2020

CISC 4331 – Systems and Network Administration Week 6

Jimmy Richford
CUNY Brooklyn College

NYC Tech-in-Residence Corps

CISC 4331 – Systems and Network Administration

WEEK 6

Midterm

- Midterm on March 17th
- Closed book, no computers or mobile devices.
- No, you cannot use a subnetting chart.
- Don’t forget office hours are 1 hour before class. For the midterm, I will be available at 5pm.

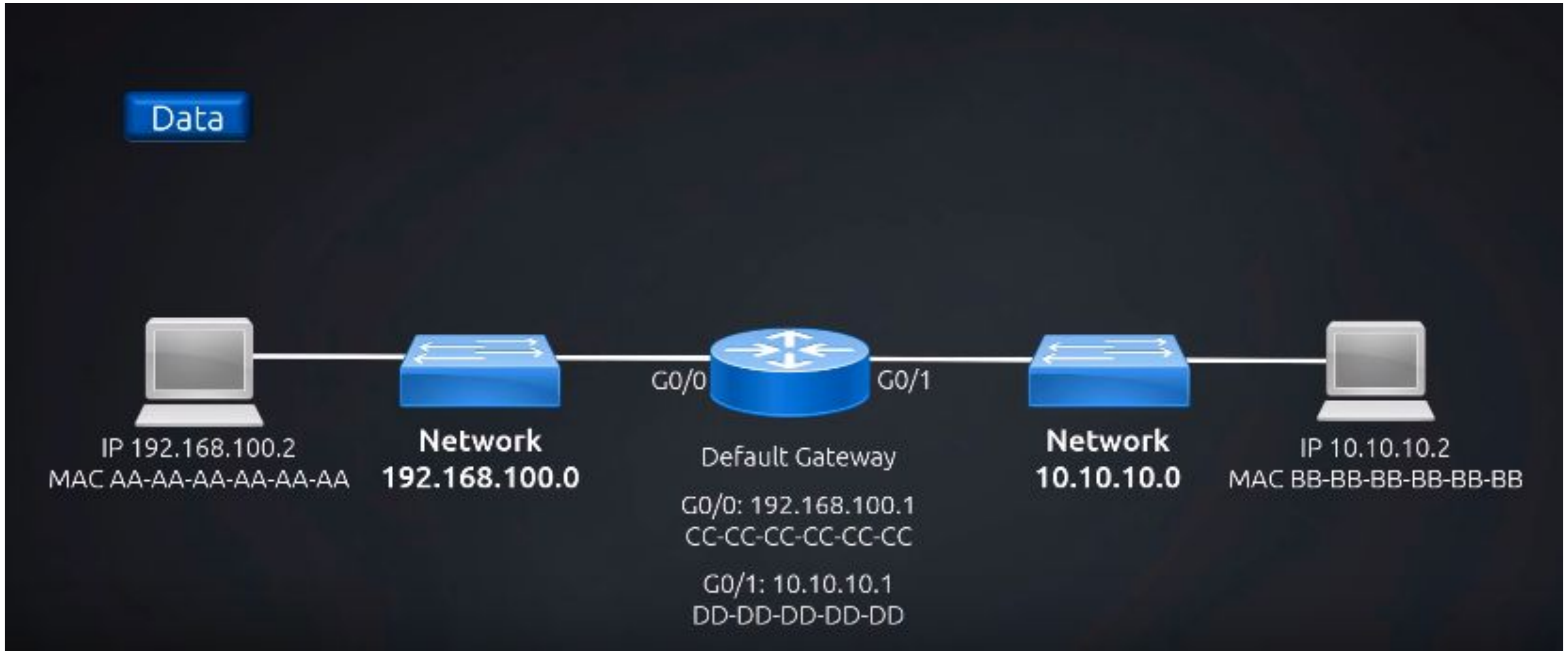
The Final Subnetting Slide

- Class A subnet masks must start with 255.0.0.0 at a minimum, because the whole first octet of an IP address (the IP address describes the specific location on the network) is used to define the network portion (the network portion describes the “street” that IP addresses are located on). Routers use the network portion to send packets through an internetwork. Routers aren't concerned about host addresses. They need to know only the “street” on which hosts are located and that the MAC address is used to find a host on a LAN. The last three octets of a Class A subnet mask are used to address hosts on a LAN; the 24 bits you can manipulate however you wish.
- One thing to remember, you first identify the class of the network (A,B,C) and the network portion will not change.

