# CCNA 200-301
# Notes

Rohit Raj Karki

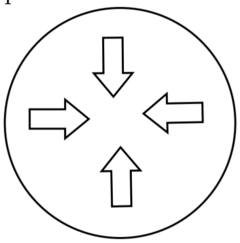
# Contents

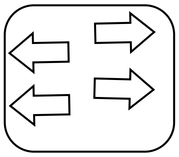
# Chapter 1

# Networks Devices

## 1.1 Computer Network

A computer network is a digital telecommunications network which allows nodes to share resources.





Two PCs connected with eachother is called networks.Now that they are connected with eachother they can share the data with eachother. **Client**
A Client is a device that accesses a service available by a server.
**Server**
A device that provides function or services for clients. A server can also be a client.

**Note:-**

The same device can be a client in some situations, and a server in other situations.

Typically you don't connect PCs or severs directly to eachother. You aggregate the connections to a device called a switch. Switches have a lot of interfaces for you to connect end hosts to. Switches are used to forward netork with a LAN a local area network. We have one LAN on the left and one LAN ont the right. The hosts within each LAN(such as network printer, pcs) can send data from one another. for example PC1 and PC2. These switches cannot cannot with eachother.

- have many network interfaces/ports for end hosts to connect to (usually 24+).
- provide connectivity to hosts with the same LAN.
- donot provide connectivity between LANS/over the internet. We need another type of device called router.

**Router**
When end hosts in the New York Branch LAN want to communicate with end hosts in the Tokyo branch LAN , they will send the data to their router R1, which will then forward the data to the Tokyo Branch via internet. So, lets suppose a scenario when the PC in LAN1 wants a data from server1 of tokyo branch. It will request the data via a switch S1 which inturn connect with the router R1 and that router connects with the internet and the router R2 via switch S2 which connects the server and the data flow in the reverse order.
Types of Router

- ISR 1000
- ISR 900

- ISR 4000

**Firewall**
Firewall are specially network security that controls network traffic entering an exiting your network. Firewalls can be placed 'outside' of your router.

- monitor and control network traffic based on configured rules
- can be placed inside the network or outside the network.
- are known as 'Next-Generation Firewalls when thry include more modern and advanced filtering capabilties.

What about the firewall on your computer?
**Types of switches**
1. Catalyst 9200

> **Note:-**
> RJ = Registered Jack

**Ethernet**
**Bits and bytes**
Bits : Series of 0's or 1's. When communicating across a copper network cable,a variation of the electrical signal is assumed as 0's or 1's.
Bytes: Series of 8 0's and 1's.
Speed is measured in bits per second.(Kbps,Mbps,Gbps,etc not bytes per second.) in Harddisk data is transmitted in the bytes per second. **Ethernet Standards**
defined in IEEE 802.3 standard in 1983.

- 10Mbps Ethernet 10BASE-T
- 1000Mbps Fast Ethernet 100BASE-T
- 1Gbps Gigabit Ethernet 1000BASE-T
- 10Gbps 10 Gig Ethernet 10GBASE-T

**UTP cables** Unshielded Twisted Pair : Un shieled means that the wires have no metallic shield which can make them vulnerable to electrical interferences. The twist actually helps protect against electromagentic interference or EMI. Four pairs of wires twisted with each other.
10BASE-T ans 100BASE-T = 2 pairs (4 wires)
1000BASE-T ans 1GBASE-T = 4 pairs (8 wires)
Routers transmits data on pin 1 and 2 and receive data on pins 3 and 6(this are same in PCs) but switch is exactly opposite.
Communication in between the routers donot work in this case .
**StraightThrough cable**
A straight through cable connects pin1 to pin1 ,pin2 to pin2,pin3 to pin3 and etc.
**Crosscable cable**
Pin1 connects to pin 3 and Pin2 connects to Pin 6 on the other end and Pin3 connects to pin1 and Pin 6 connects to pin 2 on the left side.
**Auto MDI X**
Auto MDI X allows devices to automatically detect which pins their neighbour is transmitting data on and then adjust themselves to receive data on the other pins.

**How to connect to a cisco device(console)**
Router = user EXEC mode

Router# = privileged EXEC mode
Router(config)# = Global configuration mode
Router enable = used to enter privileged EXEC mode
Router#configure terminal = used to enter global configuration mode
Router(config)# enable password ¡password¿= configures a password to protect privileged exec mode
Router(config)# service password -encryption = encrypts the enable password
Router(config)# enable secret ¡password¿ = configures a more secure ,always -encypted enable password
Router(config) # run privleged -exec level command from global configuration mode
Router(config) #no command = removes the command
Router(config) #show running-config = displays the current ,a ctive configuration file
Router(config) #show startup-config = displays the saved confiuration file which will be loaded if the device is restarted
Router(config) #write = saves the configuration
Router(config) # write memory = saves the configuration

### Ethernet Frame

- The minimum size for an Ethernet frame (Header + Payload + trailer)is 64 bytes.
- 64bytes -18(header + trailer size )= 46 bytes
- therefore the minimum payload is less than 46 bytes .
- if the payload is less than 46 bytes , padding bytes are added.

