**Module 3 Review**

1. What is an IP address? IP address is your device’s digital address or its unique identifier.
   1. What is the purpose? IP address is needed to communicate on a TCP/IP network.
   2. What is the structure? IP address usually contains 32-bit numbers formatted four 8-bit separated by periods and will contain two component of a network ID and the host ID. Each 8-bit field represent a byte of the IP address. It will usually be in a format such as xxx.xxx.xx.xx with the network ID always coming before the host ID.
   3. What is the difference between IPv4 and IPv6? IPv4 is 32-bit while IPv6 is 128-bit IP address. IPv6 will contain letters while IPv4 won’t. Ipv4 are separated by periods while IPv6 is separated by colons. IPv4 use ARP (address resolution protocol) to map MAC address when IPv6 uses NDP (neighbor discovery protocol) to map MAC address.
      1. Advantages: auto-config, no more NAT, better multicast routing[[1]](#footnote-1)
      2. Disadvantages: system issues, difficult to remember, may cause load on network infrastructure, not supported on older devices[[2]](#footnote-2)
   4. What is the highest number used in IPv4? The highest number used in IPv4 is 255, with the lowest being 0.
   5. What are the classes of IP addresses? A, B, C, D?

* Class A is designed for large networks. Network uses 8 bits leaving 24 bits for host identification, meaning it could hold up to 16,777,214 hosts.
* Class B is designed for medium sized network. They split 16 and 16 bits for network and host ID bits, which allows 16,384 host with as many as 65,534 host per network.
* Class C is designed for smaller networks. Network portion is 24 bits, only 8 bits for host ID. Allows for 2,097,152 networks but each network can only have a max of 254 host.
* Class D is used for multicasting applications, they have a 32-bit network addresses.

