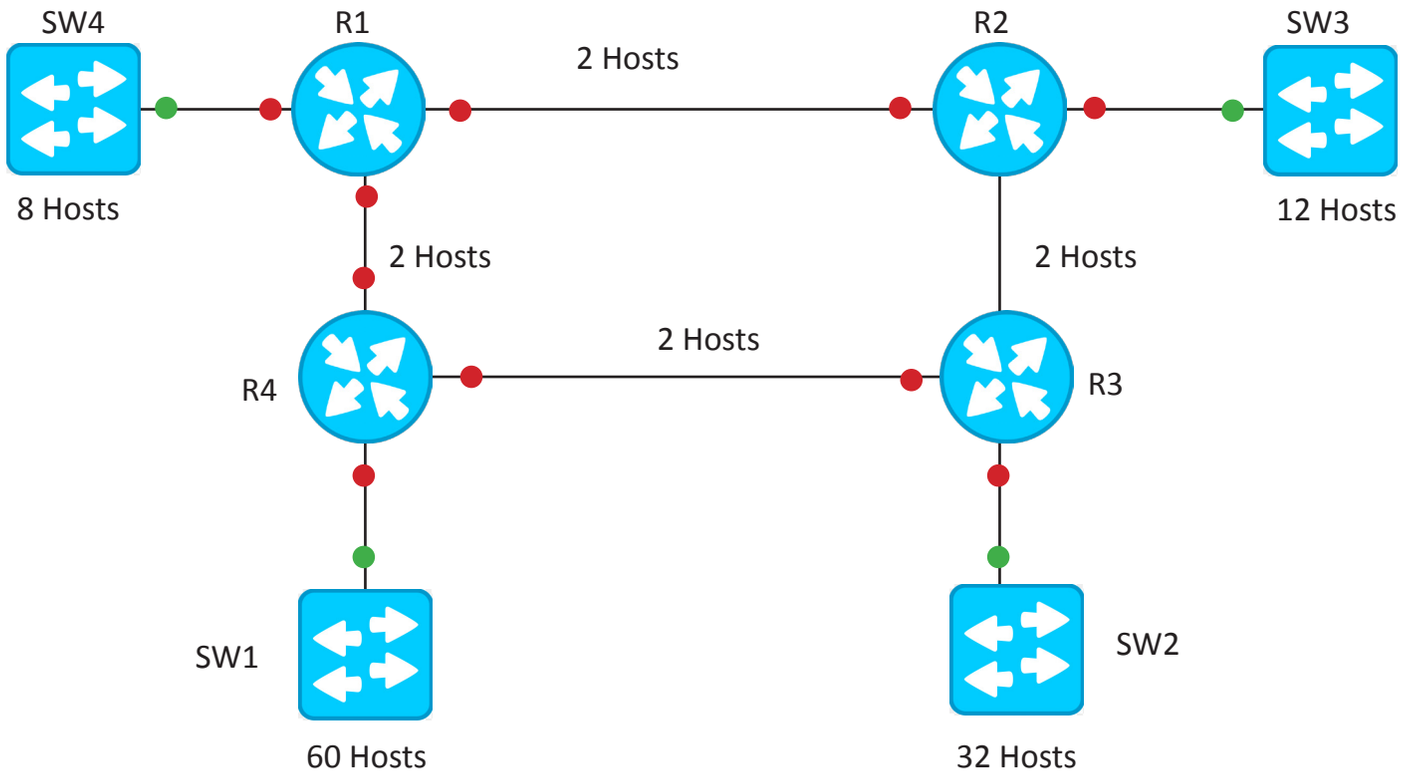
10. In the implementation of VLSM techniques on a network using a single Class C IP address, which subnet mask is the most efficient for point-to-point serial links?
    A. 255.255.255.240
    B. 255.255.255.254
    C. 255.255.255.252
    D. 255.255.255.0
    E. 255.255.255.248

11. You have an interface on a router with the IP address of 192.168.192.10/29. Including the router interface, how many hosts can have IP addresses on the LAN attached to the router interface?
    A. 6
    B. 8
    C. 30
    D. 62
    E. 126

12. Which configuration command must be in effect to allow the use of 8 subnets if the Class C subnet mask is 255.255.255.224?
    A. Router(config)#ip classless
    B. Router(config)#ip version 6
    C. Router(config)#no ip classful
    D. Router(config)#ip unnumbered
    E. Router(config)#ip subnet-zero
    F. Router(config)#ip all-nets

13. You have a network with a subnet of 172.16.17.0/22. Which is the valid host address?
    A. 172.16.17.1-255.255.255.252
    B. 172.16.0.1-255.255.240.0
    C. 172.16.18.255-255.255.252.0

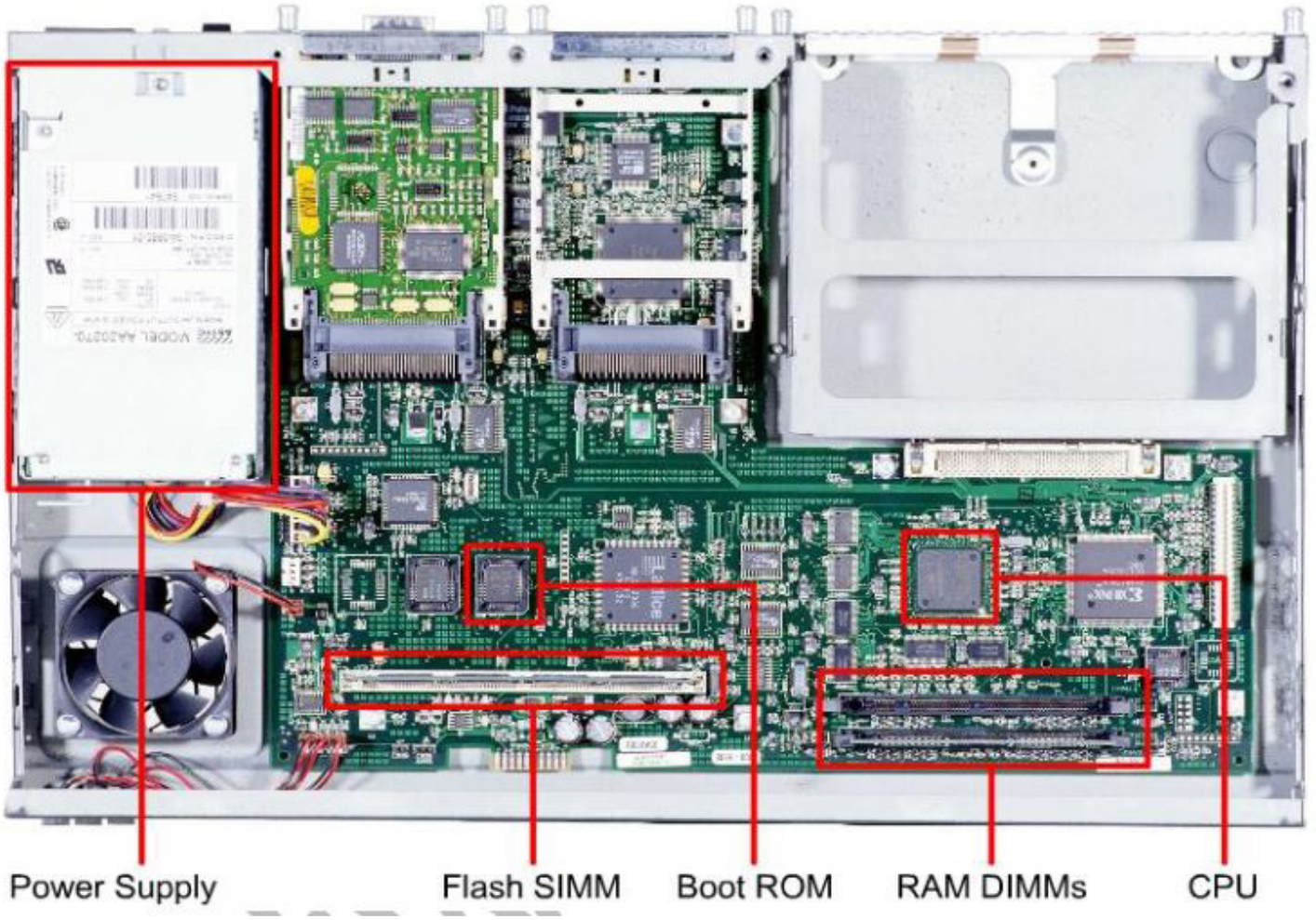
14. Your organization told you to use the network 192.168.10.0/24 for below diagram but there is condition that you have to use the subnets with specific hosts according to the diagram. And do not waste the IP addresses.



15. Do the summarization of below subnets-
192.168.10.24/30
192.168.10.28/30
192.168.10.32/30
192.168.10.36/30

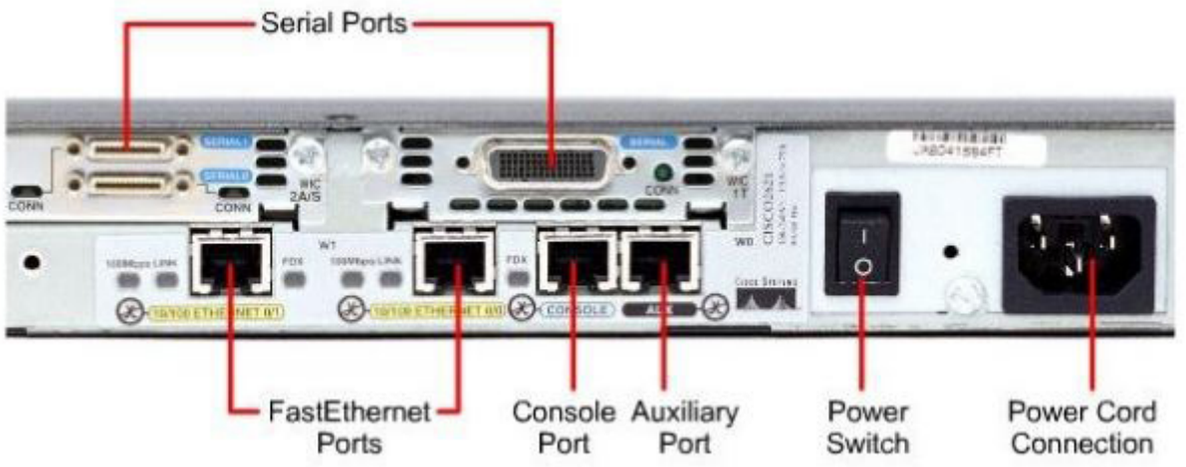
ROUTER BASICS

Router Components



Think of a router as just like another computer just it is dedicated to its job in networks. So the components of the router are:

Power supply	Supplies the power to the router just like we have a power supply in a Computer Cabinet.
Flash	Contains IOS the operating system of the router. It is an EEPROM-Electrically Erasable Programmable Read Only Memory i.e. non-volatile.
Boot ROM	It is the ROM of the router just like a motherboard in PC. It contains bootstrap program which locates and loads the IOS from flash into RAM
RAM	It is volatile. Stores the running copy of IOS, running-config
CPU	The processor of the router responsible for processing functions of router.



