Notes for Cisco Routing and Switching1 – Introduction to Networks
Chapter 5. Ethernet

1. A MAC address is composed of 6 bytes. The first 3 bytes are used for vendor identification and the last 3 bytes must be assigned a unique value within the same OUI. MAC addresses are implemented in hardware. A NIC needs a MAC address to communicate over the LAN. The IEEE regulates the MAC addresses.

2. Contention-based methods are nondeterministic and do not have the overhead that is found with controlled access methods. They do not track the turns because devices do not take turns to access the media. Contention-based methods do not scale well under heavy use.

3. Logical link control is implemented in software and enables the data link layer to communicate with the upper layers of the protocol suite. The NIC driver software interacts directly with the hardware on the NIC to pass the data between the MAC sublayer and the physical media. Logical link control is specified in the IEEE 802.2 standard. IEEE 802.3 is a suite of standards that define the different Ethernet types. The MAC (Media Access Control) sublayer is responsible for the placement and retrieval of frames on and off the media.

4. The multicast MAC address is a special value that begins with 01-00-5E in hexadecimal. The value ends by converting the lower 23 bits of the IP multicast group address into the remaining 6 hexadecimal characters of the Ethernet address. The remaining bit in the MAC address is always a "0".
   In this case:
   224 (decimal) => 01-00-5E
   139 (decimal) = 10001011 (binary) ==> (23 bits) = 0001011 (binary) = 0B (hexadecimal)
   34 (decimal) = 00100010 (binary) = 22 (hexadecimal)
   56 (decimal) = 00111000 (binary) = 38 (hexadecimal)
   Putting all together: 01:00:5E:0B:22:38

5. Destination and source MAC addresses change at every router hop if the entire path is Ethernet based. The destination IP address remains unchanged along the path unless Network Address Translation is active.

6. When a node encapsulates a data packet into a frame, it needs the destination MAC address. First it determines if the destination device is on the local network or on a remote network. Then it checks the ARP table (not the MAC table) to see if a pair of IP address and MAC address exists for either the destination IP address (if the destination host is on the local network) or the default gateway IP address (if the destination host is on a remote network). If the match does not exist, it generates an ARP broadcast to seek the IP address to MAC address resolution. Because the destination MAC address is unknown, the ARP request is broadcast with the MAC address FFFF.FFFF.FFFF. Either the destination device or the default gateway will respond with its MAC address, which enables the sending node to assemble the frame. If no device responds to the ARP request, then the originating node will discard the packet because a frame cannot be created.

7. When a network device wants to communicate with another device on the same network, it sends a broadcast ARP request. In this case, the request will contain the IP address of PC2. The destination device (PC2) sends an ARP reply with its MAC address.
8. When sending a packet to a remote destination, a host will need to send the packet to a gateway on the local subnet. Because the gateway will be the Layer 2 destination for the frame on this LAN segment, the destination MAC address must be the address of the gateway. If the host does not

already have this address in its ARP cache, it must send an ARP request for the address of the gateway.

9. Large numbers of ARP broadcast messages could cause momentary data communications delays. Network attackers could manipulate MAC address and IP address mappings in ARP messages with the intent to intercept network traffic. ARP requests and replies cause entries to be made into the ARP table, not the MAC address table. ARP table overflows are very unlikely. Manually configuring static ARP associations is a way to prevent, not facilitate, ARP poisoning and MAC address spoofing. Multiple ARP replies resulting in the switch MAC address table containing entries that match the MAC addresses of connected nodes and are associated with the relevant switch port are required for normal switch frame forwarding operations. It is not an ARP caused network problem.

10. Modern switches can negotiate to work in full-duplex mode if both switches are capable. They will negotiate to work using the fastest possible speed and the auto-MDIX feature is enabled by default, so a cable change is not needed.

11. With shared memory buffering, the number of frames stored in the buffer is restricted only by the of the entire memory buffer and not limited to a single port buffer. This permits larger frames to be transmitted with fewer dropped frames. This is important to asymmetric switching, which applies to this scenario, where frames are being exchanged between ports of different rates. With port-based memory buffering, frames are stored in queues that are linked to specific incoming and outgoing ports making it possible for a single frame to delay the transmission of all the frames in memory because of a busy destination port. Level 1 cache is memory used in a CPU. Fixed configuration refers to the port arrangement in switch hardware.

12. When another switch or a hub is connected to a switch port then frames could be received from the multiple nodes connected to the other switch or the hub. This will result in the MAC address for each of those multiple nodes to be recorded in the MAC address table against that one port. When a router is connected to a switch port, only the MAC address of the router interface would be recorded against the switch port. ARP broadcasts are used to associate MAC addresses with IP addresses and such broadcasts would not directly result in multiple MAC addresses being recorded against a single switch port. Configuring the switch to perform Layer 3 switching will not result in multiple MAC addresses being recorded against a single switch port. The ARP table associated with the Layer 3 switch port may contain multiple IP address to MAC address mappings but this is to enable the correct framing of Layer 3 packets, not the Layer 2 frame switching function.

13. The MAC address of PC3 is not present in the MAC table of the switch. Because the switch does not know where to send the frame that is addressed to PC3, it will forward the frame to all the switch ports, except for port 4, which is the incoming port.

14. The term "fixed configuration" when applied to an Ethernet switch means that the hardware configuration, such as the number of ports, is fixed. Most fixed configuration switches can be configured using the IOS with features including multiple VLANs and SVIs. Configuring VLANs on a fixed configuration switch would put the ports in different subnets.

15. Ethernet line cards are added into modular switches to increase the number of ports. The more line that are added cards, the higher the port density.

16. The **no switchpor**t and **ip address** commands enable network layer services on a data link layer interface, configuring this port as a Layer 3 interface.

17. Increasing the number of hosts on an Ethernet segment will increase the number of collisions. This will eventually reduce the level of performance of the network segment since each host executes the back-off algorithm and must wait to retransmit for each collision.

18. The binary number 0000 1001 can be expressed as 09 in hexadecimal
    The binary number 0000 1010 can be expressed as ?? in hexadecimal

19. A store-and-forward switch always stores the entire frame before forwarding, and checks its CRC and frame length. A cut-through switch can forward frames before receiving the destination address field, thus presenting less latency than a store-and-forward switch. Because the frame can begin to be forwarded before it is completely received, the switch may transmit a corrupt or runt frame. All forwarding methods require a Layer 2 switch to forward broadcast frames.

20. What destination address will PC1 include in the destination address field of the Ethernet frame that it sends to PC2? PC1 will use the MAC address of its default gateway, Router1, in frames sent to PC2.