1. CIDR and Subnet Mask: Subnet mask is a value that is written like an IP address, such as 255.255.255.0, if the number on subnet mask is a zero, that part of the IP address is the host potion, CIDR just means that you can use more than 255 as an octet to your subnet mask, such as 255.128.0.0.
2. Network Address Translation: (nat) translate your private, nonroutable IP addresses into public IP address.
3. DNS: purpose is to resolve hostnames into Ip addresses, example is when you type in a URL into a webbrowser, the DNS translate the URL into an ip address so communication can happen.
4. What is a port? A port is something used by TCP and UDP to keep track of different connections connected to a web server
5. Port Security: A method to restrict host based on specific MAC address, it is configured on the switch port(s) of a network switch.
6. Data Loss Prevention: system used to ensure that end users do not send sensitive and critical information outside of the organization, ensuring that data lost will not occur.
7. What is a MAC address? Every network interface card has their own unique MAC address, connected with switches, for use as a network access within a network segment.
   1. How is it assigned? It is assigned by the Network interface card
   2. What is the length? It is 48 bits long written in hexadecimal for example B6-15-53-8F-29-6B
   3. Can it be changed? They are hardcoded into the network card so they cannot be changed but there is tricks and ways you can still change it.
   4. What is the purpose? The purpose is to identify which device is which and allow the router to transfer data into the specified address.
8. Difference between TCP and UDP. TCP is connection-oriented while UDP is connection-less. TCP is guaranteed to be delivered while UDP might not provide guaranteed delivery. TCP also uses a flow control so that user will not be overwhelmed by data while UDP does not have flow control.
   1. How are TCP connections established? TCP will send a segment called a SYN to the TCP protocol on the receiving end, then the receiving TCP returns a segment which confirm, then the sending TCP will start sending over data.
   2. What are common types of TCP connections? HTTP and HTTP/2
   3. What are common types of UDP connections? NTP TFTP DHCP RTSP
   4. Difference between a connectionless and connection oriented service: connection oriented service will guarantee the packet delivery through data acknowledgement, while connectionless does not.
9. What are the differences between these network devices.
   1. Gateway: If the host needs to communicate outside the local network, it also needs a default gateway, which is normally the internal address of the router.
   2. Bridge: Bridges isolate network traffic, preventing unwanted traffic from entering a segment when there are no receiving targets on that segment. They are also used to divide network segments into multiple collision domains.
   3. Router: They route packets across multiple networks and use addresses to determine destination. They also make decision based on IP addresses.
   4. Switch: Switches provide centralized connectivity, just like a hub but switches can decide which port to forward packet to, allowing switches to deliver packet to specific target
   5. Repeater: a device that receives a signal, amplifies it, then sends it out, usually use for cable extension
   6. Hub: used to link several PC together, they repeat any signal that comes in 1 port and copy it to the other ports.
   7. VPN: a secure (private) network connection that occurs through a public network
   8. Firewall: a hardware or software application that serves as your network’s security guard.
   9. DMZ: Some firewalls have a third network port for a second semi-internal network. This port is used to connect servers that can be considered both public and private, such as web and email servers, this is known as DMZ.
   10. SSL: cryptographic protocols designed to provide communications security over a computer network.
   11. TLS: successor to SSL, now more popular than SSL
10. What is a wireless network? Allowing the user device to be able to access the internet without the use of cable, through wi-fi, the user will be able to surf the internet.
    1. Advantages: does not need to be physically connected to the router, more access point in the location where wireless network is enabled which will allow the user more flexibility on where to place their device.[[3]](#footnote-3)
    2. Disadvantages: more prone to attack by unauthorized user, some might have really bad coverage which mean not allowing the user to have the best signals[[4]](#footnote-4)
11. Define and describe the following.
    1. Phishing: asking for personal information by making it as if it was a legitimate request, the user then will give out personal information relating to the request because they will not know that it is a scam.
    2. Pharming: a form of redirection in which traffic intended for one host is sent to another.
    3. Whaling: A scammer trying to receive/scam information from a specific target, which the specific target will have most/all data that the scammer wants.
    4. Wardriving: driving around in a car looking for unsecured wireless networks to hack into
    5. Spoofing: attempt by someone or something to masquerade as someone else.
    6. Virus: A virus will try to render your system, making it slower or even unusable, or try and spread to other system on the connected network.
    7. Worm: Can reproduce itself, it can contain itself and it does not need a host, it also can use TCP/IP to reach their target. It can also contain a virus to spread.
    8. Trojan: programs that enter system or network as a disguise as another program.
    9. R.A.T.: A RAT or remote administration tool, is software that gives a person full control a tech device, remotely. The RAT gives the user access to your system, just as if they had physical access to your device. With this access, the person can access your files, use your camera, and even turn on/off your device.
12. Principles of Authentication: When giving a user permission on a computer, only give them the permissions they need to do their work and nothing else.
13. Principles of Password: security password should be unique to yourself, it should be very difficult to guess, should be too complex to memorize, should be well-managed, and some passwords should have a second password (aka F2A).
14. Incident response evidence collection: When an alerts happen and/or there is something suspicious on the networks, a person could come in to collect digital evidence to confirm that a breach has happened.
15. What is Personally Identifiable Information? PII is anything that can be used to identify an individual person on its own or in context with other information.
    1. Risks: could causes millions of monetary damages if a security breach happen containing those information
    2. Types: linked and linkable information
    3. Examples: someone’s credit card, phone number address, other contact information.
16. What is TCP/IP: Is a model and set of communication protocol used by all computer on the internet.
    1. What does it do? It allows computer on the internet to interact with each other/ Specify how they transfer data from one device to another.
    2. When was it invented? It was invented in the 1960s.
    3. Who invented it? It was developed by the US department of Defense, or Defense Advanced Research Projects Agency to be exact.
    4. What are the layers? The four layers are Process/Application, Host2Host/transport, Internet and then Network access/link
    5. What protocols are associated with each layer? The most commons protocols are:

