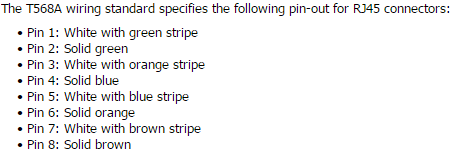
IDF- intermediate distribution frame is the demarc on another floor

3 2 1 2 4

BGOB



**EMI-** Electromagnetic interference is a field that is emitted from a wire.

**Drain wire**- a wire with no coating that absorbs EMI found in (CAT 6) and (CAT 7)

**Copper cables**- 100m or less otherwise signal is too bad to communicate. Heat also affects

**Repeater**- amplifies the cable so it can be longer than 100meters

**Angled Physical contact polish**- slight slanted fiber optic

**Plenum**- non toxic gas when burned.

**First pair of wiring**- sends and receives TX (transmit) and RX (receive)

**Category 5**- more twists per inch than CAT 3 to reduce the cross-talk and support higher data rates.

**BNC**- older 10Base2 Ethernet

**MT-RJ** - they can use multimode fiber optic cable, they use a metal guide pins to ensure accurate alignment.

**Connect two wiring closet**- 25 pair and Horizontal cross connect

**CAT 6**- solid plastic core

**F-Type-** broad band that uses coaxial cables

**Coaxial Cables**- uses two concentric metallic conductors, has conductor made from copper in the center, and the ends of the cable must be terminated.

**LC**- use a housing latch system similar to an RJ-45, and half the size of standard connectors.

**T1 WAN service**- RJ48c used in a WAN network

Fiber Optic that includes both cables in 1 connector- **LC and MT-RJ**

**Insertion loss**- loss of signal right away and back reflection, better polish better

**PC (physical Contact)**- signal mode fiber

**SPC and UPC (super Physical Contact) & ( Ultra Physical Contact)**- higher polish and signal and multi mode.

**APC ( Angled Physical Contact)**- 8 degree angle and uses the highest polish to reduce back reflection.

**Fiber optic**- the center of the cable is fragile and can break.

**Routers**- links multiple networks and directs traffic

**Layer 1 (Application)**- OSI layer where media converter operate

**Hubs & Repeater**- regenerates a signal out all connected ports without examining frames.

**Switches and Bridges**- frames enter a port the source MAC address is copied from the frame header.

**Bridge**- selects certain information and allows it depending what the MAC address is

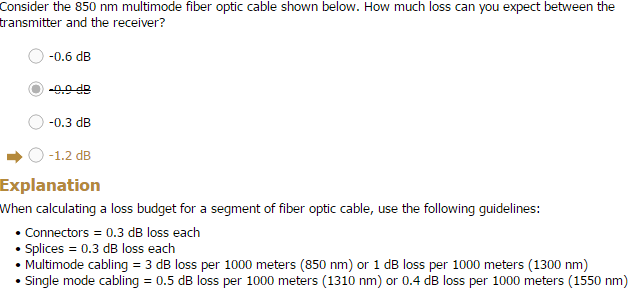
**MAC address**- typically represented by hexadecimal number and 48-bit address

**Modems**- demodulates analog data from telephone network into digital PC data &

Modulates digital data from the PC into analog data and transmits it on telephone network.

**Transceiver**- Sends signal from the computer onto a network.

**HUB**- does NOT segment the network, sends the signal to every port and does not examine



**SFP**- used to plug switch and routers to modify the media type used, can convert RJ-45 to fiber

**Media Converter**- make two cables compatible like a ethernet to a fiber.

**MAC address**- uniquely identifies the device (data link)

**ARP**- to figure the MAC address from the IP address.

**WAP**- wireless internet hub sent to all devices.

**MAC address filtering**- will only allow certain devices that have that MAC address access that information.

FF-FF-FF-FF-FF-FF- sends to all devices (broadcast)

**Switch**- It connects multiple cable segments and forwards frames to the appropriate segment.

**Repeater and HUB**- regenerates a signal without examining the frames.

**Switches & bridges learn where devices by**- source when the MAC address is copied from the header.

On a 8 port switch If port 1 sends a frame addressed to a unknown device it sends it to port 2-8.