Console port of a switch is generally at the back side of the switch

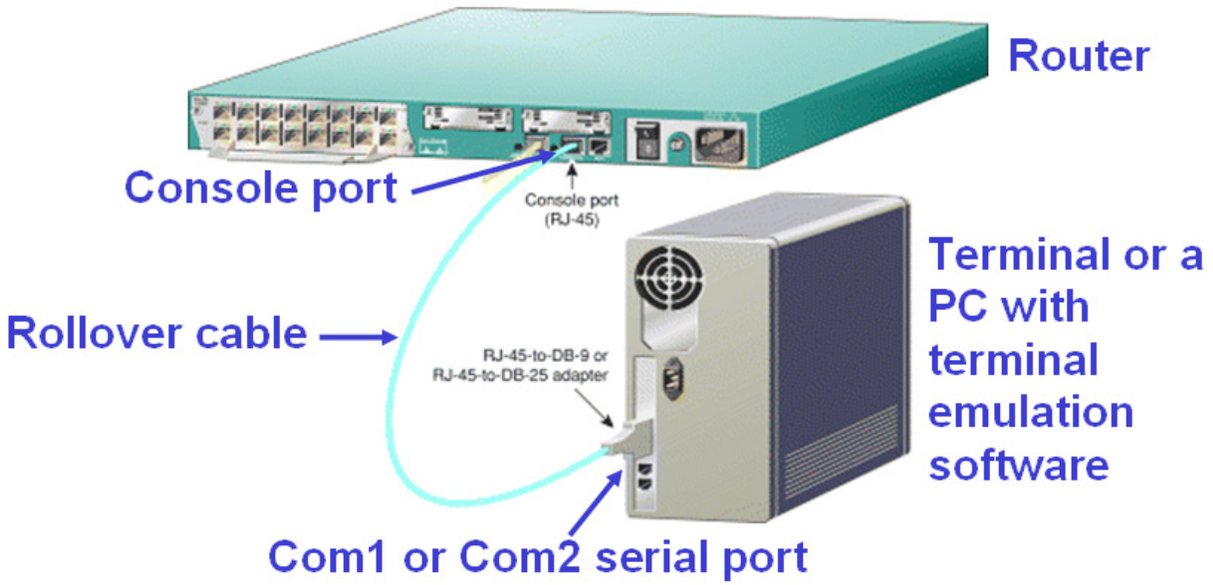
How to access the router or switch?

1. **Console**

   You should have the physical access of router for this. This is used more commonly for putting initial configuration on to the router or switch so that we can access it remotely. Common use-

   - Configuring a device that has never been configured.
   - Configuring a device directly, because you are physically located where the device is.
   - Troubleshooting a device that you can no longer access remotely.
   - Performing password recovery

   We connect this DB9 connector side to PC's COM port and the RJ45 side of this cable is put into the console port of the router.



Terminal emulation software is used to access the router on PC. When connected using console port PC is acting as a Dumb Terminal, everything you do is being done in real time on the router. There are various terminal emulation softwares like- HyperTerminal, TeraTerm, Secure CRT, Putty, etc. You can use any software of your choice as terminal emulator.

As many people nowadays use Laptops and even new computer do not have COM ports, there are DB9 to USB converters as shown below that can be used if you want to connect console to a computer that doesn't have DB9 COM port

2. Virtual terminal

There are two options commonly used for virtual terminal:

- **Telnet :** This method of configuring is less commonly used in Enterprise networks because the commands you give to router are sent without encryption i.e. in clear text. So if someone manages to capture the packets, he will be able to know what you are configuring on the router.
- **SSH :** This method is used widely in Enterprise networks. Before sending the commands it encrypts them so even if packet is captured, the text in them is not understandable.

IOS BASICS

1. Getting familiar with the modes

```
Router>
Switch>
```

This mode you see here is called User mode. It will allow you to view the state of the router, but will not allow you to modify its configuration.

```
Router> enable
Router#
```

If you give the enable command as shown up here in user mode notice the prompt changes and you move to the privilege mode. This mode allows administrator to modify some of the configuration of the router or switch.

```
Router> disable
Router#
```

If you give the **disable** command as shown up here in privilege mode, notice the prompt changes and you move back to the user mode.

```
Router#configure terminal
Router(config)#
```

If you give the above shown command in privilege mode you move into global configuration mode. This mode is used commonly for configuring most of the configurations on router or to go further into other configuration modes like interface configuration mode.

```
Router(config)#exit
Router#
```

If you want to move back to privilege mode use the command as shown.

NOTE: - There are other modes in a router which we will see as we configure routers and switches. Make sure before typing in a particular command that you are in the appropriate mode otherwise the command will not be executed correctly.

2. Basic config of Router and shortcuts in CLI

If the router do not have a saved configuration,
After several lines of information on the screen you should eventually see:

```
Would you like to enter the initial configuration dialog? [yes/no]: n
```

- Always answer “n” for no.
- We will never be using setup mode.
- If you accidentally press “y” and enter Setup Mode, press and hold down the control key and press C (CTRL-C).
- Wait a few seconds, and then press Enter.

On some routers you may see the following message

```
Would you like to terminate autoinstall? [yes/no]: y

  <There will be several lines of output>

Router>
```

Shortcuts and help in CLI

Entering a short command is sufficient in router CLI as long as there is no confusion over the command you are asking for. For example

```
Router>en
Router#
```

As shown above, **en** is as good as **enable** because there is no other command in the user mode beginning with **en**.

You can use Tab key on the keyboard to complete your command in CLI. For example, if tab key is pressed after conf, the command is completed with the command **configure**. If tab is pressed after **configure t** command, it would be completed as **configure terminal.**

```
Router#conf
Router#configure t
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

You can use? for help. Like shown below it shows all the command that can be typed in this mode. Here the output has been omitted to save space

```
Router#?
Exec commands:
  <1-99>     Session number to resume
  auto       Exec level Automation
  clear      Reset functions
  clock      Manage the system clock
```

If done like below it shows all commands that begin with s.

```
Router#s?
setup  show  ssh
```

3. Configure a hostname on the router

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#
```

4. Banner Config

```
R1(config)#banner motd @
Enter TEXT message.  End with the character '@'.
                NOTICE
THIS IS A PRIVATE NETWORK. DON'T PROCEED FURTHER IF YOU ARE NOT AUTHORISED TO.
@
```

5. Saving the configuration on a router

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

6. Enable password config

```
R1(config)#enable password cisco
R1(config)#end
%SYS-5-CONFIG_I: Configured from console by console
R1#disable
R1>en
Password:
R1#
```

7. Enable secret config

```
R1(config)#enable secret cisco123
```

Verification shown below

```
R1#show running-config
Building configuration...
Current configuration : 627 bytes
hostname R1
enable password cisco
enable secret 5 $1$mERr$5.a6P4JqbNiMX01usIfka/
```

8. Configure Console password

Console password will be asked whenever someone is trying to access the router through console port

```
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
```

The first command here moves you into line configuration mode for console port. Then we set cisco as the password. The login command here enables password checking or you can say that it tells the router to ask for password when someone is trying to access through console port.

Now again this password is also shown as clear text if someone checks the running-config. So to encrypt all of our clear text passwords we can use the below mentioned command to encrypt all of our passwords that are shown in clear text like console password, enable password. To verify this you can use show run after this command.

```
R1(config)#service password-encryption
```

9. Configure IP on a router

You can configure IP on some interface of a router. Here first we move in to the interface configuration mode for the interface fastethernet 0/0 using the first command. There we specify the IP address we want to assign to interface followed by the subnet mask we intend to use.

```
R1(config)#interface fastEthernet 0/0
R1(config-if)#ip address 10.0.0.1 255.0.0.0
R1(config-if)#no shutdown
R1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
```

Now by default the interface is administratively down or in other words the interface has a command shutdown under interface configuration. To remove any command from a router we can add no in front of that command. So we turn on the interface by no shutdown. Router can be seen displaying a log message that it was successful in bringing the interface up.

10. Configure Router for Telnet

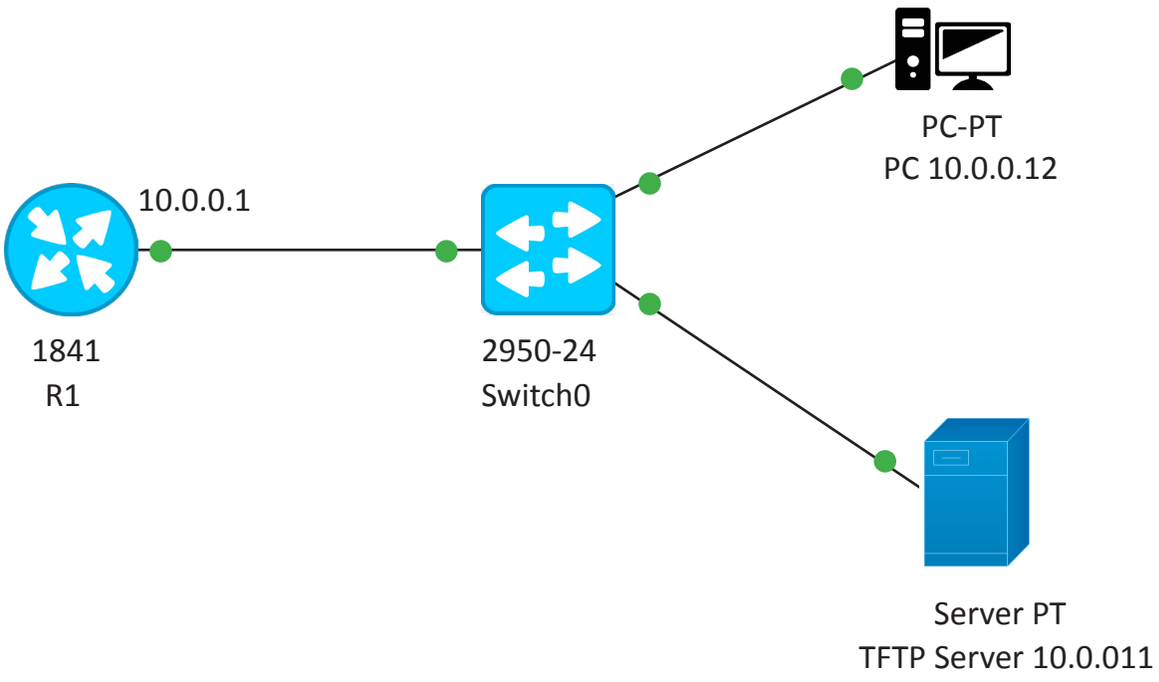
```
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#
```

First we move into the line configuration mode for virtual terminal line. Here '0 4' means we are configuring the router for 0 to 4 i.e. a total of five concurrent telnet sessions. A total of 5 people can telnet this router at the same time. Now we configure the password as cisco for telnet and just like we enabled password checking for console using the login command, we are enabling password checking for telnet. There are these 3 sub portions of telnet config which should be configured on to the router before you can access it through-

1. An interface with IP
2. Enable or Enable secret
3. Vty config (which we just did)

Since our router R1 has these all these, lets verify by trying to telnet it.

