220-1101 Networking Study Guide

General Information - Understanding all types of networks and their corresponding connections is vital if you are in an IT support position. You will need to know everything about TCP/IP, Wi-Fi, and SOHO connections. About 20% of the CompTIA A+ 1101 test concerns various aspects of networking. Around 25% of the questions concerning networking will begin with a scenario.

Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) Ports -, you must be able to **compare and contrast** TCP and UDP ports and protocols and their respective purposes. **Memorizing port numbers** is highly recommended for this section.

Ports and Protocols - the protocols that run over those ports, and the **primary use** for each. A port is the unique identifier number for transmission control and direction. A protocol is a set of rules that govern communications.

20/21—File Transfer Protocol (FTP) - is used to manipulate files. FTP can copy files, list and manipulate directories, and view file contents. FTP runs on ports 20 and 21. **Port 21** is mainly used for file management and **port 20** is used for data transfer. FTP is **not secure** and transmits in **plain text**.

22—Secure Shell (SSH) - is a connection-oriented protocol used to set up secure Telnet connections for remote logins. SSH is **secure** and runs on **port 22**.

23—Telnet - is a terminal emulation program that allows for remote access to text on another computer. Telnet is **not secure** and transmits **plaintext**. Telnet uses **port 23**.

25—Simple Mail Transfer Protocol (SMTP) - is used to send **email only** and is a **push protocol**. SMTP uses **port 25**.

53—Domain Name System (DNS) - is used to resolve hostnames to IP addresses and uses **port 53**.

67/68—Dynamic Host Configuration Protocol (DHCP) - assigns IP addresses dynamically to network clients. DHCP uses **port 67** for the server and **port 68** for the client.

80—Hypertext Transfer Protocol (HTTP) - manages communications between a web server and a client to view internet content. HTTP is **not secure** and transmits in **plain text**. HTTP uses **port 80**.

110—Post Office Protocol 3 (POP3) - is used for **downloading email**. POP3 uses **port 110**.

137/139—Network Basic Input/Output System (NetBIOS)/NetBIOS over TCP/IP (NetBT) - is an API for **communication between computers** over a network. NetBIOS works over OSI layer 4 and needs to work with a layer 5 protocol, namely TCP/IP, to function properly. NetBIOS over TCP/IP is called NetBT. NetBIOS runs on **ports 137/139**.

143—Internet Message Access Protocol (IMAP) - is currently in its fourth version, or IMAP4, and is used for downloading email. IMAP4 is **secure** and runs over **port 143**.

161/162—Simple Network Management Protocol (SNMP) - is used for network management. SNMP uses **port 161** for sending and receiving requests and **port 162** for receiving transmissions from managed devices.

389—Lightweight Directory Access Protocol (LDAP) - is used for **accessing information** stored in an information directory. LDAP uses **port 389**.

443—Hypertext Transfer Protocol Secure (HTTPS) - is the **secure version of HTTP**. HTTPS uses **port 443**.

445—Server Message Block (SMB)/Common Internet File System (CIFS) - SMB is primarily a **Microsoft protocol** used for **shared file access**. CIFS is an enhanced version of SMB. SMB/CIFS use **port 445**.

3389—Remote Desktop Protocol (RDP) - allows for remote connection to computers. RDP uses **port 3389**.

TCP vs. UDP - Transmission Control Protocol (TCP) is a connection-oriented protocol used to send and receive data over a network. Before data is sent, a connection is established with the receiving host. It is considered a **reliable protocol** because the receiving host acknowledges that it received the data. TCP is used in cases where receiving the proper data is more important than speed. **User Datagram Protocol (UDP)** is a **connectionless protocol**. Data is sent without any assurance that the receiving host is actually receiving the data. For that reason, it is considered an **unreliable protocol**. The advantage of UDP over TCP is that it is faster.

Connectionless - protocols allow for data to flow without guaranteeing an established connection. This allows for faster data flow but does not guarantee reliable data flow. UDP is connectionless.

DHCP—Dynamic Host Configuration Protocol is used to dynamically **assign IP configuration information** to clients through a lease and uses UDP as its transport protocol. DHCP runs on **port 67/68**.

TFTP—Trivial File Transfer Protocol is a **faster version of FTP** that **uses UDP** rather than TCP as its transport protocol. TFTP uses **port 69**.

Connection-Oriented - communication establishes a set connection before data flow begins between two devices. ***TCP***

HTTPS—Hypertext Transfer Protocol Secure is a connection-oriented protocol that uses TCP as its transport protocol. HTTPS uses **port 443**.