**HUB**- does **NOT** segment the network.

**Layer3**- router, firewall (traffic data), layer three switch (IP address same)(MAC address changes) -SUB net

**Collision of data**- two computers send information to the same computer at the same time, which corrupts the data. BUS topology

**Switches**- NO collisions and can send multiple data at the same time unlike HUBs.

**CSMA/CD**- media access control method of all ethernet networks, 10BaseT & 1000BaseT

Devices listen and determine when the media is free.

**Ethernet “Speed” *BASE* “Twisted”**- cat 3(T), cat 5 (Tx), cat 5e or cat 6 (Tx)(Cx), cat 6a

**Fiber “Speed” *BASE* “*S*hort, *L*ong, *E*xtended”**- **FL** (MMF 1000-2000 m),

**Fx** (MMF 412m), **Sx** (MMF 220- 550 m), **Lx** (SMF 10km), **SR SW** (MMF 300-400 m),

**LR LW** (SMF 10km), **ER EW** (SMF 40km)

1024 Hosts per network

**10G BASE LW**- is used by SONET

**Crossover**- when connecting two computers

**Straight through**- when connecting two computers with a **switch,** and when one switch is connected to the uplink and the other is connected to the receiver port.

**Cross over**- when connecting two switches with the uplink port

**Cross over-** when connecting two routers or router to switch

**Uplink**- is Crossover unless connected to a standard port on another switch.

**RS-232**- used in a rollover cable where serial on one end and RJ-45 on the other.

**Link light**- Green (10GB) yellow (100MB) Red not working ( bad cables or wrong type)

**Activity light**- flashes when data is being transferred, if solid the network card is jabbering

**Collision light**- should be off, when collision is detected it lights up and usually common if there isn't a switch and they used a HUB instead. Two devices try to transfer data at the same time.

**Physical Bus**- one cable connecting to a workstation breaks no devices will be able to communication.

**TDR**- Measure the length of a cable & Identify the location of a fault on a cable.

**Certifier**- if a device is only working at 100 Mbps on a 1000BaseT

**Smart Jack**- to test if the line connecting to your building is working properly.

**Replace order**- Cable, Network card, switch/hub (all devices should not work).

**EMI-** florescent lights.

**Switch not working**- Failed patch cable between the client system and the wall jack

**Crosstalk-** can reduce your Gmps

**Attenuation-** a loss of signal strength from one end of the cable to the other. Longer the cable tyhe more attenuation.

**Echo-** occurs when you connect cables and devices that have different impedance rating,

like a 75 ohms with a 50 ohms.

**Multimeter-** measures the voltage, amps, and ohms

FX- 412 meters

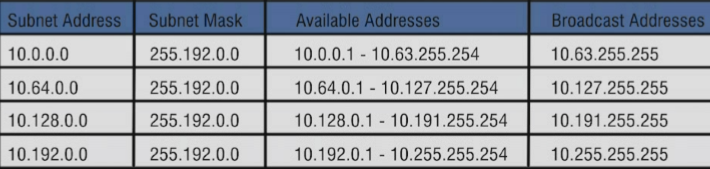
1km or greater- Signal and 10G BASE LR

Standard Fiber- FX, LX

1000mbps min- Cat5

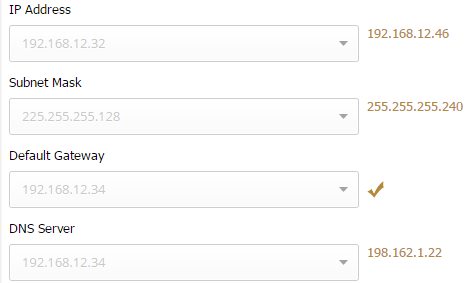
Use twisted pair with Fiber- CX

Subnet- 00000000 (0), 10000000 (128),11000000 (192), 11100000 (224), 11110000 (240), 11111000 (244),11111100 (252),11111110 (254),11111111 (255)

Static IP assign- each computer needs to be given a: IP address, Subnet mask, Default gateway, and DNS server.