Our topology looks like this. We haven't configured anything on the switch.



We just assigned these two hosts IP address so that they can communicate with router. So let's verify the reach ability to R1 using Ping.

```
PC>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Reply from 10.0.0.1: bytes=32 time=1ms TTL=255
Reply from 10.0.0.1: bytes=32 time=0ms TTL=255
Reply from 10.0.0.1: bytes=32 time=0ms TTL=255
Reply from 10.0.0.1: bytes=32 time=0ms TTL=255

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Since we are able to ping let's try to telnet to R1 from PC

```
PC>TELNET 10.0.0.1
Trying 10.0.0.1 ...Open

                NOTICE
    THIS IS A PRIVATE NETWORK. DON'T PROCEED FURTHER IF YOU ARE NOT AUTHORISED
TO


User Access Verification

Password:
Router>EN
Password:
Router#CONF T
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

11. Backup IOS on a TFTP server

We are still using the same topology and continuing on. Before beginning with the process of backup let's verify connectivity to TFTP server using ping.

```
Router#PIng 10.0.0.11

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

! - means the reply for it was received successfully
. - means the device timed out while waiting for the reply.
U - means the destination is unreachable
Also let's check the exact filename of IOS in flash because we will need it next step.

```
R1#SHOw FLAsh:

System flash directory:
File  Length   Name/status
  3   33591768 c1841-advipservicesk9-mz.124-15.T1.bin
  2   28282    sigdef-category.xml
  1   227537   sigdef-default.xml
[33847587 bytes used, 30168797 available, 64016384 total]
63488K bytes of processor board System flash (Read/Write)
```

Now you need to copy from flash to tftp

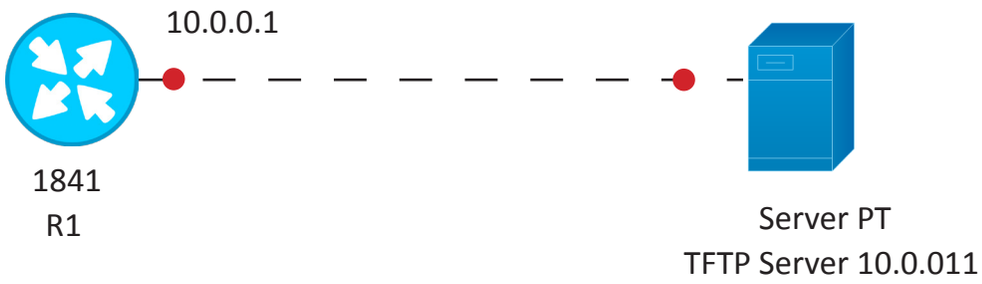
```
R1#copy flash: tftp:
Source filename []? c1841-advipservicesk9-mz.124-15.T1.bin
Address or name of remote host []? 10.0.0.11
Destination filename [c1841-advipservicesk9-mz.124-15.T1.bin]?

Writing c1841-advipservicesk9-
mz.124-15.T1.bin...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 33591768 bytes]

33591768 bytes copied in 1.201 secs (2936716 bytes/sec)
R1#
```

12. IOS installation through ROMMON mode

For this delete the IOS file from flash and reboot the router using reload command in privilege mode or just turn it off and on using the switch on router. Now since there is no IOS in flash router goes into ROMMON mode




```
Boot process failed...

The system is unable to boot automatically.  The BOOT
environment variable needs to be set to a bootable
image.
rommon 1 >
```

So we need to set values for some variables using the below. Make sure you give these variables as it is. There meaning is quite self explanatory.

```
rommon 1 > IP_ADDRESS=10.0.0.1
rommon 2 > IP_SUBNET_MASK=255.0.0.0
rommon 3 > DEFAULT_GATEWAY=10.0.0.1
rommon 4 > TFTP_SERVER=10.0.0.11
rommon 5 > TFTP_FILE=c1841-advipservicesk9-mz.124-15.T1.bin
rommon 6 >
```

To initiate the process of download of the file from TFTP server use

```
rommon 7 > tftpdnld

          IP_ADDRESS: 10.0.0.1
      IP_SUBNET_MASK: 255.0.0.0
     DEFAULT_GATEWAY: 10.0.0.1
         TFTP_SERVER: 10.0.0.11
           TFTP_FILE: c1841-advipservicesk9-mz.124-15.T1.bin
Invoke this command for disaster recovery only.
WARNING: all existing data in all partitions on flash will be lost!

Do you wish to continue? y/n:  [n]:
```

Show the file being received from tftp server

```
-
Receiving c1841-advipservicesk9-mz.124-15.T1.bin from 10.0.0.11 !!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
|
```

Router will erase all the registers on the flash and copy the file to flash.

13. Password recovery for a cisco router

It may happen that you forget the line console password or enable password of a router. So how do you recover the password of the router? The step by step procedure is

1. Power cycle the device and interrupt the boot sequence by using a combination of the keys ctrl+break. It will take you to the ROMMON mode
2. Change the configuration register value to 0x2142.

```
Self decompressing the image :
##################
monitor: command "boot" aborted due to user interrupt
rommon 1 > confreg 0x2142
rommon 2 >
```

In show version commands output previously you can verify that the configuration register value by default is 0x2102. So if this value is at default the router after copying IOS from flash it during booting copies the startup-config from NVRAM if present. By setting the value to 0x2142 we are telling the router to bypass the NVRAM during booting, so the router will start fresh without any config.

3. Power cycle the device. It will boot without any config.
4. Go to privilege mode and do the following

```
Router#copy startup-config running-config
Destination filename [running-config]?

606 bytes copied in 0.416 secs (1456 bytes/sec)
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

5. Go to the global config mode and change or remove the password.

```
R1(config)#no enable password
```

6. Change the configuration register value back to 0x2102.

```
R1(config)#config-register 0x2102
R1(config)#
```

7. Verify its value by using show version. Here the output has been omitted to the part which we are interested in.

```
Configuration register is 0x2142 (will be 0x2102 at next reload)
```

8. Save the configuration using

```
R1#write
Building configuration...
[OK]
R1#
```

9. Reload the router using

```
Router#reload
Proceed with reload? [confirm]
System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)
Initializing memory for ECC
..
c2811 processor with 524288 Kbytes of main memory
Main memory is configured to 64 bit mode with ECC enabled

Readonly ROMMON initialized

Self decompressing the image :
################################################################################
```

TELNET PROTOCOL

The TELNET protocol provides a standardized interface, through which a program on one host (the TELNET client) may access the resources of another host (the TELNET server) as though the client were a local terminal connected to the server.

For example, a user on a workstation on a LAN may connect to a host attached to the LAN as if the workstation was a terminal attached directly to the host. Of course, TELNET may be used across WANs as well as LANs.

Most TELNET implementations do not provide you with graphics capabilities.

TELNET Overview

- TELNET is a general protocol, meant to support logging in from almost any type of terminal to almost any type of computer.
- It allows a user at one site to establish a TCP connection to a login server or terminal server at another site.
- A TELNET server generally listens on TCP Port 23.

How it works

- A user is logged in to the local system, and invokes a TELNET program (the TELNET client) by typing
- telnet xxx.xxx.xxx

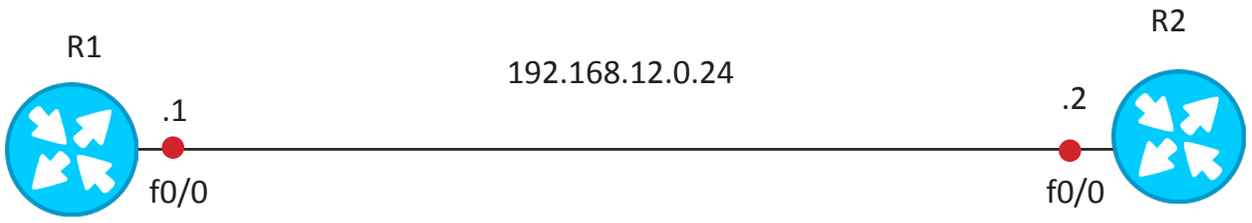
where xxx.xxx.xxx is either a host name or an IP address.