The Final Subnetting Slide

- Class A: A Class A IP address reserves 8 bits for a network with 24 bits dedicated to hosts. Its IP address spans from 0 to 126. The Class A subnet mask is 255.0.0.0. Accordingly, Class A IP addresses are best used to serve incredibly large networks. The first bit of the octet is always set to 0. (1-127). 00000001-01111111
  - Range: 1.x.x.x - 126.x.x.x (127 is the loopback)
- Class B: The first two bits are always set to 10. (128-191). Class B IP addresses are better suited to serving smaller networks since they reserve 14 bits for a network, which leaves only 18 bits for hosts. Network addresses for these range from 128 to 191. Consequently, the default subnet mask for Class B is 255.255.0.0. 100000000-10111111
  - Range: 128.0.x.x - 191.255.x.x
- Class C: The first 3 bits set to 110. (192-223). Class C IP addresses are normally assigned to a very small-sized network. Their IP addresses range from 192 to 233 and their default subnet mask is 255.255.255.0. 11000000-11011111
  - Range: 192.0.0.x-223.255.255.x

How A Packet Traverses A Network

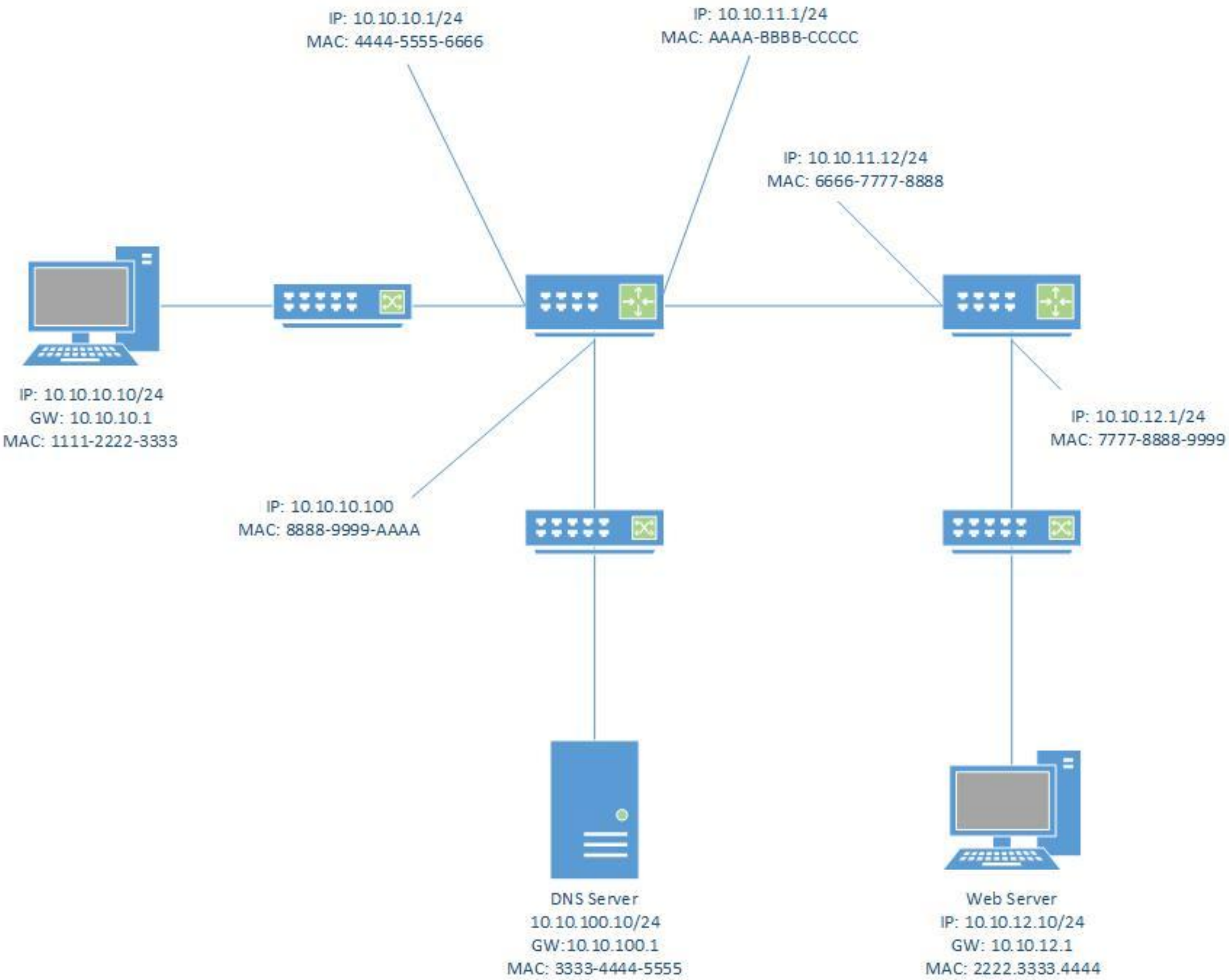


Lifecycle of a Packet

1. Remember: data -> packet -> frame.
2. Before it can send it out, it needs to create an IP packet with a destination IP.
3. Create an IP packet containing the data with the destination IP, as well as the source. So the header has 192.168.100.2 with a destination of 10.10.10.2.
4. Before sending it on the LAN, it creates a frame with the destination MAC address, which it doesn't know because it's on a different network (not on its own). But it has a default gateway and knows the MAC address of its default gateway (the router), so it puts a destination MAC address of the header frame of all C's in this example, since it knows its default gateway's MAC address.
    1. Packet gets stuffed in the frame (data -> packet -> frame)
5. Switch receives the frame, opens the header, sees CC-CC-CC-CC-CC-CC as the destination MAC address, looks at its table, has an entry for the router, and the frame moves on to the router.

Lifecycle of a Packet

1. Router takes the frame, analyzes the MAC header, sees the header as CC-CC-CC-CC-CC-CC and know it's for itself so it opens the frame, sees the packet header with a destination IP of 10.10.10.2. It knows this IP, leaves the destination the same, puts the packet in a new frame with a destination MAC of BB-BB-BB-BB-BB-BB which sends it to the 10.10.10.0 switch.