SSH—Secure Shell is a connection-oriented protocol that uses TCP as its transport protocol. SSH uses **port 22**.

Common Networking Hardware - includes the physical components used to achieve network connectivity.
Router - is a device that connects multiple network devices and determines the best path for reaching a specified device using routing tables. Routers are **OSI Layer 3** devices and make decisions based on logical addresses. Key functions of a router include **connecting multiple network devices** to one another, breaking up broadcast domains, and connecting one LAN to another LAN on a WAN.
Switch - is a device that works at **OSI Layer 2**, examines the header of incoming packets for the MAC address, and forwards the packet to the correct location. Switches can be managed or unmanaged.
Managed - is one that **allows for port configuration**, traffic management, and traffic monitoring. Managed switches offer quality of service (QoS), redundancy, port mirroring, and VLANs.
Unmanaged - A switch does *not* allow for configuration and passes on all data for a MAC address to its ports.
Access Point - is technically any device to which a host can connect in order to access a network. Wired access points include **hubs** and **switches**. However, the term usually refers to a wireless access point (WAP) that allows Wi-Fi devices to connect to a network.
Patch Panel - is a dumb device that is essentially a large rack-mounted HUB whose sole purpose is to **connect cables** together. A **dumb device** is a device that broadcasts all data coming in through the input port out over all output ports. A dumb device, like a patch panel, makes no logical decisions and simply serves as a connection and relay point.
Firewall - is a **security appliance**, either hardware or software, that filters network traffic based on a preconfigured set of rules.
Power over Ethernet (PoE) - is a technology that **delivers power to devices** over data lines, such as an ethernet cable, rather than having a separate power cord.
Injector - is a **midspan device** that sits between the switch and the access point and supplies power via an ethernet connection.
Switch - sits in front of the midspan injector device and provides **power to the ethernet cable**.
PoE Standards - are the **IEEE 802.3 standards** that define PoE specifications.

- **PoE- 802.3af-15.4 W**—WAPs, static surveillance cameras, VoIP phones
- **PoE+- 802.3at-30W**—alarm systems, PTZ cameras, video IP phones
- **PoE++- 802.3bt (Type 3)-60 W**—multi-radio WAPs, video conferencing equipment
- **PoE++- 802.3bt (Type 4)-100 W**—laptops, flat-screen monitors

Hub - is a dumb **Layer 1** device that sends all incoming data to all connected devices as a broadcast. Hubs are also known as **multiport repeaters**.
Cable Modem - is a device that connects to a cable line to provide **connectivity**. A cable modem is technically no longer a modem, however, since it does not modulate and demodulate analog signals.
Digital Subscriber Line (DSL) - modem provides connectivity **via a telephone line**.
Optical Network Terminal (ONT) - modem is one that provides connectivity **via a fiber-optic line**.
Network Interface Card (NIC) - also known as a **network adapter card**, is used to provide the physical interface between a computer and the cabling used for connectivity.
Software-Defined Networking (SDN) - sets up a network virtually **via the cloud**. The SDN replaces the functionality of the router in a network.
Protocols for Wireless Networking
Frequencies - of a wireless protocol refers to the audio range in which the technology broadcasts. The **two operating frequencies for Wi-Fi** are 2.4 GHz and 5 GHz. The frequency has an impact on transmission range and data throughput.
2.4 GHz—This relatively low frequency (compared with 5 GHz) has a **greater transmission range** because it passes through objects such as walls and floors better. On the negative side, **throughput is slower** and it is an open frequency range that other devices use. Devices like cordless phones and microwave ovens can **interfere** with it.
5 GHz—At this higher frequency, **throughput is faster**. On the negative side, the **transmission range is shorter** as the signal is attenuated by objects such as walls and floors.
Channels- are different frequencies that are used for communications between the end-user device and the wireless access point. The **2.4 GHz range** has 14 channels, but the top three cannot be used in **North America**, so the U.S. has **11 available channels**. Devices will automatically select a channel, but if there seems to be interference, we can manually select another channel. The **5 GHz range** also has channels, but there is more room in the RF spectrum at that range, so we never have to set those channels.
Regulations - The Federal Communications Commission (FCC) has defined 14 different 22 MHz communications channels but only allows for the use of the first 11 channels.