- The TELNET client is started on the local machine (if it isn't already running). That client establishes a TCP connection with the TELNET server on the destination system

```
R2#telnet 192.168.12.1
Trying 192.168.12.1 ... Open


User Access Verification

Password:
R1>en
Password:
R1#
```



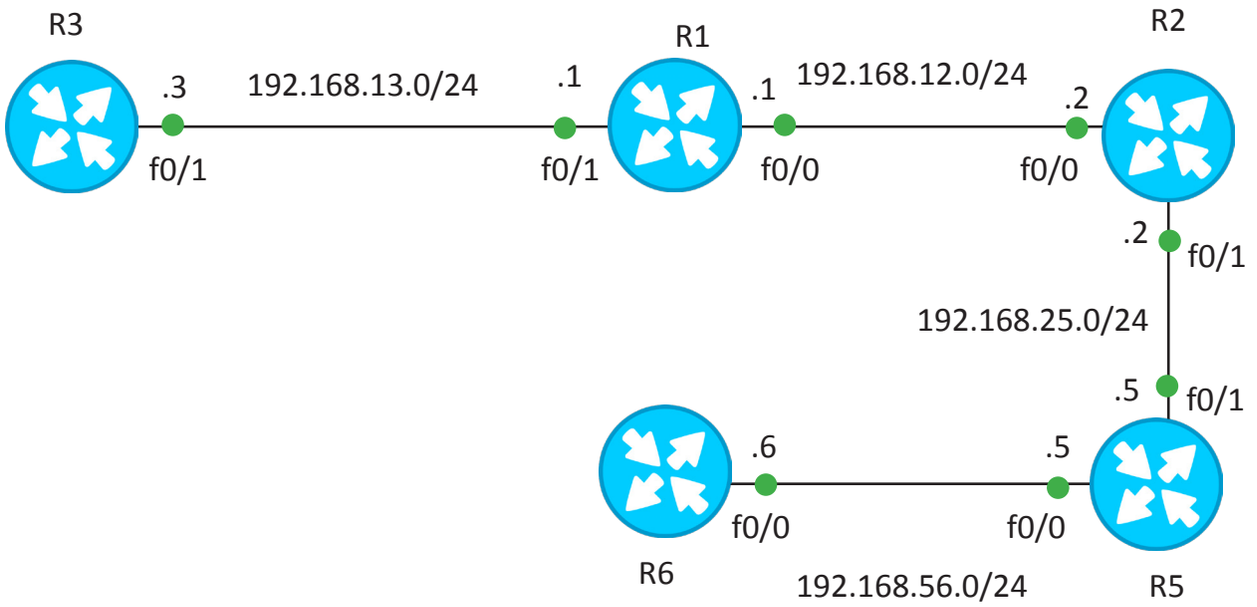
Now you can see R2 configuring R1 by remotely accessing R1 through telnet.
Configuration of telnet on R1:

```
R1#show running-config | section line vty 0 4
line vty 0 4
 password cisco
 login
```

And enable password is necessary for telnet client.

The Traceroute Command

The traceroute command is used to discover the routes that packets actually take when traveling to their destination. On end devices like Windows PC, we use tracert command which works like traceroute command in Cisco Routers.



In the above diagram we will traceroute from r6 to r3 and check the results.

```
Router#traceroute 192.168.13.3
Type escape sequence to abort.
Tracing the route to 192.168.13.3

  1   192.168.56.5    2 msec    0 msec    0 msec
  2   192.168.25.2    0 msec    0 msec    0 msec
  3   192.168.12.1    11 msec   0 msec    0 msec
  4   192.168.13.3    3 msec    0 msec    0 msec
```

With the help of traceroute command we figure out the path of the network and the transit networks.

Cisco Discovery Protocol

Cisco Discovery Protocol (CDP) is a proprietary protocol designed by Cisco to help administrators collect information about both locally attached and remote devices. By using CDP, you can gather hardware and protocol information about neighbor devices, which is useful info for troubleshooting the network.

CDP messages are generated every 60 seconds as multicast messages on each of its active interfaces. The information shared in a CDP packet about a Cisco device includes the following:

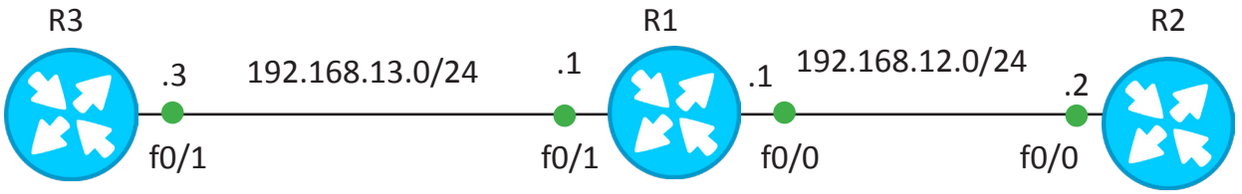
- Name of the device configured with the hostname command
- IOS software version
- Hardware capabilities, such as routing, switching, and/or bridging
- Hardware platform, such as 2600, 2950, or 1900
- The layer-3 address(es) of the device
- The interface the CDP update was generated on

CDP allows devices to share basic configuration information without even configuring any protocol specific information and is enabled by default on all interfaces. CDP is a Data link Protocol occurring at Layer 2 of the OSI model. CDP is not routable and can only go over to directly connected devices.

CDP is enabled, by default, on all Cisco devices. CDP updates are generated as multicasts every 60 seconds with a hold-down period of 180 seconds for a missing neighbor. The no cdp run command globally disables CDP, while the no CDP enable command disables CDP on an interface. Use show CDP neighbors to list out your directly connected Cisco neighboring devices. Adding the detail parameter will display the layer-3 addressing configured on the neighbor.

Cisco Discovery Protocols Configuration commands

Router#show cdp	Displays global CDP information (such as timers)
Router#show cdp neighbors	Displays information about neighbors
Router#show cdp neighbors detail	Displays more detail about the neighbor device
Router#show cdp entry word	Displays information about the device named word
Router#show cdp entry *	Displays information about all devices
Router#show cdp interface	Displays information about interfaces that have CDP running
Router#show cdp interface x	Displays information about specific interface x running CDP
Router#show cdp traffic	Displays traffic information—packets in/out/version
Router(config)#cdp holdtime x	Changes the length of time to keep CDP packets
Router(config)#cdp timer x	Changes how often CDP updates are sent
Router(config)#cdp run	Enables CDP globally (on by default)
Router(config)#no cdp run	Turns off CDP globally
Router(config-if)#cdp enable	Enables CDP on a specific interface
Router(config-if)#cdp enable	Enables CDP on a specific interface
Router(config-if)#no cdp enable	Turns off CDP on a specific interface
Router#clear cdp counters	Resets traffic counters to 0
Router#clear cdp table	Deletes the CDP table
Router#debug cdp adjacency	Monitors CDP neighbor information
Router#debug cdp events	Monitors all CDP events
Router#debug cdp ip	Monitors CDP events specifically for IP
Router#debug cdp packets	Monitors CDP packet-related information



Show CDP Neighbors

```
Router#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce   Holdtme    Capability   Platform    Port ID
Router       Fas 0/1          175           R       C1841       Fas 0/1
Router       Fas 0/0          147           R       C1841       Fas 0/0
```

With cdp neighbors command we get the interface type and platform type of the neighbor. It's a easy way to find the device types connected to a device.

Show CDP Neighbor Details

```
Router#show cdp neighbors detail

Device ID: Router
Entry address(es):
  IP address : 192.168.13.3
Platform: cisco C1841, Capabilities: Router
Interface: FastEthernet0/1, Port ID (outgoing port): FastEthernet0/1
Holdtime: 176

Version :
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team

advertisement version: 2
Duplex: full
---------------------------

Device ID: Router
Entry address(es):
  IP address : 192.168.12.2
Platform: cisco C1841, Capabilities: Router
Interface: FastEthernet0/0, Port ID (outgoing port): FastEthernet0/0
Holdtime: 148

Version :
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team

advertisement version: 2
Duplex: full
```

“

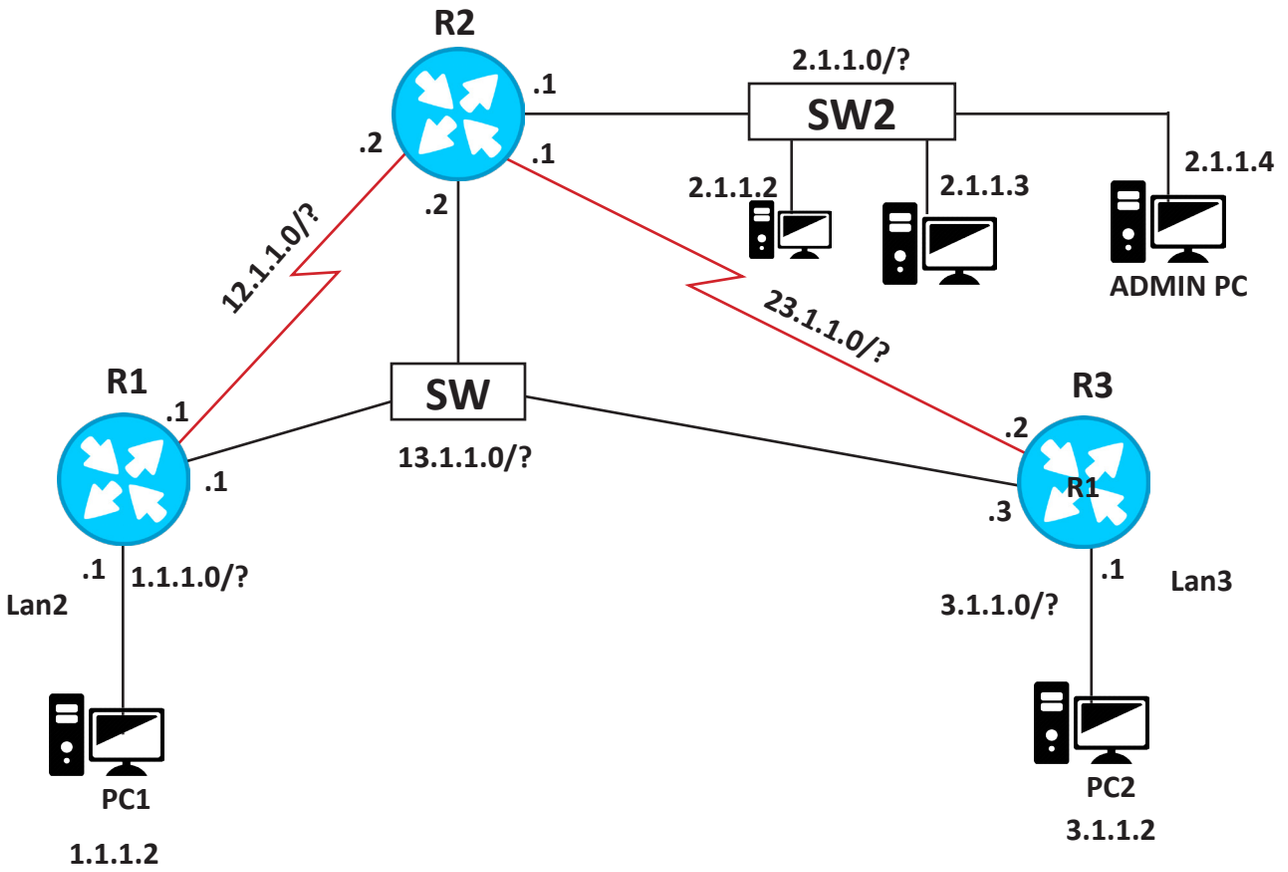
Wow,

You are here finally. 2nd Milestone is also completed successfully.

KEEP YOUR MIND ON THE GO AND GET READY FOR NEXT SET OF CHALLENGES.