DHCP- auto gives a IP address to each device, provides a central point of administration for IP address management in your organization. Weakness some devices don't really support DHCP

IANA- responsible for allocating IP addresses used on the internet.





**Chapter 5**

APIPA- auto assigns itself a IP address if the DHCP server is down

IPconfig- the client system is unable to reach the DHCP server & the client system is configured to use DHCP

DHCP server lease by Default Monday Morning- renew Wednesday morning.

True about DHCP- can deliver other configurations information in addition to IP & DHCP server assigns addresses to request hosts.

Prevent duplicate IP addresses- install a DHCP server on the network & Auto Private IP Addressing.

DHCP- auto config IP, must configure a DHCP server with an option that delivers the IP address of the DNS server.

The clients must be configured to obtain IP addresses from the DHCP

DHCP- makes sure that every IP address is different.

Config a DHCP relay agent- find the specific server network interface the agent listens on for DHCP messages

If you want to use a DHCP relay agent- **Routing and Remote Access**

Forward DHCP frames to the appropriate subnet- **ip helper-address**

To enable hosts to find a IP address- DNS Server

DNS- allows you to find a IP address from a logical name

PTR- points an IP address to a host name

MX- Identifies servers that can be used to deliver mail

CNAME- gives alternative names to hosts that already have a host

A- IPv4

AAAA- IPv6

Dynamic DNS- Auto creates and deletes hosts recorded when a IP address lease is created

Cause of the Dynamic hosts- IPCONFIG /RELEASE or DHCP server renews a IP lease

Teredo- Host to host protocol: dual stack hosts, Works through NAT, and Tunnel endpoint configured on hosts.

Miredo- Host to Host on Linux

IPv6- 141:0:0:0:15:0:0:1 or 6858:1232:7004:44A6:5511:B879:AC68:8679

The entire 128-bit address and other information is statically assigned to the host

- **Static Full**

The Prefix is statically assigned and the interface ID is derived from the MAC address

- **Static Partial**

Clients automatically generated the interface ID and learn the Subnet prefix and the default gateway through the NDP neighbor discovery protocol

- **Stateless Autoconfig**

Provides each client with a IP address default gateway and other IP configuration info

- **Stateful DHCPv6**

Supplies the client with DNS server IP address only, does not provide the client with an IP address and won't track the status of each client

- **Stateless DHCPv6**

4-to-6 tunneling - send IPv4 to IPv6

Unicast- sends the same message to each device, a IP address of 198.162.12.254

Broadcast- sends a signal message to every device

Multicast- always starts with 01-00-5E

IGMP- way to inform a router that it wants to receive a specific multicast frame.

Multicast- IP 232.111.255.250

unavailable DHCP server- will not have a default gateway

Ipconfig- windows

Ifconfig- Linux

Inncorect subnet mask- IP 192.168.1.102 should be 255.255.255.0 NOT 255.255.0.0

Gateway- always has to be correct to the IP address

IP address- always correspond to the Gateway NOT to the DNS

DNS 192.168.2.20- IP address and Gateway HAVE to be 192.168.**1**.2 or 3

Ping- to check the connectivity between sources

Netstat- checks the TCP connection

Nbtstat- troubleshoots NetBios name problems, and what about them.

Nbtstat -c --shows the resolved NetBIOS name cache for the computer, names 2 IP addresses.

Netstat -s -- displays network activity statistic for TCP UDP and IP

Traceroute- linux utility that allows you to track the route of a packer as it traverses the network

