CCNA (200-120) Quick notes before exam

Make sure you know everything mentioned here before attending the CCNA 200-120 exam.For complete and detailed notes click here

Points to Remember

- Only router can break up broadcast domains
- Both router and switch can break up collision domains
- Routing occur in internet layer in DOD TCP/IP reference model
- PPP perform in layer 2
- FTP belongs to Application layer
- When Global command that is set once and affects the entire router
- LCP PPP sub protocol negotiates authentication options
- PPP and DSL are valid WAN connectivity methods
- Datalink layer of the OSI model uses RSTP to prevent loops
- When using the term “frame” we can easily recognize it belongs to the Data Link layer
- When using the term “Packet” we can easily recognize it belongs to the Network layer
- Show version command reveals the last method used to powercycle a router
- show ip interface command is used to verify which interfaces are affected by the ACL
- Both routers must use the same password for CHAP to authentication

Basic notes

To check the connectivity between a host and a destination (through some networks) we can use both “tracert” and “ping” commands. But the difference between these 2 commands is the “tracert” command can display a list of near-side router interfaces in the path between the source and the destination. The “traceroute” command has the same function of the “tracert” command but it is used on Cisco routers only, not on a PC

When powered on, the router first checks its hardware via Power-On Self Test (POST). Then it checks the configuration register to identify where to load the IOS image from. In the output above we learn that the Configuration register value is 0×2102 so the router will try to boot the system image from Flash memory first.

The last known good router will try to inform you that the destination cannot be reached (with a Destination Unreachable message type) so from that information you can learn how far your packets can travel to and where the problem is.

Each interface on a router must be in a different network. If two interfaces are in the same network, the router will not accept it and show error when the administrator assigns it.
When no startup configuration file is found in NVRAM, the System Configuration Dialog will appear to ask if we want to enter the initial configuration dialog or not.

Ping command can be used from a PC to verify the connectivity between hosts that connect through a switch in the same LAN

Organizational Unique Identifier (OUI) is the first 24 bits of a MAC address for a network device, which indicates the specific vendor for that device as assigned by the Institute of Electrical and Electronics Engineers, Incorporated (IEEE). This identifier uniquely identifies a vendor, manufacturer, or an organization.

The Maximum Transmission Unit (MTU) defines the maximum Layer 3 packet (in bytes) that the layer can pass onwards.

Modern Ethernet networks built with switches and full-duplex connections no longer utilize CSMA/CD. CSMA/CD is only used in old switches

The Network layer is responsible for network addressing and routing through the internetwork. So a ping fails, you may have an issue with the Network layer.Packets are created when the network layer adds Layer 3 addresses and control information to a segment.

The transport layer divides a data stream into segments and may add reliability and flow control information.

Application layer in the OSI reference model is responsible for determining the availability of the receiving program and checking to see if enough resources exist for that communication

When upgrading new version of the IOS we need to copy the IOS to the Flash so first we have to check if the Flash has enough memory or not. Also running the new IOS may require more RAM than the older one so we should check the available RAM too. We can check both with the "**show version**" command.

When will devices transmit in a Ethernet network ?
Ethernet network is a shared environment so all devices have the right to access to the medium. If more than one device transmits simultaneously, the signals collide and cannot reach the destination. If a device detects another device is sending, it will wait for a specified amount of time before attempting to transmit. When there is no traffic detected, a device will transmit its message. While this transmission is

occurring, the device continues to listen for traffic or collisions on the LAN. After the message is sent, the device returns to its default listening mode.

Two purposes does the Ethernet protocol use physical addresses

Physical addresses or MAC addresses are used to identify devices at layer 2

To allow communication between different devices on the same network

The following locations can be configured as a source for the IOS image:

Flash (the default location)
TFTP server
ROM (used if no other source is found)

What is the difference between a CSU/DSU and a modem?

A CSU/DSU converts digital signals from a router to a leased line; a modem converts digital signals from a router to a phone line.

Router boot process:

The Power-On Self Test (POST) checks the router's hardware. When the POST completes successfully, the System OK LED indicator comes on.
The router checks the configuration register to identify where to load the IOS image from. A setting of 0×2102 means that the router will use information in the startup-config file to locate the IOS image. If the startup-config file is missing or does not specify a location, it will check the following locations for the IOS image:
1. Flash (the default location)
2. TFTP server
3. ROM (used if no other source is found)

Basic IOS notes

service password-encryption command, all the (current and future) passwords are encrypted. This command is primarily useful for keeping unauthorized individuals from viewing your password in your configuration file.