”

STATIC ROUTING



Task 1 – BASIC CONFIGURATION

1. Configure IP addressing in accordance with the diagram and follow the instructions given below –

   a. On point to point links, subnet mask should be configured in such a way that it yields only 2 valid IP addresses.

   b. On multi-access segment where R1, R2 and R3 are connected via switch, the subnet mask should be selected in such a way that all the routers get a valid IP address without the wastage of usable IP addresses.

   c. LAN connected to R1 must be able to accommodate at least 50 hosts.

   d. LAN connected to R2 should accommodate 254 hosts.

   e. LAN connected to R3 should accommodate 40 hosts.

   f. While choosing subnet mask or subnet length avoid the wastage of usable IP addresses.

2. Configure the hostname NB followed by the router number on all the routers for example: on router 1 it must be NBR1.
3. Configure console password “CCNA” and enable password “CISCO” on all the routers as well as make sure that passwords must not appear in running configuration in clear text.
4. Configure the banner for console login and remote login on all the routers. The banner must be $WARNING ACCESS RESTRICTED NB ENTERPRISES$
5. Configure the IP address on the end devices as shown in the diagram.

Task 2 : STATIC ROUTING

1. Configure the static routes on R1 to reach the LAN connected to R2 in such a way that its primary path should be via Ethernet link. If the Ethernet link fails then traffic should automatically fall back to serial link. Do not configure any static route to reach PC2 (hint - use AD value).
2. Similarly, configure the static routes on R3 to reach the LAN connected to R2 in such a way that its primary path should be via Ethernet link. If the Ethernet link fails then traffic should automatically fall back to the serial link. Do not configure any static route to reach PC1 (hint - use AD value).
3. In order to reach the LAN networks of R1 and R3, the primary path of R2 should be via Ethernet link. If the Ethernet link fails then traffic to LAN1 and LAN2 must fallback to serial link. **Note :** In the above task, you can use the AD value as lower AD route is always preferred over the higher AD route.
4. At the end, PC1 and PC2 should reach the LAN connected to the router R2 i.e. the Data Center but they must not be able to reach each other.

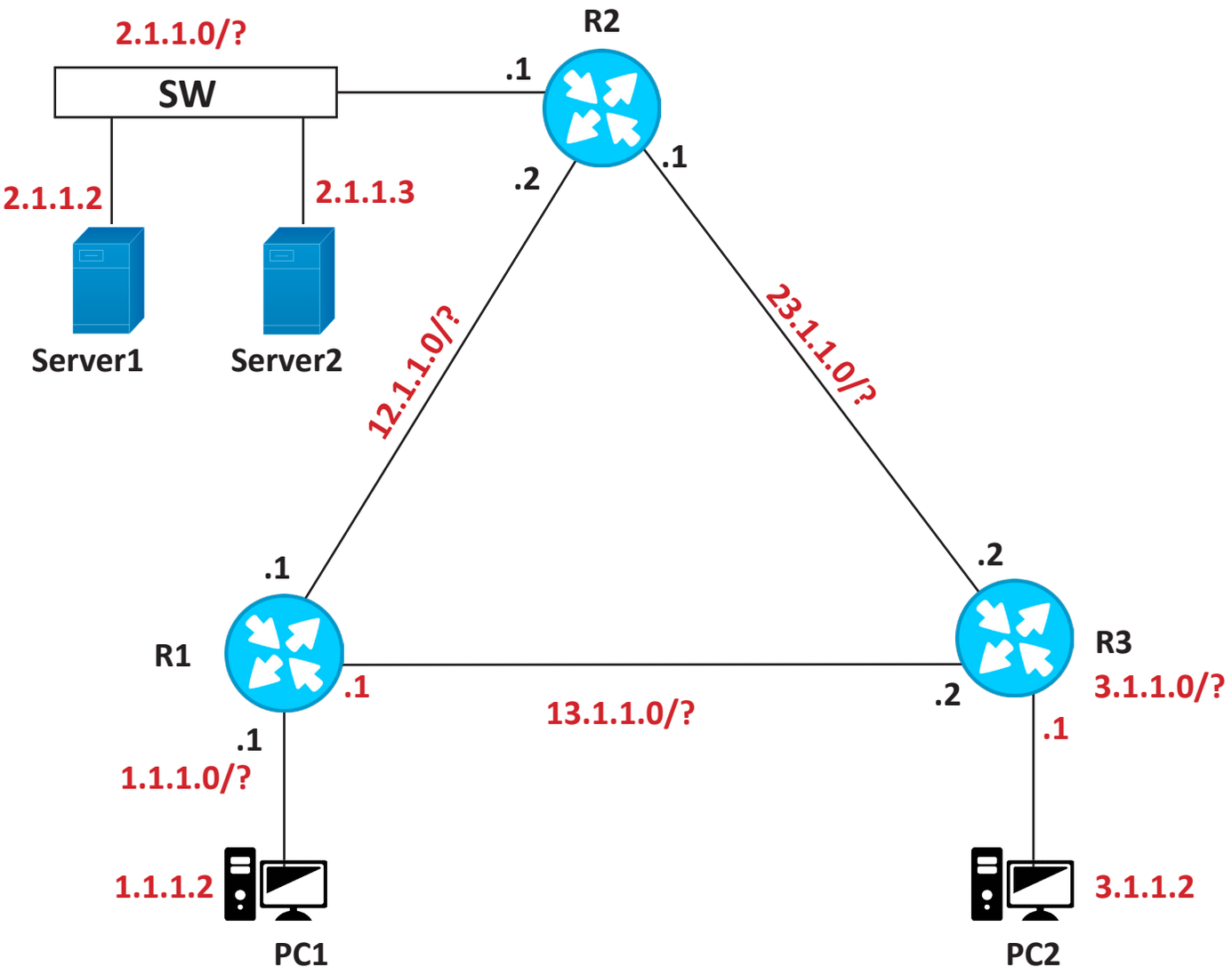
Task 3 : SERVICES AND SECURITY

TELNET

a. Admin PC connected to R2 LAN must be able to telnet all the routers. Now, configure telnet on all the routers in such a way that only admin PC is able to telnet the routers.

b. For remote login use the password “CCNA” on all the routers.

RIP



Task 1 – BASIC CONFIGURATION

1. Configure the hostname on all routers as NB followed by the router number, for example – NBR1 on R1.
2. Configure the username “NETWORKBULLS” and password “CCNA” on all the routers.
3. All the routers must be configured with enable password “CISCO” and the password must not appear in clear text in the running configuration.

4. IP ADDRESSING

   Configure IP addressing on all the routers in accordance with the diagram and choose the appropriate subnet length in such a way that:

   a. Network on the links between the routers must have only two valid IP addresses.
   b. LAN connected to router 1 should have 30 valid IP to accommodate the hosts.
   c. LAN connected to router 3 should have 20 valid IP to accommodate the hosts.
   d. LAN connected to router 2 must have 50 valid IP to accommodate the hosts
   e. Avoid the wastage of usable IP addresses while choosing subnet lengths.

4. Configure the IP addresses as shown in the diagram –

Task 2 : CONFIGURING RIP (RIPv1)

a. Configure RIP version1 on all the router interfaces.
b. Make sure LAN devices connected to the routers must not receive any RIP updates or messages.

Task 3 : CONFIGURING RIPv2

a. Now, change the RIP version1 to version2 on all the routers.
b. Configure the RIP in such a way that all the routers must advertise the routes with actual subnet length as configured on the interfaces.
c. Change the RIP timers –
   Hello interval - 10 sec
   Invalid timer - 30
   Hold interval - 30 sec
   Flush timer - 90 sec

Task 4 : SERVICES AND SECURITY

TELNET

a. Configure telnet for remote access on all the routers and make sure only PC1 is able to telnet all the routers using username and password configured in section 1.2

b. All the routers must prompt PC 1 with banner:
$WARNING ACCESS RESTRICTED NB ENTERPRISES$

SSH

a. For secure remote access you need to configure the domain name “NETWORKBULLS.COM” on all the routers and enable SSH.

b. Only PC1 must be able to SSH all the routers using the username and password configured in section 1.2.

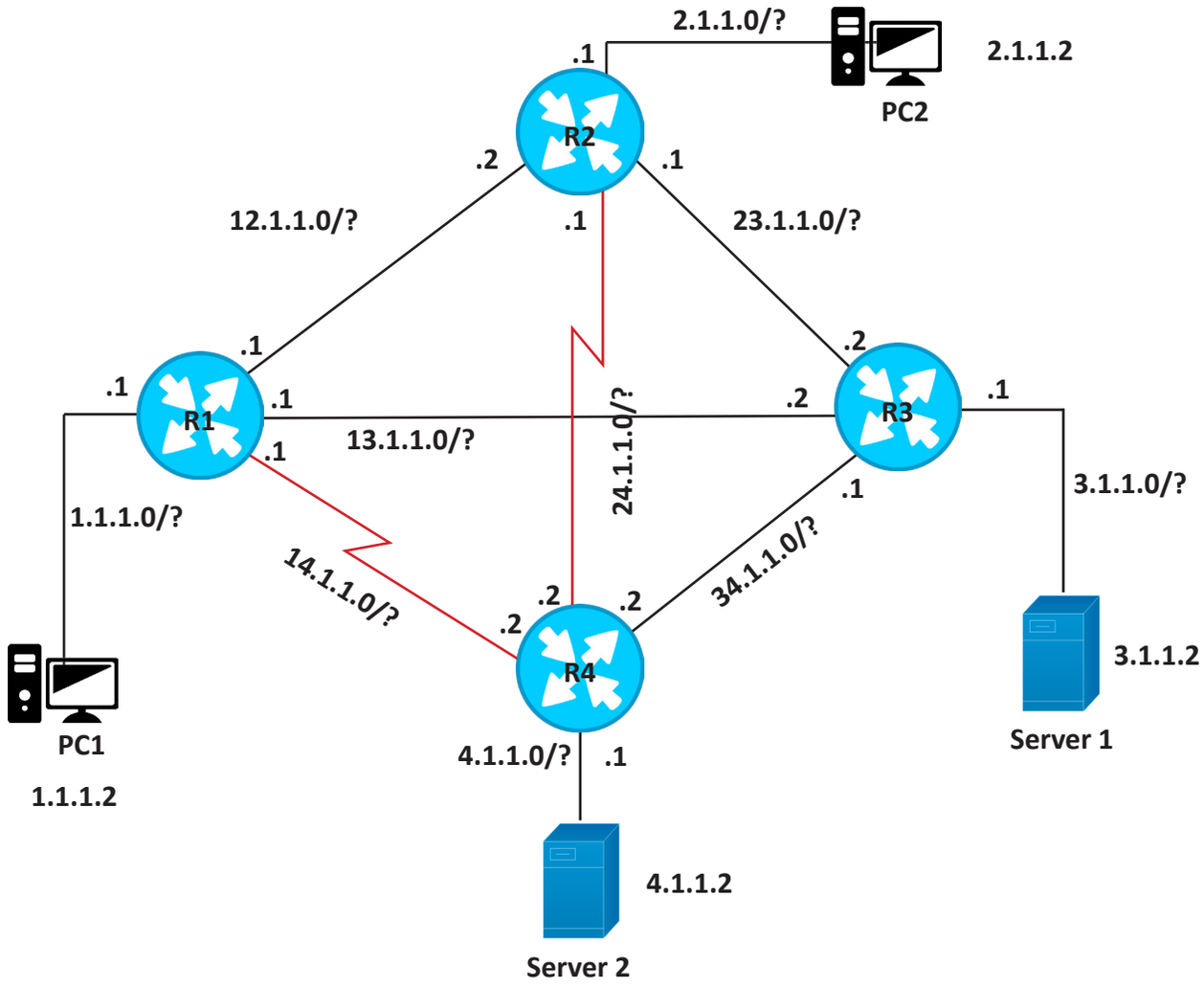
ACCESS-CONTROL

a. PC1 should be able to access all the services on Server1 but it should not be able access any service on Server 2.

b. PC 2 should be able to access all the services on Server2 but it should not be able access any service on Server 1.