Telnet FTP LDAP SNMP DHCP SMTP HTTP HTTPS

TCP UDP

ICMP ARP RARP IP

Ethernet Fast Ethernet Gigabit Ethernet 802.11

1. Internet Layer: most important layer, contain the IP or internet protocol that is responsible for managing logical network addresses and ultimately getting data from point A to point B, even if there are dozens of points in between.
2. Transport Layer: Contains TCP and UDP, depending on the application layer’s protocol, also uses ports to manage connections.
3. Application Layer: Contain a bunch of different protocol that is used depend on the user’s wants and need. They just need to make sure that the protocol delivers what it needs to and can communicate with the layers below it, AKA transport and internet.
4. Link Layer: What the physical or nonphysical type of network that the user is using, examples are wi-fi and ethernet.
5. What is a network collision? A network collision occurs when two or more devices attempt to transmit data over a network at the same time. For example, if two computers on an Ethernet network send data at the same moment, the data will "collide" and not finish transmitting. This is why most networking protocols confirm that packets have been received before transmitting additional data.[[5]](#footnote-5)
6. What are 5 types of networks? (each are 3 letter acronyms): LAN, WAN, PAN, MAN, and WMN
7. Network Toplogies
   1. Star: Each network device is connected to a hub or a switch, making it super easy to add new device. If a device goes down, does not affect the network, but if the hub/switch goes down, everything goes down.
   2. Ring: Each device connects to two other devices, joining them in a circle and create a path where it move from device to device.
   3. Mesh: Each device is connected to every other device; this will use a large amount of cables the more device a system contains. The equation for the amount of cables require is ( x \* ( x – 1)) ÷ 2) with x being the amount of device in such system.
   4. BUS: A single cable is connected to every device; they all share the same data and address path. If a message is received, each device will check if the address matches it, if yes then the network adapter will retrieve it, if not the message is ignored.
   5. Hybrid: a mix of the other topologies. Hybrid network is maybe more expensive than other topologies but takes the best features from all of them.
8. What is a datacenter and its purpose? A physical facility that is used to store critical applications and data, it is designed to enable the delivery of shared applications and data. Key components include routers, switches, firewalls, storage systems, servers, and application-delivery controllers.[[6]](#footnote-6)
9. What is troubleshooting? The process of working out problem/error shown by the computer or any machinery caused by unknown issues on the computer/machinery and the user is trying to figure out ways to fix such issues.
10. What are the steps of troubleshooting? Identify the Problem, establish a Theory, Test the Theory, Establish a Plan of Action, Verify Functionality, and then Document Findings
11. From the lecture – what are the 6 principles of dealing with customers:

Communicate, using understandable language for the customers, reproducing the error because they might not know what the issue is, what was different before and after the error, be polite with the customers, and follow up with them even if you are able to resolve the issue.

1. What mnemonic sentence was used in the lecture to remember the 7 layers of the OSI model? “All People Seem To Need Data Processing”
   1. What are the seven layers? Application, presentation, session, transport, network, datalink, and physical
2. What is bandwidth? How is it measured? Bandwidth is the amount of data that can be sent to you, usually measured in seconds, Kbps Mbps and Gbps.
3. What is a protocol? It is a language(s), with different type of rules for each language, used by computer to communicate and share data with each other.
4. Know how to convert to and from binary and decimal.
   1. Base10: decimal, 123456789…
   2. Base2: binary, 1 and 0 only
   3. Base16: hexadecimal, uses 0-9 and a-f
5. Protocols – what are they and what is the standard port
   1. HTTP: It manages the communication between a web server and client, and lets you connect to and view all the content that you enjoy on the Internet, port 80.
   2. HTTPS: To encrypt traffic between a web server and client securely uses Secure Sockets Layer (SSL) or Transport Layer Security (TLS), port 443.
   3. HTMP(L?): HTML is a language used by webpage, HTMP is hospitality and tourism management program for high school(?).
   4. URL: Uniform Resource Locator, a “link” or address used to access a certain website/webpage, such as http://www.wiley.com.
   5. FTP: optimized to transfer files, both uploading and downloading files from one host to another. It let you copy files, list and control directories and view file contents, port 20,21.
   6. SMTP: used to send email from mail server to mail server as well as server to client. By querying the DNS server for mail exchange record, SMTP is used to push the message to the email server, which then the server will process the message for delivery, port 25.
   7. DHCP: dynamically assigns IP addresses and other IP configuration information to network clients, port 67,68.
   8. P2P: Is a model usually used for small and simple networks. Does not require extra hardware and many OS supports it. Such network is also preferred to as workgroups.
   9. VLAN: virtual local area network (VLAN) is designed to help segment physical networks into multiple logical (virtual) networks, created by using a managed switch. The switch uses Spanning Tree Protocol (STP) to manage configurations and to ensure that there are no infinite network loops.
   10. SSH: can be used to set up a secure Telnet session for remote logins or for remotely executing programs and transferring files, port 22.
   11. RDP: Remote Desktop Protocol (RDP) allows users to connect to remote computers and run programs on them, port 3389.
   12. 1053: TCP, port 1053 is a malware called the thief(?)
   13. 7850: TCP, is a paltalk trojan(?)
   14. 161: Simple Network Management Protocol (SNMP) used for collecting and organizing info about managed devices on IP networks.
6. Commands
   1. ipconfig - Displays all current TCP/IP network configuration.
   2. Nslookup - Displays information that you can use to diagnose Domain Name System (DNS).
   3. Ping - Try to verify connectivity with another IP through a set of messages.
   4. Hostname – find the computer host name.
   5. Tracert - A command toll used to determine the path taken to a destination by sending messages to the designation.
   6. Netstat - Displays TCP connections, port, ethernet information, IP tables, IPv4 info, and IPv6 info.
7. Social Engineering - a process in which an attacker attempts to acquire information about your network and system by social means, such as talking to people in the organization.
8. Denial of Service/DDOS - an attack launched to disrupt the service or services a company receives or provides via the Internet.
9. Difference between a Vulnerability/Threat/Exploit:

Vulnerability: weakness in security for an OS or network product

Threat: Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset.

Exploit: something that is used to exploit the vulnerability by a threat agent

1. Zero-Day: The exploiter will learn of a vulnerability the same day as the developers so they will have a few days to exploit such weakness until a patch is released.
2. Principles for securing your network – change default username and password, assign static IP address, disabling unused ports, use a firewall, content filtering
3. Securing an operating system best practices – setting strong passwords, requiring password, have a password expiration, restricting user permission, limit failed login attempts, disable guest account, having a firewall.

Citation

Collision. (n.d.). Retrieved November 08, 2020, from https://techterms.com/definition/collision

Docter, Q., & Buhagiar, J. (2019). *CompTIA A+ complete study guide: Exam 220-1001 and exam 220-1002*. INpolis, IN: Sybex, a Wiley brand.

Hoffman, J. (2020, August 13). Pros and Cons of IPv6. Retrieved November 08, 2020, from https://wisdomplexus.com/blogs/pros-cons-ipv6/

IPv4 vs. IPv6 Benefits - What is it? (n.d.). Retrieved November 08, 2020, from https://www.thousandeyes.com/learning/techtorials/ipv4-vs-ipv6

What Is a Data Center? (2020, September 04). Retrieved November 08, 2020, from https://www.cisco.com/c/en/us/solutions/data-center-virtualization/what-is-a-data-center.html

Wireless technology. (n.d.). Retrieved November 08, 2020, from https://www.nibusinessinfo.co.uk/content/pros-and-cons-wireless-networking

1. https://www.thousandeyes.com/learning/techtorials/ipv4-vs-ipv6#:~:text=IPv4%20uses%20a%2032%2Dbit%20address%20for%20its%20Internet%20addresses.&text=IPv6%20utilizes%20128%2Dbit%20Internet,the%20number%20of%20IPv4%20addresses. [↑](#footnote-ref-1)
2. https://wisdomplexus.com/blogs/pros-cons-ipv6/ [↑](#footnote-ref-2)
3. https://www.nibusinessinfo.co.uk/content/pros-and-cons-wireless-networking [↑](#footnote-ref-3)
4. https://www.nibusinessinfo.co.uk/content/pros-and-cons-wireless-networking [↑](#footnote-ref-4)
5. https://techterms.com/definition/collision [↑](#footnote-ref-5)
6. https://www.cisco.com/c/en/us/solutions/data-center-virtualization/what-is-a-data-center.html [↑](#footnote-ref-6)