How to secure the virtual terminal interfaces on a router?

Configure a virtual terminal password and login process.

Enter an access list and apply it to the virtual terminal interfaces using the access-class command.

Commands

Router(config)# service password-encryption command encrypts all plaintext passwords.

Router (config-if)# ppp authentication chap pap command is used to enable CHAP authentication with PAP as the fallback method on a serial interface

Router#show vlan command only displays access ports, the trunk ports are not showed in this command

"**Show frame-relay lmi**" command allows you to verify the encapsulation type (CISCO or IETF) for a frame relay link

show ip ospf database - command is used to display the collection of OSPF link states

Below lists popular modes in Cisco switch/router:

Router>	User mode
Router#	Privileged mode
Router(config)#	Configuration mode
Router(config-if)#	Interface level (within configuration mode)
Router(config-router)#	Routing engine level (within configuration mode)
Router(config-line)#	Line level (vty, tty, async) within configuration mode

Trunking Notes:

Valid Vlan Trunk Modes

Desirable
Auto
ON

Dynamic Trunking Protocol (DTP) is a Cisco proprietary protocol for negotiating trunking on a link between two devices and for negotiating the type of trunking encapsulation (802.1Q) to be used.

IEEE 802.1Q is the networking standard that supports Virtual LANs (VLANs) on an Ethernet network. It is a protocol that allows VLANs to communicate with one another using a router. 802.1Q trunks support tagged and untagged frames.If a switch receives untagged frames on a trunk port, it believes that frame is a part of the native VLAN. Also, frames from a native VLAN are not tagged when exiting the switch via a trunk port.

Three elements must be used when you configure a router interface for vlan trunking?

one IP network or subnetwork for each subinterface
subinterface encapsulation identifiers that match vlan tags
one subinterface per vlan

Cisco switches support two trunking protocols 802.1q & ISL. 802.1q is an open

standard and is thus compatible between most vendors' equipment while Inter-Switch Link (ISL) is Cisco proprietary.

Click here for detailed VTP notes

STP Notes

Only non-root bridge can have root port.

The path cost to the root bridge is the most important value to determine which port will become the root port on each non-root switch. In particular, the port with lowest cost to the root bridge will become root port (on non-root switch).

Per VLAN Spanning Tree (PVST) maintains a spanning tree instance for each VLAN configured in the network. It means a switch can be the root bridge of a VLAN while another switch can be the root bridge of other VLANs in a common topology. For example, Switch 1 can be the root bridge for Voice data while Switch 2 can be the root bridge for Video data. If designed correctly, it can optimize the network traffic.

If we connect two switches via 2 or more links and do not enable STP on these switches then a loop (which creates multiple copies of the same unicast frame) will occur. It is an example of an improperly implemented redundant topology.

PVST+ is based on IEEE802.1D Spanning Tree Protocol (STP). But PVST+ has only 3 port states (discarding, learning and forwarding) while STP has 5 port states (blocking, listening, learning, forwarding and disabled). So discarding is a new port state in PVST+.

RSTP only has 3 port states that are discarding, learning and forwarding. When RSTP has converged there are only 2 port states left: discarding and forwarding

A BPDU is superior than another if it has:
1. A lower Root Bridge ID
2. A lower path cost to the Root
3. A lower Sending Bridge ID
4. A lower Sending Port ID

Click here for detailed STP Notes

ACL Notes

The standard access lists are ranged from 1 to 99 and from 1300 to 1999

We can have only 1 access list per protocol, per direction and per interface. It means:
We can not have 2 inbound access lists on an interface
We can have 1 inbound and 1 outbound access list on an interface

We can use a dynamic access list to authenticate a remote user with a specific username and password. The authentication process is done by the router or a central access server such as a TACACS+ or RADIUS server.