Tracert- is the utility for windows

ARP- looks up the arp cache

Arp -a -- shows the current entries in the computer's ARP cache

Netstat -r -- shows the computer route table

Netstat -a -- shows all active listening ports

Lookup- nslookup and dig -x

Nslookup- to troubleshoot a problem on your own device

Ifconfig and ipconfig- view the DNS server addresses

Unicast- 198.162.12.254 /24

VLSM and Classless- make CIDR possible

172.17.128.0 - 172.17.0.0 -- subnet mask 255.255.192.0

Traceroute- Linux utility to track the route of a packet

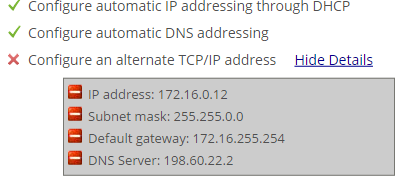
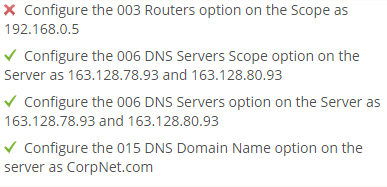
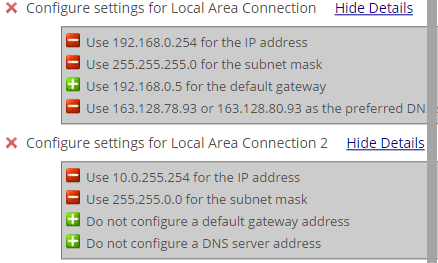
Class B 166.70.0.0-- 166.70.255.254

192.160.99.110/16 -- 255.255.0.0

ARP- TCP/IP utility gives you; Interface, Internet address physical address type

NOT valid IPs- **257**.0.122.55 , 45.22.156**.256** , 145.8.**260**.7

Subnets- divide an IP network address into multiple networks addresses

Labs- 

**Chapter 6**

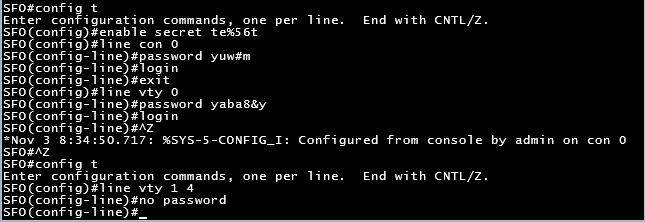
Con t- to configure a password after in enable mode

Line 0

Password \_\_\_\_\_\_

login

Enable secret \_Password\_

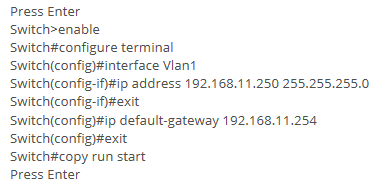


Copy run start- to save your work

Putty won't work- if the baud is 4600 or flow control = RTS/CTS

If the router is config with login, NO PASSWORD- access is denied

Command- Show ip interface



Show interface status- Fa0/?

Int fa0/1

Int fa0/3

Switchport access vlan 12

No shutdown

Reasons to config VLAN- increased security, Increased number of broadcast domain

Benefits creating Vlan- you can create multiple Broadcast domains

Broadcast domain are each switch- 2

Vlan affect broadcast traffic within an internetwork- **devices on the same VLAN have the same subnet address, and broadcast traffic is transmitted only within a VLAN.**

Using multiple VLANs on a signal switch- **the number of broadcast domains increase, the number of collision domains remain the same**

Virtual LAN can be created using- **Switch**

Can reduce collisions domains by using- **Switch**

**VLAN concept-** Devices on the same network logically group as if they were on separate networks.

**Switch port-** to identify VLAN membership of a device

**Routing-** what to Configure so two devices can communicate

**VLAN**- isolate the network logically

**(TRUNK)**

**Conf t**

**Int range fa0/?, gi0/1-?**

**Switchport mode trunk**

**No switchport access vlan**

**Int range fa0/1-?**

**Switchport mode access**

**^z**

**Copy run start**

**Enter**

**Certain VLAN-** Switchport trunk native vlan 10 (or whatever VLAN)

Trunking- allows switches to pass VLAN traffic between switches and communicate

Trunk port- is a member of all VLAN defined on a switch

Computer A sends a normal frame, the first switch appends a Vlan ID to the frame. The second switch removes the VLAN ID before forwarding it to computer B.

VLAN ID- switches append a VLAN ID to the header of each frame to identify the virtual network to which it belong

**ROOT BRIDGE**

Conf t

Spanning-tree vlan 1 priority 4096

Exit

Running-config startup-config

**STP**

Switch B

32769:000e.8411.68c0

Forwarding

Blocking

Root

Next hop- first router in the path to the destination

Static- manually configured

Routers perform- route data based on logical network addresses, and maintain information about paths through an internetwork