2.4 GHz vs. 5 GHz - There are 25 defined 20 MHz channels at 5 GHz, 24 of which can be used for Wi-Fi communications, while 2.4 GHz only has 14 defined channels, 11 of which can be used.
Bluetooth - allows devices to communicate over short distances (10 meters) in a personal area network (PAN). It is typically used to **connect peripherals**, such as headphones, to a laptop or smartphone. It is the IEEE 802.15.1 standard.
802.11 - is part of the IEEE 802 wireless networking standards. It is used for Wi-Fi communications. They all use the ethernet protocol and carrier sense multiple access with collision avoidance (CSMA/CA) media access method. The main characteristics that differentiate them are their operating frequencies, theoretical maximum data speed, and throughput.
a—5 GHz frequency, 54 Mbps maximum throughput, 120 meters range
b—2.4 GHz frequency, 11 Mbps maximum throughput, 140 meters range
g—2.4 GHz frequency, 54 Mbps maximum throughput, 140 meters range
n—5/2.4 GHz frequency, 600 Mbps maximum throughput, 250 meters range
ac (Wi-Fi 5)—5 GHz frequency, 6.5 Gbps maximum throughput, 140 meters range
ax (Wi-Fi 6)—5/2.4 GHz frequency, 9.6 Gbps maximum throughput, 140 meters range
Long-Range Fixed Wireless - connection is a point-to-point wireless technology that employs the use of directional antennas to send and receive network signals usually from **10 to 20 km**.
Licensed - frequencies are frequencies whose use is granted by the **FCC** in the US.
Unlicensed - frequencies are frequencies that can be used by anyone, such as 2.4 and 5 GHz. The common use of these frequencies, however, often causes **interference** and can create susceptibility to **eavesdropping**.
Power - can be transmitted via long-range fixed wireless and is commonly known as wireless power transfer (WPT). Power is generated by the transmitting station and sent via microwave or laser light to the receiver who turns the transmission back into electricity.
Regulatory Requirements for Wireless Power - WPT technology is regulated by the FCC in the US.
Near-Field Communication (NFC) - has a **very short range** of a few inches. It is used for contactless communications between devices that are right next to one another. The most common use today is for contactless payment systems.
Radio-Frequency Identification (RFID) - uses a **radio signal** to send information from an RFID tag with identifying information. This is commonly used to streamline the inventory of tracking applications.
Networked Host Services - You need to have a working understanding of the properties and purpose of network-delivered services in a client-server environment and know how to **summarize** them. Know the difference between a **client application** and a **server application**. Client applications request services from a server application.
Server Roles - You are expected to have a working understanding of the following network services. A server is not necessarily a stand-alone piece of hardware. A server is usually a **process running in memory** on a networked system that responds to requests from a remote client system.
DNS - Domain name system servers resolve hostnames to IP addresses. Two public DNS servers are needed for an enterprise to host a website, with one DNS server acting as redundancy. Records of hostname IP address sets are held in a zone file. If the DNS address is not located in the zone file, it requests the information from a higher-level DNS server called the **root server**.
DHCP - A Dynamic Host Configuration Protocol server provides **IP configuration information**, such as an IP address, subnet mask, default gateway, and DNS server address, automatically to clients. The scope of a DHCP server contains the information that is permitted to be shared with a client.
Fileshare - or file server is a **central repository** for the storage, management, and access of network files. A network can also use network-attached storage (NAS) for a file server.
Print Servers - is a server that manages print requests and connects printers to a network.
Mail Servers - is responsible for sending, receiving, and managing emails. A mail server must be running a **specialized server package**, such as Microsoft Exchange, Sendmail, Postfix, or Exim, to be considered a mail server.
Syslog - server in a client-server model is responsible for **collecting information** obtained through system monitoring, such as **login events or errors**. Messages compiled in a syslog server include the facility code, the severity level, and a textual description of the logged events. Syslog servers are composed of **three primary components**: the listener, the database, and the management and filtering software.
Web Servers - listens for incoming requests. The requests are executed by the web server and provide the requested content, including text, images, videos, and the running of scripts. Common web server platforms include Microsoft's Internet Information Services (IIS) and Apache.

Authentication, Authorization, and Accounting (AAA) - (triple A) server is an access control server that acts as a gatekeeper for critical network components. AAA servers are also known as domain controllers. Examples of AAA servers include remote access service (RAS), Remote Authentication Dial-In User Service (RADIUS), Terminal Access Controller Access-Control System Plus (TACACS+), and Kerberos.

Internet Appliances - is a device that aids in internet access and helps users access the internet safely.

Spam Gateways - also known as an **antispam gateway**, is an internet appliance whose purpose is to **block malicious emails** from accessing the network.

Unified Threat Management (UTM) - acts to **centralize security management** on a network. UTM typically provides packeting filtering and inspection, IPS, gateway antimalware, spam blocking, malicious website blocking, and application control.

