**CCNA ASSIGNMENT**

**Module – 2**

1. Describe IPv4 address range and explain example of subnetting.

Each IP class is equipped with its own default subnet mask which bounds that IP class to have prefixed number of Networks and prefixed number of Hosts per network. Classful IP addressing does not provide any flexibility of having less number of Hosts per Network or more Networks per IP Class.

CIDR or Classless Inter Domain Routing provides the flexibility of borrowing bits of Host part of the IP address and using them as Network in Network, called Subnet. By using subnetting, one single Class A IP address can be used to have smaller sub-networks which provides better network management capabilities.

The process of taking an extensive network and splitting into smaller networks is known as subnetting — and it's freeing up more public IPv4 addresses.

There are two parts to an IP address: The network portion and the host portion.

It's like the address for a house. The network portion is like the city, state, and zip code. The host portion is like the house and street number.

A subnet defines the number of bits, out of 32, used for the "network portion" of the address. Subnet masks can also be defined in a more common 'slash' representation, known as CIDR notation. In the following table, the red digits represent the bits used for the network. The black digits will be used for device IP addresses. Note that the 255.0.0.0 mask can also be represented as a '/8' because it reserves 8 bits of the overall 32 bits used to describe an IPv4 address as the network portion.

1. List of private address.

10.0.0.0/8 IP addresses: 10.0.0.0 – 10.255.255.255

172.16.0.0/12 IP addresses: 172.16.0.0 – 172.31.255.255

192.168.0.0/16 IP addresses: 192.168.0.0 – 192.168.255.255

1. What is routing? Explain work of Router and protocol.

Routing is a process in which the layer 3 devices (either router or layer 3 switches) find the optimal path to deliver a packet from one network to another. Dynamic routing protocols use metric, cost, and hop count to identify the best path from the path available for the destination network.

1. Distance Vector Routing Protocol:

These protocols select the best path on the basis of hop counts to reach a destination network in a particular direction. Dynamic protocol like RIP is an example of a distance vector routing protocol. Hop count is each router that occurs in between the source and the destination network. The path with the least hop count will be chosen as the best path.

2. Link State Routing Protocol:

These protocols know more about Internetwork than any other distance vector routing protocol. These are also known as SPF (Shortest Path First) protocol. OSPF is an example of link-state routing protocol.

3. Advanced Distance vector routing Protocol:

It is also known as hybrid routing protocol which uses the concept of both distance vector and link-state routing protocol. Enhanced Interior Gateway Routing Protocol (EIGRP) is an example of this class of routing protocol. EIGRP acts as a link-state routing protocol as it uses the concept of Hello protocol for neighbour discovery and forming an adjacency. Also, partial updates are triggered when a change occurs. EIGRP acts as a distance-vector routing protocol as it learned routes from directly connected neighbours.

1. Which software we practise for routing and switching.

* Solar Winds Network Insight
* Paessler PRTG Router Monitoring
* Manage Engine OpManager
* Nagios XI
* Zenoss
* WhatsUp Gold
* Icinga 2

1. Explain Basic command.

* Ping
* Netstat
* Ip Config
* Hostname
* Tracert
* Ns Lookup
* Route
* ARP
* Path Ping

1. Types of Routing – example of Static routing.

1. Static routing –

Static routing is a process in which we have to manually add routes to the routing table.

2. Default Routing –

This is the method where the router is configured to send all packets towards a single router (next hop). It doesn’t matter to which network the packet belongs, it is forwarded out to the router which is configured for default routing. It is generally used with stub routers. A stub router is a router that has only one route to reach all other networks.

3. Dynamic Routing –

Dynamic routing makes automatic adjustments of the routes according to the current state of the route in the routing table. Dynamic routing uses protocols to discover network destinations and the routes to reach them. RIP and OSPF are the best examples of dynamic routing protocols. Automatic adjustments will be made to reach the network destination if one route goes down.

Example of Static Routing:-

Lightbox

R1 having IP address 172.16.10.6/30 on s0/0/1, 192.168.10.1/24 on fa0/0.