Click here for detailed ACL notes

NAT Notes

With static NAT, translations exist in the NAT translation table as soon as you configure static NAT command(s), and they remain in the translation table until you delete the static NAT command(s).Because static NAT translations are always present in the NAT table so outside hosts can initiate the connection without being dropped

With dynamic NAT, translations do not exist in the NAT table until the router receives traffic that requires translation. Dynamic translations have a timeout period after which they are purged from the translation table.

By not reveal the internal Ip addresses, NAT adds some security to the inside network

By allocating specific public IP addresses to inside hosts, NAT eliminates the need to re-address the inside hosts

VLAN Notes

A “native VLAN mismatch” error will appear by CDP if there is a native VLAN mismatch on an 802.1Q link. “VLAN mismatch” can cause traffic from one vlan to leak into another vlan.

VLANs allow to group users by function, not by location or geography
VLANs help minimize the incorrect configuration of VLANs so it enhances the security of the network

VLANs increase the number of broadcast domains while decreasing the size of the broadcast domains which increase the utilization of the links. It is also a big advantage of VLAN

Advantages of VLANs
VLANs establish broadcast domains in switched networks.

VLANs allow access to network services based on department, not physical location.
VLANs can greatly simplify adding, moving, or changing hosts on the network.

For 802.1q encapsulation, the native VLAN must matched at both side; otherwise the link will not work.

VLAN 1 is the default VLAN on Cisco switch. It always exists and can not be added, modified or removed.
VLANs 1002-1005 are default VLANs for FDDI & Token Ring and they can't be deleted or used for Ethernet.

Click here for detailed VLAN notes

Frame Relay Notes

To configure subinterface for Frame Relay, first we have to remove the IP address from the physical interface and choose a Frame Relay encapsulation.

The PVC STATUS displays the status of the PVC. The DCE device creates and sends the report to the DTE devices. There are 4 statuses:
ACTIVE: the PVC is operational and can transmit data
INACTIVE: the connection from the local router to the switch is working, but the connection to the remote router is not available
DELETED: the PVC is not present and no LMI information is being received from the Frame Relay switch
STATIC: the Local Management Interface (LMI) mechanism on the interface is disabled (by using the "no keepalive" command). This status is rarely seen so it is ignored in some books.

DLCI: DLCI stands for Data Link Connection Identifier. DLCI values are used on Frame Relay interfaces to distinguish between different virtual circuits. DLCIs have local significance because the identifier references the point between the local router and the local Frame Relay switch to which the DLCI is connected.

Committed information rate (CIR): The minimum guaranteed data transfer rate agreed to by the Frame Relay switch. Frames that are sent in excess of the CIR are marked as discard eligible (DE) which means they can be dropped if the congestion occurs within the Frame Relay network.
Note: In the Frame Relay frame format, there is a bit called Discard eligible (DE) bit that is used to identify frames that are first to be dropped when the CIR is exceeded.

Local Management Interface (LMI) is a signalling standard protocol used between your router (DTE) and the first Frame Relay switch

Inverse ARP is a technique by which dynamic mappings are constructed in a network, allowing a device such as a router to locate the logical network address and associate it with a permanent virtual circuit (PVC).

IP Routing Notes

When one route is advertised by more than one routing protocol, the router will choose to use the routing protocol which has lowest Administrative Distance.
Routers decrement the TTL by 1 every time they forward a packet; if a router decrements the TTL to 0, it throws away the packet. This prevents packets from rotating forever

Remember these rules:
The IP addresses (of source and destination) of a packet never change during the transportation through the network. For example if PC-A wants to send a packet to PC-Z then the source and destination IP addresses of the packet will be the IP addresses of PC-A and PC-Z no matter how many devices they go through.
The MAC addresses, conversely, will change while passing the devices. The source MAC address is the address of the last sender and the destination MAC address is the address of the next device.

The simple syntax of static route:
ip route destination-network-address subnet-mask {next-hop-IP-address | exit-interface}

Explanation
destination-network-address: destination network address of the remote network
subnet mask: subnet mask of the destination network
next-hop-IP-address: the IP address of the receiving interface on the next-hop router
exit-interface: the local interface of this router where the packets will go out

DHCP Notes

Network or sub network IP address and broadcast address should never be assignable to hosts. When try to assign these addresses to hosts, you will receive an error message saying that they can't be assignable.