Note : use access-list to accomplish the above task.

CCNA EIGRP



Task 1 – BASIC CONFIGURATION

1. Subnets are already mentioned in the diagram, you are supposed to choose the subnet length in such a way that –
   a. All the links between the routers must have the subnet length that only yields two valid IP addresses.
   b. LAN connected to R1 must have 20 valid IP addresses and there should be minimum wastage of IP addresses.
   c. LAN connected to R2, R3 and R4 must have 32, 64 and 254 valid IP addresses respectively.

2. Configure hostname of all the routers as NB followed by their router number, for example – NBr1 on router 1
3. All the routers must have enable password configured as “NETWORKBULLS” and it should not appear in the running configuration in clear text.
4. All the routers must have username configured as “NETWORKBULLS” and password configured as “CISCO”. In case of remote access, this username and password should be used.

Task 2 : CONFIGURING EIGRP

1. Configure EIGRP AS 123 on all the router interfaces and ensure that routers do not send any EIGRP messages on the interfaces where the end devices are connected.
2. Configure hello interval of 3 sec and dead interval of 9 sec on all the routers.
3. After configuring EIGRP, all the routers must find neighbors on the interfaces where routers are connected.

Task 3 : SERVICES AND ACCESS CONTROL

TELNET

a. PC1 must be able to telnet R1 and R3 only.
b. PC2 must be able to telnet R2 and R4 only.
c. Username and password must be the one configured in task 1.4.
d. While remote login users must be prompted with a banner.

$WARNING ACCESS RESTRICTED NB ENTERPRISES$

SSH

a. Configure domain name “NETWORKBULLS.COM” on all the routers and secure the remote access by enabling SSH on all the routers.

ACCESS CONTROL

a. PC1 must have http access to Server1 only.
b. PC2 must have http access to Server2 only.
c. PC1 must not be able to reach Server2 and PC2 must not be able to reach Server 1.

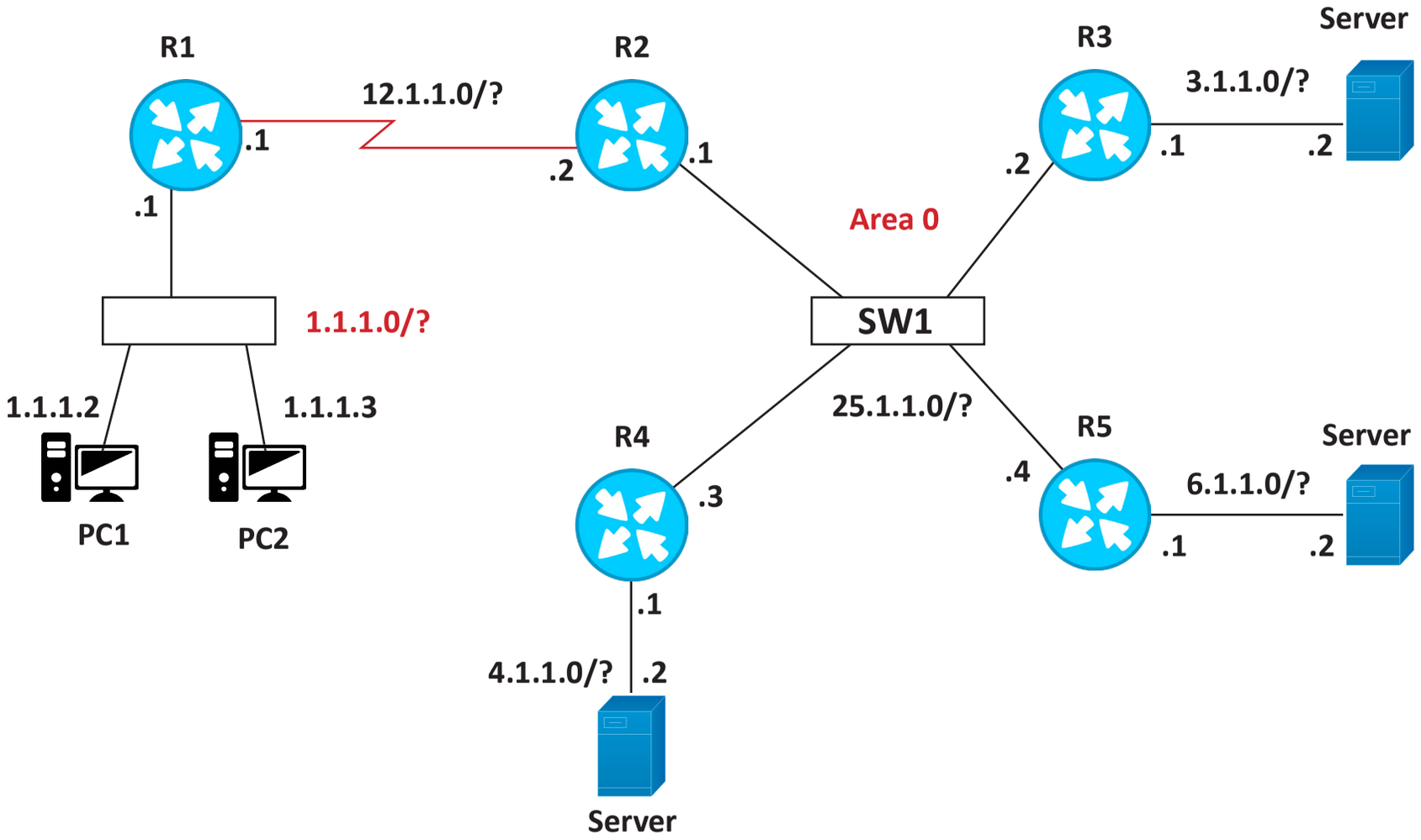
SSH

a. Configure the domain name “NETWORKBULLS.COM” on all the routers and enable SSH.
b. Make sure SSH is the only method for remote access.

ACCESS CONTROL

a. PC1 and PC2 should only access the http services on Server1 and Server2.

Note : Use extended access-list to accomplish this task.


R1
R2
R3
Server
12.1.1.0/?
.1
.2
.1
.2
.1
3.1.1.0/?
.1
.2
Area 0
.1
1.1.1.0/?
SW1
1.1.1.2
1.1.1.3
25.1.1.0/?
R4
R5
Server
.3
.4
6.1.1.0/?
.1
.2
PC1
PC2
.1
4.1.1.0/?
.2
Server

Task 1 – BASIC CONFIGURATION

1. Configure IP addressing in accordance with the diagram in such a way that-
   a. Network mask used between R1 and R2 should only accommodate 2 hosts.
   b. Network mask used between R2, R3, R4 & R5 should accommodate all the routers wasting minimum valid IP addresses.
   c. LAN connected to router 1 should be able to accommodate 180 hosts.
   d. LAN connected to R3 should only accommodate 20 hosts.
   e. LAN connected to R4 & R5 should accommodate 30 and 40 hosts respectively.
2.
   a. Configure a single loopback on all the routers as X.X.X.X where X is the router number for example – 1.1.1.1 for R1.
   b. All the loopbacks must be configured with /32 subnet length.
   c. Hostname of every router must be NB followed by router number for example – NBR1 on R1.

Task 2 – CONFIGURING OSPF

1. Configure OSPF process-id 123 on all the routers.
2. Link between R1 and R2 must be in area 1.
3. Link between R2, R3, R4 and R5 must be configured in area 0.
4. Router-id of every router must be configured manually as the loopback address.
5. Hello and dead intervals on all the routers must be configured as:
   Hello=5 sec
   Dead = 20 sec
6. On the network segment between R2, R3, R4 and R5. R2 must be elected as DR and R3 must be elected as BDR.

Task 3 : SERVICES AND SECURITY

TELNET

a. PC1 is the admin PC which is used to manage all the network routers. From PC 1, we must be able to telnet all the routers for management purpose.
b. Username and password on all the routers must be configured as “NETWORKBULLS” and “CCIE” respectively.
c. Make sure only admin PC must be able to telnet all the routers.