2. Switch knows how to get to 10.10.10.2 because it has an entry in its MAC address table for BB-BB-BB-BB-BB-BB-BB. It knows it came from 192.168.100.2, takes the data out of the packet, analyzes it, destroys the frame and it just has the data.
   - Important - if the sender knows the destination is on another IP subnet, it will not send an ARP request to 10.10.10.2 because it compares its IP and subnet mask, so it knows it has to send via a router, so it sends an ARP request to its default gateway.
   - The sender needs to know the receiver's IP address and MAC address to form the packet it's going to send.
   - The MAC address is not a logical address. You need a way to derive a MAC address -> ARP. (Maps destination IP address to MAC address).



IP: 10.10.10.1/24
MAC: 4444-5555-6666

IP: 10.10.11.1/24
MAC: AAAA-BBBB-CCCCC

IP: 10.10.11.12/24
MAC: 6666-7777-8888

IP: 10.10.10.10/24
GW: 10.10.10.1
MAC: 1111-2222-3333

IP: 10.10.12.1/24
MAC: 7777-8888-9999

IP: 10.10.10.100
MAC: 8888-9999-AAAA

DNS Server
10.10.100.10/24
GW:10.10.100.1
MAC: 3333-4444-5555

Web Server
IP: 10.10.12.10/24
GW: 10.10.12.1
MAC: 2222.3333.4444

Well Known Ports

- A network port is a process-specific or an application-specific software construct serving as a communication endpoint, which is used by the Transport Layer protocols of Internet Protocol suite, such as User Diagram Protocol (UDP) and Transmission Control Protocol (TCP).
- A specific network port is identified by its number commonly referred to as port number, the IP address in which the port is associated with and the type of transport protocol used for the communication.
- A port number is a 16-bit unsigned integer that ranges from 0 to 65535.

Well Known Ports

- FTP – File Transfer Protocol – Send files between systems. TCP 20/21
- TFTP – Trivial File Transfer Protocol – Simple unsecure file sharing. UDP 69
- SSH – Secure Shell – Encrypted console. TCP 22
- HTTP – Hypertext Transfer Protocol – Web communication. TCP 80
- HTTPS – Hypertext Transfer Protocol Secure – Secured. TCP 443
- DNS – Domain Name System. IP address to hostnames. TCP 53
- SMTP – Simple Mail Transfer Protocol. Email.   Port 25
- Telnet – Telecommunications. Remote console login (Unsecure) – Port 23