R2 having IP address 172.16.10.2/30 on s0/0/0, 192.168.20.1/24 on fa0/0.

R3 having IP address 172.16.10.5/30 on s0/1, 172.16.10.1/30 on s0/0, 10.10.10.1/24 on fa0/0.

Now configuring static routes for router R3:

R3(config)#ip route 192.168.10.0 255.255.255.0 172.16.10.2

R3(config)#ip route 192.168.20.0 255.255.255.0 172.16.10.6

Here, provided the route for 192.168.10.0 network where 192.168.10.0 is its network I’d and 172.16.10.2 and 172.16.10.6 are the next-hop address.

Now, configuring for R2:

R2(config)#ip route 192.168.20.0 255.255.255.0 172.16.10.1

R2(config)#ip route 10.10.10.0 255.255.255.0 172.16.10.1

R2(config)#ip route 172.16.10.0 255.255.255.0 172.16.10.1

Similarly for R1:

R1(config)#ip route 192.168.10.0 255.255.255.0 172.16.10.5

R1(config)#ip route 10.10.10.0 255.255.255.0 172.16.10.5

R1(config)#ip route 172.16.10.0 255.255.255.0 172.16.10.5

1. Difference between RIP, EIGRP and OSPF

|  |  |  |
| --- | --- | --- |
| **RIP** | **OSPF** | **EIGRP** |
| **RIP stands for Routing Information Protocol** | **OSPF stands for Open Shortest Path First** | **EIGRP stands for Enhanced Interior Gateway Routing Protocol** |
| **RIP is a distance vector protocol** | **OSPF is a link state protocol** | **EIGRP Is derived from Integrated Gateway Routing Protocol** |
| **The metrics used Is**[**hop**](https://en.wikipedia.org/wiki/Hop_(networking))**.** | **The metrics used are bandwidth and delay.** | **The metrics used are bandwidth, delay, load and reliability** |
| **RIP uses Distance vector algorithm to calculate the best path** | **OSPF uses the SPF algorithm to calculate the best path.** | **EIGRP uses Diffusing update algorithm to calculate the best path.** |
| **In RIP, networks are not divided into areas or tables.** | **Routing with OSPF is done in Autonomous System, Areas, Stub Areas and Backbone areas.** | **Routing with EIGRP is done in Neighbour Tables, Topology tables, and Routing tables.** |
| **Maximum hop count is 15.** | **No hop count.** | **Maximum hop count is 255.** |

1. Example of Default routing.

This is the method where the router is configured to send all packets towards a single router (next hop). It doesn’t matter to which network the packet belongs, it is forwarded out to the router which is configured for default routing. It is generally used with stub routers. A stub router is a router that has only one route to reach all other networks.

https://media.geeksforgeeks.org/wp-content/uploads/ccoco-1.png

In this topology, R1 and R2 are stub routers so we can configure default routing for both these routers.

Configuring default routing for R1:

R1 (config) #ip route 0.0.0.0 0.0.0.0 172.16.10.5

Now configuring default routing for R2:

R2 (config) #ip route 0.0.0.0 0.0.0.0 172.16.10.1

1. Explain Autonomous system number.

An autonomous system number (ASN) is something that businesses or other parties have to get from internet domain registrars, in order to set up internal network systems that interface with other networks over the Internet.

1. What is switching explain VLAN?

Switching is process to forward packets coming in from one port to a port leading towards the destination. When data comes on a port it is called ingress, and when data leaves a port or goes out it is called egress. A communication system may include number of switches and nodes.

A VLAN is identified on network switches by a VLAN ID. Each port on a switch can have one or more VLAN IDs assigned to it and will land in a default VLAN if no other one is assigned. Each VLAN provides data-link access to all hosts connected to switch ports configured with its VLAN ID.