Load Balancers - is responsible for **evenly distributing** requests over servers to balance the system. Common load balancing configurations include identical, cross-region, and content-based load balancing.

Proxy Servers - makes requests for resources on behalf of a client. The proxy server acts as an intermediary between the client and the target server.

Legacy - are older systems that for one reason or another have not been updated. It is usually due to essential applications that will not run on the updated platform.

Embedded systems are devices other than computers that have computer technology running within. Like legacy systems, these may not be able to stay updated.

Supervisory Control and Data Acquisition (SCADA) - is an example of a **critical legacy system category**. A SCADA system is a high-level management system used to control manufacturing machines and processes, manage large-scale infrastructure settings, and run building components.

Internet of Things (IoT) Devices - connects to the network through a central controller or coordinating device. Common examples of IoT devices include **smart devices** such as thermostats and home automation and security devices.

Basic Wired/Wireless Small Office/Home Office (SOHO) Networks

When setting up a (OHO network, keep the following steps in mind:

- Understand relevant regulations.
- Make a map.
- Locate the server(s).
- Identify client computer locations.
- Locate network resources.
- Determine user connectivity type.
- Designate additional connectivity options if needed.

You must be able to install and configure basic wired and wireless SOHO networks. On the CompTIA A+ exam, these concepts will be addressed in scenario-based questions.

Internet Protocol (IP) Addressing - is the assignment of a unique device identifier on a local network or the internet. The IP address is responsible for managing logical network addresses.

IPv4 - address is a **32-bit hierarchical address** that identifies a host on a network and is typically written in dotted-decimal notation. The 32-bit address is divided into 4 bytes, or octets, containing 8 bits each (ex: 192.168.10.55). IPv4 addresses are divided into designated classes, A, B, C, D, E, and F, based on the first 3 bits of the IP address. IPv4 addresses are **finite** and are running out.

Private addresses—A private IP address is **not routable** on the internet.

Class A private address range: 10.0.0.0–10.255.255.255

Class B private address range: 172.16.0.0–172.31.255.255

Class C private address range: 192.168.0.0.–192.168.255.255

Public addresses—Public addresses are **routable on the internet**. Public addresses are purchased and **only one computer** can hold any given public address at a time.

IPv6 - addresses are **128-bit addresses** expressed in **hexadecimal notation** and are composed of eight 16-bit fields separated by colons (ex: 2001:0db8:3c4d:0012:0000:0000:1234:56ab, which can be reduced to 2001:db8:3c4d:12::1234:56ab)

Automatic Private IP Addressing (APIPA) - assigns an IP address to a device that was not assigned a static or dynamic IP address. The address will be **in the 169.254.0.0 network**. This is generally not useful, other than being an indication that the device failed to get an IP address through normal means. These addresses are also referred to as link-local addresses.

Static - address is one that is **set manually** by a user or administrator. A device that is assigned a static address will keep that address until someone changes the configuration.

Dynamic - address is one that is **automatically assigned**, typically by a router or DHCP server. The next time a device that was dynamically assigned an IP address joins the network, it may be assigned a different IP address.

Gateway - is a **router that connects your network** to another network, typically the Internet. When configuring a device on the network, you specify the internal IP address of the gateway as a default destination to send traffic.

Common Network Configuration Concepts

You must be able to **compare and contrast** common network configuration concepts for the CompTIA A+ exam.

DNS - domain name system has only one function: to **resolve hostnames to IP addresses**. DNS settings are usually given out via DHCP along with IP address information, but this can be done manually as well. This allows the user (client) to resolve domain names to IP addresses in order to perform searches or lookups. These are usually given out in a primary and secondary fashion for redundancy purposes.

Address - are contained on the DNS server in **zone files**. The zone file maintains records of hostname-to-IP address mappings and contains information such as the name of the server or computer, internet protocol address, record type, computer address, and comments.

A—*A* is a common DNS record type that signifies that the host record is an **IPv4** address.

AAAA—*AAAA*, pronounced “quad A”, is a common DNS record type that signifies the host record is an **IPv6** address.

Mail Exchanger (MX) - record is a common DNS record type that signifies that the host record is the name or address of an email server.

Text (TXT) - record is a common DNS record type that signifies that the host record is a text record for human-readable or machine-readable data.

Spam Management - is the process of determining if data is spam or valid.

DKIM—DomainKeys Identified Mail is a type of spam management that authenticates using **encryption** through a public-private key pair.

SPF—Sender Policy Framework (SPF) is a type of spam management that authenticates an email server **based on its IP address**.