### Mac Address

6 byte (48) bit physical address that is assigned to the device when the device is made. AKA burned in address.
The mac address is globally unique.
The first 3 byte are the OUI (organizational unique identifier) which is assigned to the company making the device.

**Note:-**

Unicast Frame
The frame that is destined for only one single target.
Unknown unicast frame = flood to all other interfaces except the one which sent it.

**Note:-**

Dynamic or dynamically learned mac address are removed. The mac address are removed after five minutes of inactivity

### ARP

- ARP stands for 'Address Resolution Protocol'
- ARp is used to discover the layer 2 address (MAC address) of a known IP address
- ARP request is unknown unicast frame
- ARP request is unicast frame

### Network Layer

- Provides connectivity between different end hosts on different networks (i.e outside the network ).
- Provides logical addressing
- Provides path selection between sources and destination addresses
- Routers operate at Layer 3

### IPv4 Addressing

The IP address is written in dotted decimal.It is splitted into four octets and then written in dotted decimal for our easiness. Since IP address is of 32 bits from which first 24 bits specify network portion and remaining 8 bytes specify hosts address.
So 192.168.1.254/24 means 192.168.1 represent network portion and 254 reperesent host portion.

### Loopback Address

- Address range 127.0.0.0-127.255.255.255.
- Used to test the network stack on the local device.

### TTL(Time to Live)

In practice, indicates a 'hopcount ': each packet arrives at arouter,the router decreses TTL by 1.

- Value of 6 :TCP
- Value of 17 :UDP
- Value of 1 :ICMP
- Value of 89 :OCPF(dynamic routing protocol)

### Routing Fundamentals

Routing is the process that routers use to determine the path that IP packets should take over a network to reach theri destination.

- WHen routers receive packets, they look in the routing table to find the best route to forward that packet.
- Routers store routes to all of their known destinations ina routing table.

A route tells the router : to send a packet to destination X you should send the packet to next hop Y
or if the setination is directly connected to the touter ,send the packet directly to the destination
or if the destination is the routers own IP address receive the packet dor yourself(dont forward it) When you configure an IP address on an interface and enable the interface , two routes are automatically added to the routing table Connected route A route to the network connected to the internet
i.e if the interface' IP is 192.168.1.1/24 the route will be to 192.168.1.0/24
Tells the router "To send a packet to a destination in this network, send it out of the interface specified in the route
Local route A route to the exact IP address configured in the interface. If the router receive a packet and it doesnot have a route that matches the packet destination it will drop the packet.

### The Life of a packet

The source is 192.168.1.1 pc1's ip address and the destination is 192.168.4.1 pc4's ip address. because pc1's ip address is in the range of 192.168.1.1 so it notices that the the ip address 192.168.4.1 is in a different network so it knows that it needs to send the packet to its default gateway which is R1. SO it is necessary for ARP request to find the mac of destination, So it will send a broadcast to all the interfaces of the switch S1 except the one that sent.

# Chapter 2

# Subnetting

## 2.1 CIDR(Classless Inter-Domain Routing)

IANA assignes IPv4 addresses/network to company based on their size. Howerver, this leads to wastage of IPs.

## 2.2 Subnet Mask

# Chapter 3

# VLANS

## 3.1 Part 1

VLANs are configured on switches on aper interface basis.Thwy logically seprate end hosts at Layer 2.
Switches donot forward teaffic directly betwenn hosts in different VLANS as well as in same VLANS.
Lots of unnecessary brodcast traffic can reduce network performance.
Even within the same office you want to limit who has access to what. YOu can apply security policies on a router/firewall. because this is one LAN ,PCs can reach each other directly without traffic passing through the router.
So, even if you configure security policies,they won't have any effect A switch willnot forward traffic between VLANs, including brodcast/unknown unicast traffic.
Vlans 1,1002-1005 exists by default and cannot be deleted.
Although we seprated the three departments into three subnets (layer3) they are still in the same broadcast domain (Layer 2).
The router is used to route between VLANs. The switch doesnot perfoem inter VLAN routing.
VLANs logically separate end hosts at Layer 2.
An access port is a switchport which belongs to a single VLAN and usually connects to end hosts like PCs.It gives endhost access to internet.
Switch Ports which carry multiple VLANs are called trunk ports .

- interface range g2/0 -2
- switchport mode access
- switchport access vlan 20
- Access VLAN doesnot exist. Creating Vlan 10
- interface range g3/0 -3
- switchport mode access
- switchport access vlan 30
- Access VLAN doesnot exist. Creating Vlan 10

## 3.2 Part 2

**What is trunk ports or Tagged Port?**
The Switches will tag all frames that they send over a trunk link. This allow the receiving seitch to know which VLAn the frame beelongs to. IEEE 802.1Q is an industry standard protocol created by IEEE. The 802.1Q tag is inserted between the source and type/length fields of the ethernet header which is of length 32 bits. VID Vlan id identies the vlan the frame belongs to . 12 bits in length = 4096 total vlans range of 0-4095 Vlan 0 and 4095 are reserved and can't be used.
The range of VLANs (1-4094) is divided into two sections

- Normal VLANs 1-1005
- Extended VLANs 1005-4094

A standard layer 2 switch wiil only forward traffic in the same VLAN. IT willnot forward traffics betwenn VLANs.