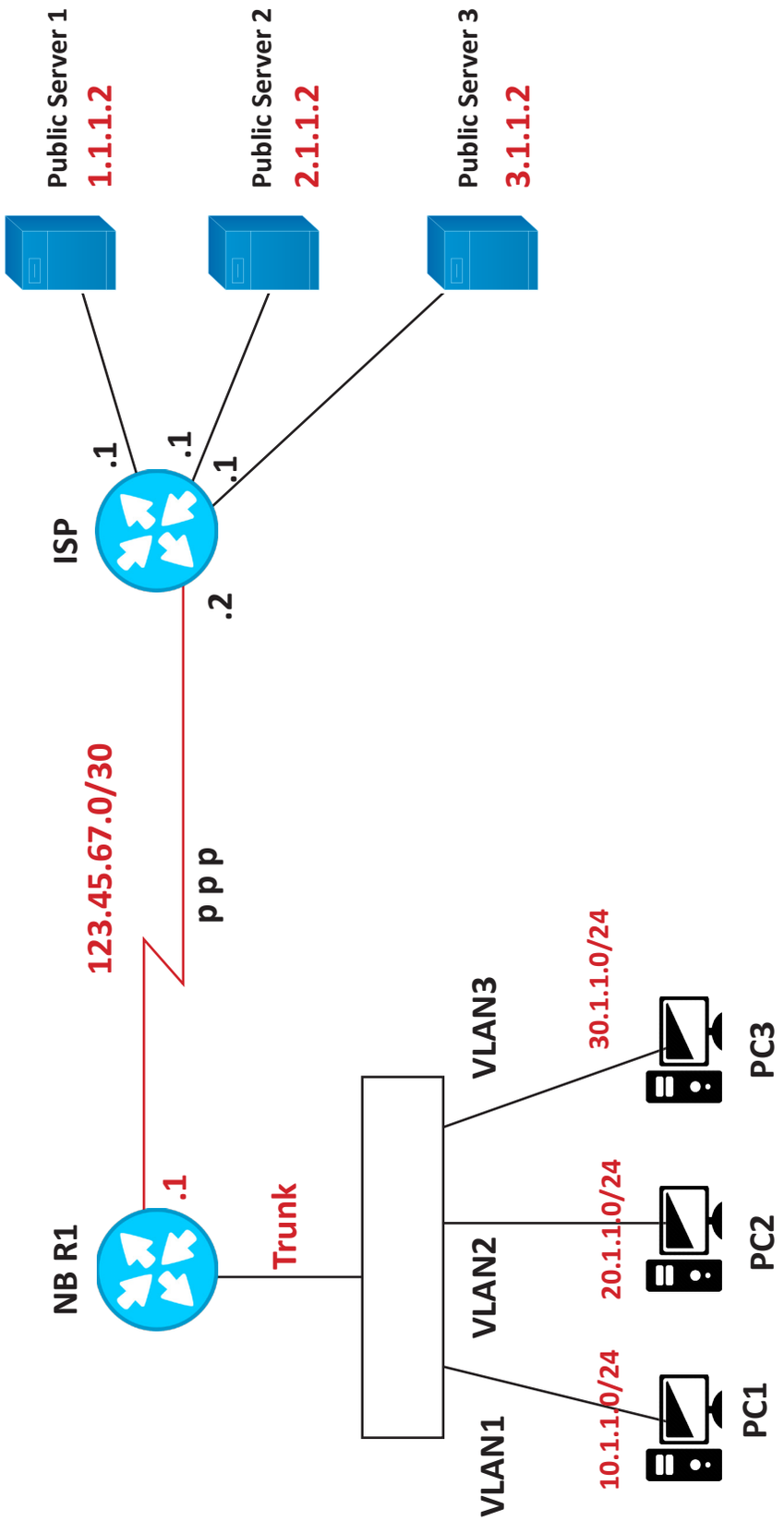
SSH

a. Now, configure domain name NETWORKBULLS.COM on all the routers and enable SSH.
b. Now, only PC1 must be able to SSH all the routers using same username and password as used for telnet.

ACCESS-CONTROL

a. PC1 being the admin PC must be able to ping all the routers and end devices for reachability test.
b. Now, all the servers are running http service but this service must be denied if admin PC tries.
c. PC2 in admin LAN is the end user so from PC2 we must be able to have http access of the server.

Note : use extended access-list to accomplish the above tasks.


Public Server 1
1.1.1.2
Public Server 2
2.1.1.2
Public Server 3
3.1.1.2
.1
.1
.1
ISP
.2
123.45.67.0/30
p p p
.1
NB R1
Trunk
VLAN3
VLAN2
VLAN1
30.1.1.0/24
20.1.1.0/24
10.1.1.0/24
PC3
PC2
PC1

Task 1 : LAN CONFIGURATION

1. In local area network of NB enterprises, configure PC1 in vlan 1, PC2 in vlan 2 and PC3 in vlan 3.
2. Link between switch and router must be configured as 802.1q static trunk on switch.
3. DHCP CONFIGURATION:
    a. Configure router NBR1 as the DHCP server.
    b. PC1 must get the IP address from network 10.1.1.0/24 from the DHCP server and default gateway address 10.1.1.1.
    c. PC2 must get the IP address from network 20.1.1.0/24 from the DHCP server and default gateway address 20.1.1.1.
    d. PC3 must get the IP address from network 30.1.10/24 from the DHCP server and default gateway address 30.1.1.1.
    e. All the computers must get 8.8.8.8 as the DNS server address.
4. INTERVLAN ROUTING:
    a. Make sure all the computers in all the vlans must be able to reach each other.

Task 2 : WAN

1. **IP ADDRESSING**
    a. Configure IP addressing on the link between NBR1 and ISP as shown in the diagram.
    b. Also configure IP addressing on all the public servers connected to ISP as shown in the diagram.

2. **PPP**
    a. Configure encapsulation PPP on the link between NBR1 and ISP.
    b. Configure CHAP authentication on the PPP link where ISP is the authenticator and NBR1 is authenticate.
    c. Username “NBR1” and password “CCIE” must be used for the authentication.

3. DEFAULT ROUTING:

a. Configure a static default route on NBR1 pointing to the ISP for reachability to the public servers.
b. Do not enable any routing protocol on NBR1 as well as do not configure any static route and routing protocol on ISP (no default route on ISP).

4. NAT

STATIC NAT

a. Configure the static network address translation on NBR1 in such a way that only PC1 gets the access to the public servers.
b. Nated traffic must have 123.45.67.1 as the source address.

PAT

a. Configure port address translation on NB1 in such a way that source address of all traffic from PC1, PC2 and PC3 to the public servers must be translated into the address 123.45.67.1 assigned on WAN interface of NBR1.

“

Force your heart,
mind and soul to serve your turn until you are done.

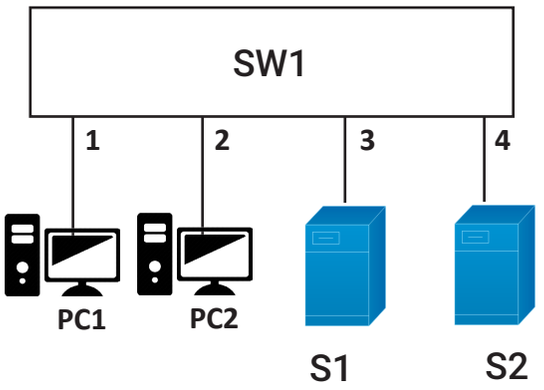
YOU ARE JUST FEW MORE CHALLENGES AWAY FROM THE FINISH LINE, GIVE YOUR BEST SHOT!!

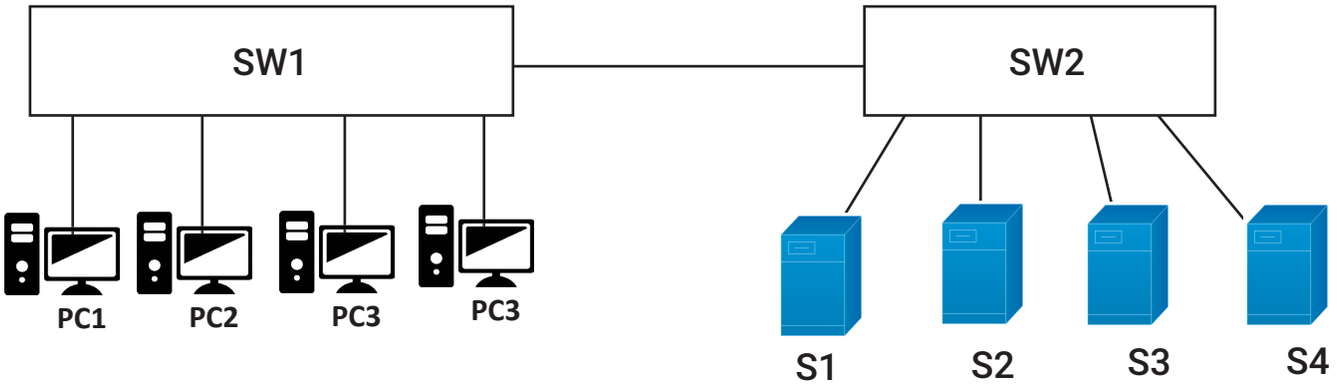
”

BASIC VLAN & TRUNKING

Lan Switching

Digram - 1





Digram - 2

Task 1 :

a. Connect PC1, PC2, Server1 and Server2 to switch one.
b. Now, configure IP addresses on all the devices from the network 10.1.1.0/24.
c. Verify that PC's are reachable to each other.
d. Also verify the mac address table of the switch.

Task 2 :

a. Now, ensure that PC1 only communicates with Server1 and PC2 only communicates with Server2.
b. Refer to the diagram 1.1 for Task 1 and Task 2.

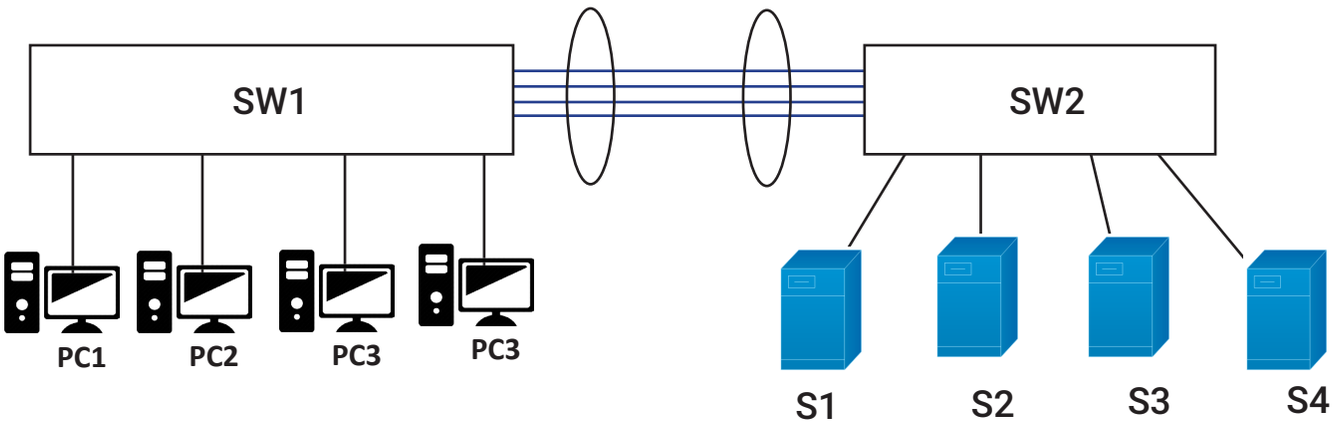
Task 3

a. Now, it has been decided to scale the network by adding one more switch, more PCs and 2 Servers. Make the connections as shown in the diagram.
b. Now, all the PC's and servers must be able to communicate with each other. Use the IP addresses from the network 10.1.1.0/24. (Use diagram 2 for accomplishing the task) Refer to the diagram 1.2.