1. What is Access port and trunk port?

Access port - An access port is a connection on a switch that transmits data to and from a specific VLAN. Because an access port is only assigned to a single VLAN, it sends and receives frames that aren’t tagged and only have the access VLAN value. This doesn’t cause signal issues because the frames remain within the same VLAN. If it does happen to receive a tagged packet, it will simply avoid it. This is a simpler configuration, but not the most efficient choice if the network is even moderately complex.

Trunk port - Unlike an access port, a trunk port can transmit data from multiple VLANs. If you have a dozen VLANs on a particular switch, you don’t need additional cables or switches for each VLAN—just that single link. A trunk port allows you to send all those signals for each switch or router across a single trunk link. In contrast to an access port, a trunk port must use tagging in order to allow signals to get to the correct endpoint. Trunk ports typically offer higher bandwidth and lower latency than access ports.

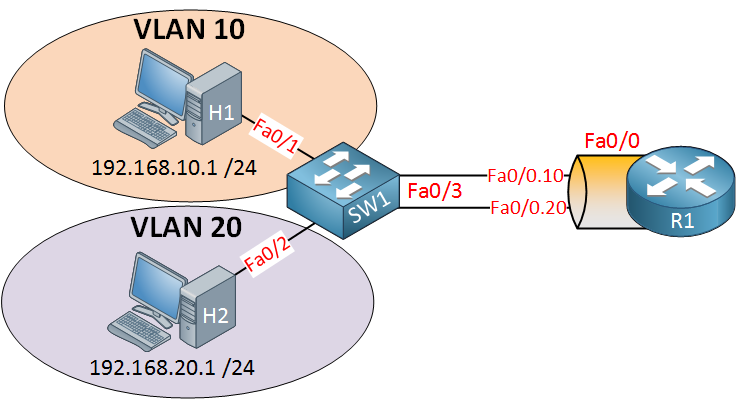
1. List of basic SHOW command.

* Show version
* Show running-config
* Show interfaces
* Show logging
* Show tech-support
* Show version
* Show running-config
* Show controllers
* Show stacks
* Show interfaces
* Show buffers
* Show processes memory
* Show processes CPU

1. Explain Layer 2 and Layer 3 switch.

Layer2 is the process of using devices and MAC addresses on a LAN to segment a network. A Layer 3 switch is a switch that performs routing functions in addition to switching. Layer 2 switches perform the switching function to re-arrange the data frames from the source to its destination network.

1. Example of inter VLAN routing.



SW1(config)#**interface fa0/3**

SW1(config-if)#**switchport trunk encapsulation dot1q**

SW1(config-if)#**switchport mode trunk**

SW1(config-if)#**switchport trunk allowed vlan 10,20**

R1(config)#**interface fa0/0.10**

R1(config-subif)#**encapsulation dot1Q 10**

R1(config-subif)#**ip address 192.168.10.254 255.255.255.0**

R1(config)#**interface fa0/0.20**

R1(config-subif)#**encapsulation dot1Q 20**

R1(config-subif)#**ip address 192.168.20.254 255.255.255.0**

SW1(config)#**ip routing**

SW1(config)#**interface vlan 10**

SW1(config-if)#**no shutdown**

SW1(config-if)#**ip address 192.168.10.254 255.255.255.0**

SW1(config)#**interface vlan 20**

SW1(config-if)#**no shutdown**

SW1(config-if)#**ip address 192.168.20.254 255.255.255.0**

1. Explain switching method and VTP.

A switching method defines how a switch processes a frame. A frame is a piece of the data stream that is transferred between two devices in the network. It consists of four objects: the hardware address of the source device, the hardware address of the destination device, control options, and data.

Hardware addresses of the source and destination devices are respectively used to identify the sender and receiver devices of the frame. A hardware address is also known as the MAC address. Control options are mainly used for two purposes: to verify the integrity of the frame and to identify the upper-layer protocol that should be used to process the frame at the destination device. A frame is also known as the Ethernet frame.