DMARC—Domain-based Message Authentication, Reporting and Conformance is a type of spam management that **combines DKIM and SPF** in one framework and offers **more control** over what the user can do with spam email.

DHCP - Dynamic Host Configuration Protocol automatically assigns all of the settings needed to access resources on your LAN or the internet. It can provide IP address, subnet, gateway, and DNS information. If you want to ensure that a device gets a specific IP address, you can configure a DHCP reservation in the DHCP server.

Leases - is a temporary IP configuration assigned by the DHCP server to a client. A lease typically includes an IP address, subnet mask, default gateway, and DNS server address.

Reservations - is the reserving of an IP address for a specific client based on the client’s MAC address and is primarily used for devices that require a static IP address.

Scope - is information provided outside the IP address and the subnet mask issued by the DHCP server, such as the default gateway, DNS server address, or domain name.

virtual local area network (VLAN) is a **logical subnet**, typically configured on a switch, that acts as a separate subnet. Without VLANs, every device connected to a switch would be on the same subnet. By configuring VLANs on the switch, you can have devices on that one switch in different subnets or VLANs.

Virtual Private Network (VPN) - is an **encrypted connection** between two networks or between a host and a network. When a host connects to a network over a VPN, it is assigned a separate IP address that is in the network’s address range.

Internet Connection Types - are methods, either wired or wireless, through which a device can connect to the internet.

Satellite—connection is a wireless connection type that employs the use of satellites to achieve connectivity. Satellite connections are typically slower than wired broadband connections and require a satellite dish. Weather and misalignment can affect connectivity.

Fiber—connection is a type of wired connection that uses a fiber-optic cable made of thin flexible glass or plastic fiber surrounded by a rubberized outer sheath to send data via light signals. Fiber offers fast data transmission. There are **two types** of fiber varieties: **single-mode fiber (SMF)** and **multimode fiber (MMF)**.

Cable—connection is a type of wired connection that uses a cable, either **coaxial/coax** or **twisted pair**, for data transmission. Coax and twisted pair cables use different connector types and cable specifications.

DSL—A digital subscriber line is a type of **wired connection** that uses existing phone lines paired with a DSL modem to provide internet service.

Cellular—connection is a type of wireless connection type that uses a **provider's cellular network** for connectivity.

WISP—A wireless internet service provider is a wireless connection type in which an internet service provider (ISP) offers connectivity using wireless technology. WISP connections are **fixed point-to-point connections**.

Network Types - define the general area that is covered by a network.

LAN—A local area network is a collection of devices connected to one another in **one physical area**, such as an office building, and can be small or large.

WAN—A wide area network is a network that covers a **large geographical area** and is composed of multiple LANs. The internet is a WAN.

PAN—A personal area network is composed of primarily **Bluetooth-connected devices**.

MAN—A metropolitan area network is a network larger than a LAN but smaller than a WAN and **limited to a smaller geographical area**, such as a city or a campus.

SAN—A storage area network is a network area composed of **storage devices**.

WLAN—A wireless local area network is a LAN in which the **connections are wireless** rather than wired.

Networking Tools - evaluate a set of network requirements in a **given scenario** and select the best tool for the job.

Crimper - is used to **connect a connector to a cable**. It is not usually practical to use cables of a fixed length. It is also easier to run cable without the connectors on it. So, the cable is run and cut to the desired length, and then the connector is crimped on using a crimper. There are **different types** of crimpers for ethernet, coaxial, and fiber-optic cables.

Cable Stripper - are used to **remove the insulation** from the end of a cable before the connector is crimped onto it.

Wi-Fi Analyzer - is used to design, optimize, or troubleshoot a Wi-Fi network. This device is used to show strong and weak spots in wireless coverage. It is a way to **visualize Wi-Fi network** coverage.

Toner Probe - These devices are used to **locate cables** in a wiring closet. The tone generator is typically placed at the user end, and a probe is waved around in the wiring closet to locate the connection. It will make a distinctive noise when it is near the correct cable.

Punchdown Tool - is used to **connect the exposed ends of a wire into a wiring harness**.

Cable Tester - This device is used to certify that the cable meets the standards of the **wiring code** and to ensure it can be used for communication. It will identify broken wires or missing pin connections.

Loopback Plug - is a special cable that is wired to **transmit and receive on a single connector**. There are loopback plugs for different types of connectors, like USB or ethernet, for testing network interface cards (NICs).

Network TAP - A network test access port (TAP) is a hardware device that creates a copy of **network traffic** for use by monitoring devices without interfering with network traffic. A network TAP can be easily moved from location to location to identify problems.