Task 4

a. Now, only PC1, PC2, Server1 and Server2 should be able to communicate with each other. They should not communicate with any other device in the network.
b. Similarly, PC3, PC4, Server3 and Server4 should communicate with each other and not with any other device in the network. Refer to the diagram 1.2.

ETHERCHANNEL



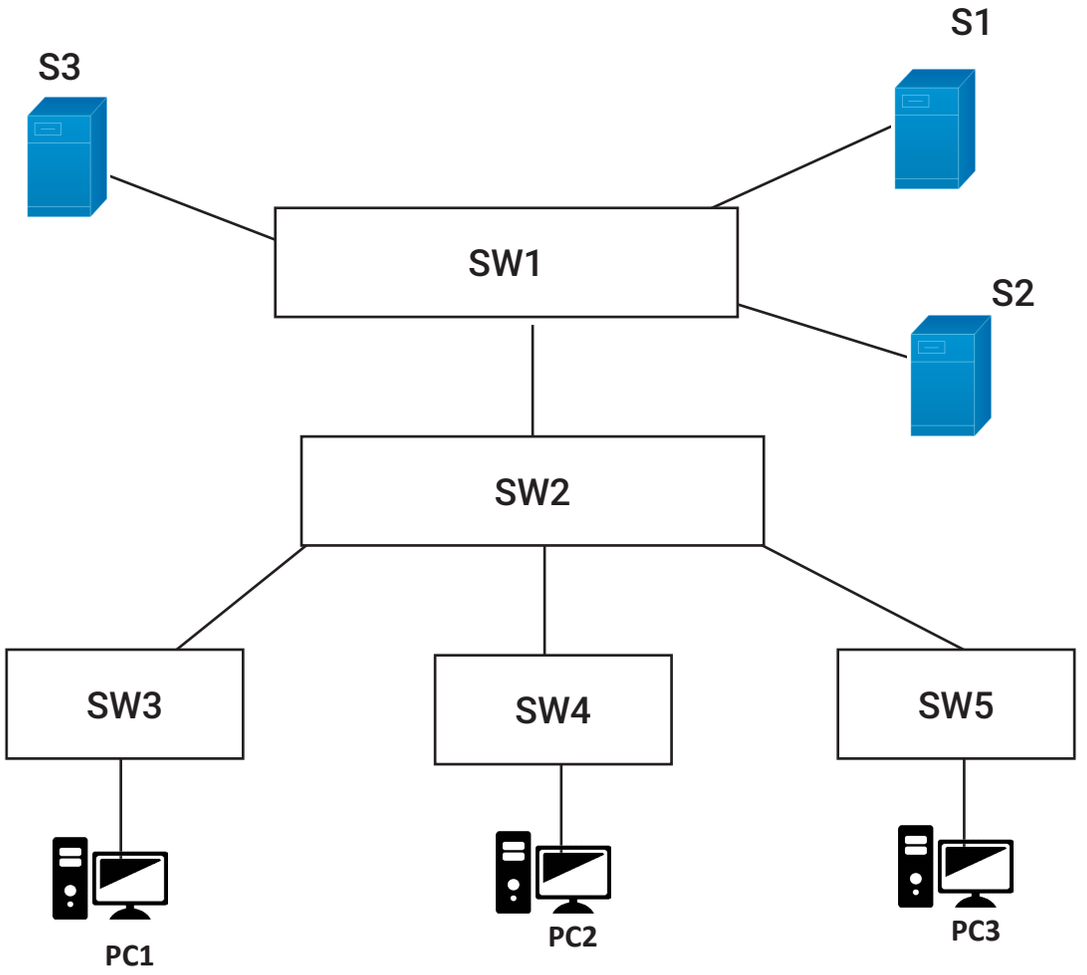
Task 1 :

1. To avoid the congestion configure a port-channel between SW1 and SW2.
2. All the links must be configured as 802.1q static trunks.
3. Use the cisco proprietary protocol for creating the port-channel.
4. SW1 must negotiate the port-channel and SW2 should only respond to the channel negotiation.
5. Configure IP address from the network 10.1.1.0/24.

Network Requirements

1. PC 1, PC2, Server1 and Server2 should only communicate with each other and not with any other device in the network.
2. Similarly, PC3, PC4, Server3 and Server4 should only communicate with each other and not with any other device in the network.

VTP (VLAN TRUNKING PROTOCOL)



Task 1 : BASIC CONFIGURATION

a. Connect the devices as shown in the diagram.

b. All the links between the switches must be configured as the static 802.1q trunks.

Task 2 : VTP CONFIGURATION

a. SW1 must be configured as the VTP server, SW2 must be configured as the VTP transparent switch.

b. SW3, SW4 and SW5 must be configured as VTP clients.

c. Configure VTP domain “networkbulls.com” on all the switches.

d. Configure VTP password “CCNA” on all the switches except the transparent switch.

e. Create VLAN 1-10 on server switch and make sure that the VLANs must be propagated to all the client switches by the server.

Task 3 : HOST CONFIGURATION

a. Configure PC1 on SW3 in VLAN3, PC2 on SW4 in VLAN4 and PC3 in VLAN 5 on SW5.

b. Configure Server1, Server2 and Server3 on SW1 in VLAN 3, 4 and 5 respectively.

c. Now, PC1 must be able to communicate with Server1, PC2 must be able to communicate with Server2 and PC3 must be able to communicate with Server3 in the network.

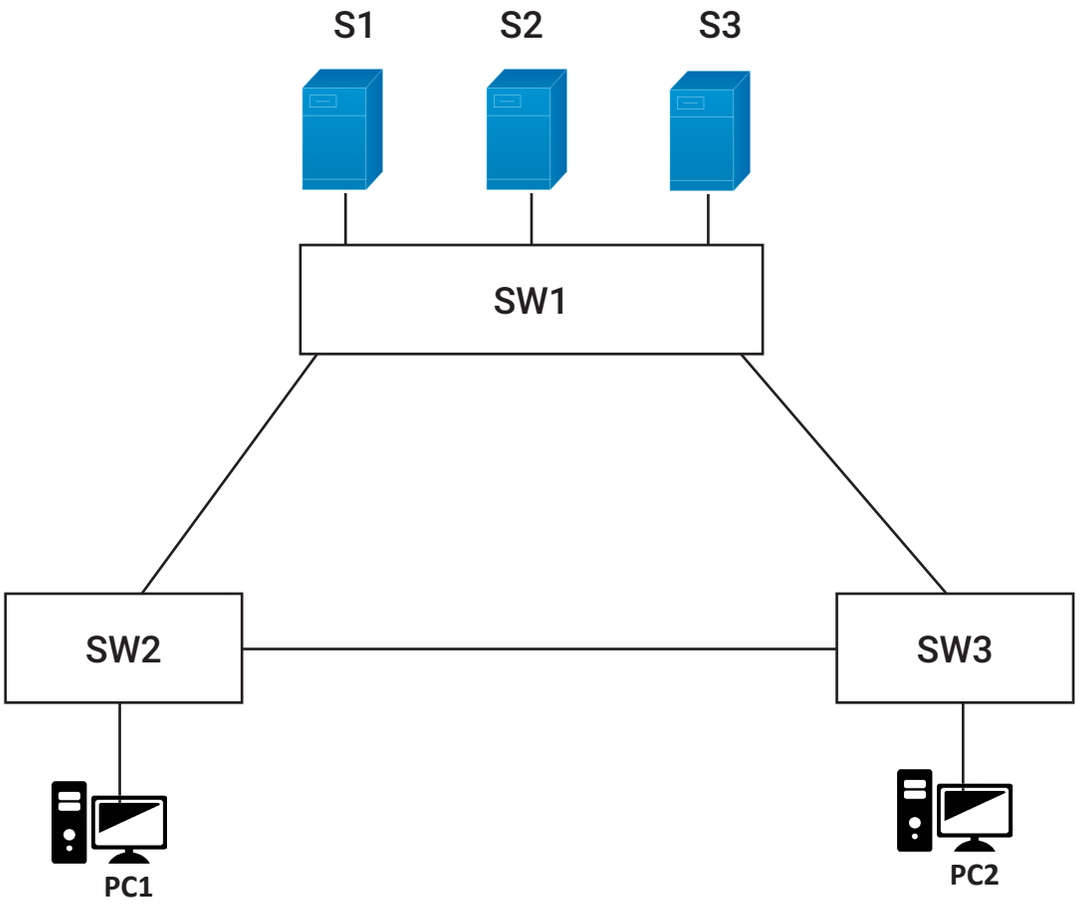
Task 4 : PORT-SECURITY

a. Configure port security on SW3 in such a way that if any other user connects to the port where PC1 is connected then the port should immediately shut-down.

b. Configure port security on SW4 in such a way that if any other user connects to the port where PC2 is connected then the port should remain up but no data transmission should be allowed through the port.

c. Configure port security on SW5 in such a way that if any other user connects to the port where PC3 is connected then the port should remain up but no data transmission should be allowed through the port. In addition, switch must also generate the log messages.

VTP AND SPANNING-TREE PROTOCOL



Task 1 : BASIC CONFIGURATION

a. Connect the devices as shown in the diagram.
b. All the links between the switches must be configured as the static trunk with 802.q encapsulation.

Task 2 : VTP

a. Configure SW1 as the VTP server and SW2 & SW3 as the VTP client.
b. VTP domain name must be “NETWORKBULLS.COM”.
c. VTP password must be “CCNA”.
d. Create VLAN 1-10 on server switch and all the VLANs must be propagated to the client switches by the server.

Task 3 : STP

a. Configure per- VLAN spanning-tree on all the switches (pvst).
b. Make sure SW1 is the root-bridge for all the VLANs.
c. In case SW1 fails, SW2 should become the root bridge.
d. Spanning-tree cost of all the interfaces must be configured as 1.
e. Spanning-tree port priority of every interface must be 16.

Task 4 : HOST Configuration

a. All the ports where end devices are connected must be configured as the static access ports.
b. Enable portfast on all the access-ports.
c. Configure all the PCs and servers in such a way that they all can communicate with each other. Use the IP addressing scheme of your choice.

www.trainme.bh