1. What is spanning Tree – Mention spanning tree protocol and algorithm?

A spanning tree is a subset of Graph G, which has all the vertices covered with minimum possible number of edges. Hence, a spanning tree does not have cycles and it cannot be disconnected.. By this definition, we can draw a conclusion that every connected and undirected Graph G has at least one spanning tree.

STP Protocol is defined as a link management protocol designed to support redundant links that stops switching loops in the STP network.

Spanning trees use an algorithm to search for the redundant links in the LAN and select the best paths. It is mainly used to put all links in either forwarding or blocking.

After this process, all the links without a redundant link is likely to be in the forwarding state. The redundant links that were not as good as the selected links would be blocking. Spanning Tree never uses multiple links to the same destination. There is no load-sharing feature with Spanning Tree.

1. Example of Per VLAN spanning tree.

One of the things that must be considered with VLANs is the function of the Spanning Tree Protocol (STP). STP is designed to prevent loops in a switch/bridged topology to eliminate the endless propagation of broadcast around the loop. With VLANs, there are multiple broadcast domains to be considered. Because each broadcast domain is like a unique bridged internetwork, you must consider how STP will operate.

The 802.1Q standard defines one unique Spanning Tree instance to be used by all VLANs in the network. STP runs on the Native VLAN so that it can communicate with both 802.1Q and non-802.1Q compatible switches. This single instance of STP is often referred to as 802.1Q Mono Spanning Tree or Common Spanning Tree (CST). A single spanning tree lacks flexibility in how the links are used in the network topology. Cisco implements a protocol known as Per-VLAN Spanning Tree Plus (PVST+) that is compatible with 802.1Q CST but allows a separate spanning tree to be constructed for each VLAN. There is only one active path for each spanning tree; however, in a Cisco network, the active path can be different for each VLAN.

1. What is IPv6? Explain types and ip address range.

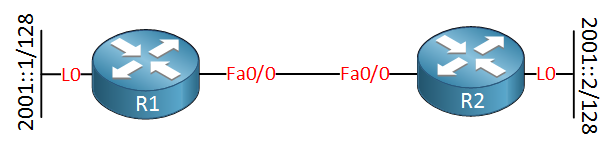
IPv6 addresses consist of 128 bits, instead of 32 bits, and include a scope field that identifies the type of application suitable for the address. IPv6 does not support broadcast addresses, but instead uses multicast addresses for broadcast. In addition, IPv6 defines a new type of address called any cast.

All IPv6 addresses are 128 bits long, written as 8 sections of 16 bits each. They are expressed in hexadecimal representation, so the sections range from 0 to FFFF. Sections are delimited by colons, and leading zeroes in each section may be omitted. If two or more consecutive sections have all zeroes, they can be collapsed to a double colon.

Example of IPv6:-

3FFE:0000:0000:0001:0200:F8FF:FE75:50DF

1. Example of Ipv6 – RIP



R1(config)#**ipv6 unicast-routing**

R1(config)#**interface loopback 0**

R1(config-if)#**ipv6 address 2001::1/128**

R2(config)#**ipv6 unicast-routing**

R2(config)#**interface loopback 0**

R2(config-if)#**ipv6 address 2001::2/128**

R1(config)#**interface fastEthernet 0/0**

R1(config-if)#**ipv6 enable**

R2(config)#**interface fastEthernet 0/0**

R2(config-if)#**ipv6 enable**

R1(config)#**ipv6 router rip RIPNGTEST**

R1(config-rtr)#**exit**

R1(config)#**interface fastEthernet 0/0**

R1(config-if)#**ipv6 rip RIPNGTEST enable**

R1(config-if)#**exit**

R1(config)#**interface loopback 0**

R1(config-if)#**ipv6 rip RIPNGTEST enable**

R2(config)#**ipv6 router rip RIPNGTEST**

R2(config-rtr)#**exit**

R2(config)#**interface fastEthernet 0/0**

R2(config-if)#**ipv6 rip RIPNGTEST enable**

R2(config-if)#**exit**

R2(config)#**interface loopback 0**

R2(config-if)#**ipv6 rip RIPNGTEST enable**