An address conflict occurs when two hosts use the same IP address. During address assignment, DHCP checks for conflicts using ping and gratuitous ARP. If a conflict is detected, the address is removed from the pool. The address will not be assigned until the administrator resolves the conflict.

OSPF Notes

The highest IP address of all loopback interfaces will be chosen as Router-ID
110 is the default administrative distance of OSPF

The default number of equal-cost paths that can be placed into the routing of a Cisco OSPF router is 4. We can change this default value by using "maximum-paths" command:
Router(config-router)#maximum-paths 2
Note: Cisco routers support up to 6 equal-cost paths

Characteristics of a link-state routing protocol
Provides common view of entire topology
Calculates shortest path
Utilizes event-triggered updates

Describe the routing protocol OSPF
It supports VLSM.
It confines network instability to one area of the network.
It allows extensive control of routing updates

Hierarchical design of OSPF (basically means that you can separate the larger internetwork into smaller internetworks called areas) helps us create a network with all features listed like (decrease routing overhead, speed up convergence; confine network instability to single areas of the network).

Hello packets and LSAs from other routers are used by router running a link-state protocol to build and maintain its topological database

To form an adjacency (become neighbour), router A & B must have the same Hello interval, Dead interval and AREA number.

Click here for detailed OSPF notes

EIGRP Notes

- AD of EIGRP Internal Route is 90
- AD of EIGRP external Route is 170
- AD of EIGRP summary Route is 5

Passive Interface: In EIGRP (and OSPF) the passive interface command stops sending outgoing hello packets, hence the router cannot form any neighbor relationship via the passive interface. This behavior stops both outgoing and incoming routing updates

Feasible successor is a route whose Advertised Distance is less than the Feasible Distance of the current best path. A feasible successor is a backup route, which is not stored in the routing table but stored in the topology table.

EIGRP stub advertises summary and directly connected routes. EIGRP stub routing feature improves network stability, reduce resources utilization and simplifies stub router configuration. Any neighbor that receives a packet informing it of the stub status will not query the stub router for any routes.EIGRP stub configuration command increases scalability by limiting the
EIGRP query range

Active State: When a route (current successor) goes down, the router first checks its topology table for a feasible successor but it can't find one. So it goes active on the that route to find a new successor by sending queries out to its neighbors requesting a path to the lost route.

Click here for detailed EIGRP Notes

Security Notes

We only enable PortFast feature on access ports (ports connected to end stations). But if someone does not know he can accidentally plug that port to another switch and a loop may occur when BPDUs are being transmitted and received on these ports.
With BPDU Guard, when a PortFast receives a BPDU, it will be shut down to prevent a loop

We can verify whether port security has been configured by using the "show running-config" or "show port-security interface" for more detail

Port security is only used on access port (which connects to hosts) so we need to set that port to "access" mode, then we need to specify the maximum number of hosts which are allowed to connect to this port.
Note: If we want to allow a fixed MAC address to connect, use the "switchport port-security mac-address " command.

One of the most widely deployed network security technologies today is IPsec over VPNs. It provides high levels of security through encryption and authentication, protecting data from unauthorized access.

IPV6 Notes

Features of the IPv6 protocol
Autoconfiguration
No broadcasts

Plug-and-play
A single interface may be assigned multiple IPV6 addresses of any type.
Every IPV6 interface contains at least one loopback address.

With IPv6, devices can build a link-local address automatically. But notice this address is only used for communications within the local subnetwork, routers do not forward these addresses.
Below is the list of common kinds of IPv6 addresses:

Loopback address	::1
Link-local address	FE80::/10
Site-local address	FEC0::/10
Global address	2000::/3
Multicast address	FF00::/8

Click here for Detailed IPv6 notes

SNMP protocol can cause overload on a CPU of a managed device
TRAP and INFORM are the alert message generated by SNMP agents
In a GLBP network, AVG is responsible for the arp request

Components of SNMP
MIB
SNMP Manager
SNMP Agent

3 features are added in SNMPv3 over SNMPv2
Message Integrity
Authentication
Encryption

Popular destinations for syslog messages to be saved
The logging buffer .RAM
The console terminal
Syslog server

The benefit of using Netflow
Network, Application & User Monitoring
Security Analysis
Accounting/Billing

3 things that the Netflow uses to consider the traffic to be in a same flow
IP address

Port numbers
L3 protocol type