

# Instructional Terminology

NETWORK SECURITY 15.1200.30



## A

**Acceptable Use Policy (AUP)** - a user's rights and guidelines to access an organization's resources

**Accepted Domains** - an organization's domains that it is responsible for

**Access Control List (ACL)** - a list of rules that control the flow of network traffic

**Access points** - devices that connect to a router/switch/hub and provide WiFi signals in a large building or office

**Access token** - a set of user information that defines their access to network resources during a logon

**Account lockout** - the process of locking a user's account after predefined failed attempts to logon

**Account Operator** - a user assigned the role of creating, managing, and deleting user and user group accounts in a network

**Account Policy** - set of guidelines for creating user accounts and passwords

**Active Desktop** - the use of dynamic HTML, webcasting, etc. to display web pages on a PC using Internet Explorer

**Active Server Pages (ASP)** - web pages with server-side scripting to create dynamic http web pages

**ActiveX** - small programs or add-ons that optimize the speed and size of internet applications

**Adapter Card**- used to create an interface between a computer and the network media/cable; also known as NIC or Network Card

**Adapter Teaming** - use of multiple adapter cards in a device to avoid a single failure point and to create redundancy

**Address Resolution Protocol (ARP)** - used to find the MAC address of a device in a LAN using the IP address/broadcast request/response

**AdHoc** - a small network that is created spontaneously to connect devices without a Wireless Access Point

**Administrator** - a network or device user with maximum control, usually to create, delete, modify, and manage the system

**Advanced Encryption Standard (AES)** - an encryption specification based on the Rijndael block cipher algorithm

**Adware** - a malware that displays advertisements often as a pop-up

**Anti-Passback System** - a security system where a user can't pass their entry card to another person behind them

**Anti-Virus Software** - a software program that prevents, detects, and eliminates malware from a system

**Asset** - a device, system, or software with significant usage and value

**Asynchronous Transfer Mode (ATM)** – a networking standard that uses switching and multiplexing to transmit data, voice, and video at high speeds. A data-link layer protocol that can be used in both local area networks (LANs) and wide area networks (WANs)

**Attack Surface** - parts of a network or computer system that can be exploited for an attack

**Attenuation** - the loss of signal strength from one end to the other

**Authentication** - the process of validating a user to provide access

**Automatic Private IP Addressing (APIPA)** - assigning IP addresses without a DHCP server

## **B**

**Backup** - a redundant or extra copy of system data created for later recovery

**Backup (Differential)** - backing up only the data that has changed since the last full backup; see also Differential Backup

**Backup (Full)** - backing up all the data, new as well as old; see also Full Backup

**Backup (Incremental)** - backing up only the data that has changed since the last full or incremental backup; see also Incremental Backup

**Baiting** - leaving behind malicious software/devices in a public area that a user might load on their device thereby infecting their systems

**Base 3** – a ternary numeral system that has three as its base. Counting can only be done with 0, 1, and 2.

**Base 10** – a decimal number system that uses ten digits from 0 to 9.

**Base 16** – a hexadecimal numbering system with base 16 that can be used to represent large numbers with fewer digits. Includes 16 symbols or possible digit values from 0 to 9, followed by six alphabetic characters (A, B, C, D, E, and F)

**Binary Numbering System** - a number system with base 2, or only two values 0/1; also see Numbering System (Binary)

**Biometric security** - use of physical characteristics such as fingerprints/facial recognition to authenticate users

**Black-Box Testing** - when the tester has zero knowledge of the target system prior to the test; see also Testing (Black-Box)

**Black-Hat hacker** - an unauthorized hacker who intrudes into a system to exploit it for malicious reasons

**Blue Team** - a team of cybersecurity professionals who work internally to stop external attacks from a red team during a system check

**Botnet** - Network of zombies/computers infected by a trojan

**Bottom-Up Approach** – when the priority is to establish a functional network first, focusing on decisions around the hardware, bandwidth, security, etc.

**Bridge** - a network device that interconnects multiple network segments into one

**Bring Your Own Device (BYOD)** - the policy to allow employees to use their personal devices for professional usage, often increases security risks to organizational data/system

**Broadcast Domain** - a network segment where devices can reach each other through broadcast messages

**Brute force** - trying to crack user password by working through all possibilities

**Bus Physical Topology** - a single cable that connects all the devices, and has two endpoints; also called linear topology; see also Physical Topologies (Bus)

## **C**

**Caching Engine** - storage of data in a network device for quicker access in the future

**Cat Cable** – Category cables such as Cat5e, Cat6e, etc. which identify their bandwidth (measured in MHz), maximum data rate (measured in megabits per second), and shielding

**Certificate** - a digital document that identifies a valid user or system

**Chain of Trust** - an ordered list of validation certificates to create a trusted SSL certificate from the root

**Cipher (Cypher)** - steps of a cryptography algorithm to encrypt or decrypt data

**Classful** - IP addresses that use a default subnet mask; ex. Class A: 255.0.0.0, Class B: 255.255.0.0, Class C: 255.255.255.0

**Classless Inter-Domain Routing (CIDR)** - creation of classless IP addresses using variable length subnet masks

**Closed Source Software (CSS)** – software that keeps its source code protected and encrypted so that only the original creators or an IT service desk can access, copy, or modify it

**Cloud** - storage and retrieval of data over the internet instead of local computer storage

**Cloud Storage** - see Cloud

**Cloud-based network controller** - used to automatically move less used data over to cloud storage

**Code of Ethics** - rules to define ethical behavior

**Cold Site Recovery** - recovery site with limited resources and lesser initial cost, but higher time to get the site up and running; see also Recovery (Cold Site)

**Collision** - a situation where two devices on an Ethernet network transmit data simultaneously, resulting in data loss

**Collision Domain** - a network segment where simultaneous data transmissions collide

**Confidentiality** - a responsibility to protect an individual's personal information or an organization's data

**Content Switch** - a Switch that can operate on higher OSI layers and can make forwarding decisions

**Copyright** - protections granted by the government to creators, and inventors for rights to copy, sell, distribute, or use their work

**Cost Analysis** - the process of projecting and analyzing the cost/benefit of a proposed system or network plan

**Crosstalk** - unwanted signals that cause disturbance to the original signals over a network media

**Cryptographic key** - a character string used in cryptography to code or decode a message in a cryptography algorithm

**Cryptography** - the process of encrypting or decrypting data to secure it; also known as Cryptology

**Cyberbullying** - use of technology/internet to bully or intimidate a person

**Cyberwarfare** - the use of technology to attack the network, system, revenue, economy, or data of an adversary/nation

**Cyclic Redundancy Check (CRC)** - an error check value used to determine whether a frame arrived error-free or uncorrupted

## **D**

**Data Integrity** - maintenance of accurate and consistent information/data

**Data remanence** - remnants of data that can be used to recover deleted data using recovery software

**Data wiping** - permanent removal of data from a device using techniques such as data wiping software, degaussing wand, etc.

**Day Zero** - refer to zero-day attack

**Decimal Numbering System** - a number system with base 10, uses digits 0-9; see also Numbering System (Decimal)

**Decryption** - the reverse process of encryption to decode secured data

**Demilitarized Zone (DMZ)** - a subnetwork of an organization that is unsecured and exposed to external services

**Denial of Service (DoS)** - an attack to overwhelm network servers down by sending a large number of false requests, resulting in denial of service to legitimate users

**Divide and conquer network technology tasks** - an algorithm that recursively breaks down a problem into two or more sub-problems of the same or related type until they become simple enough to be solved directly

**DHCP Relay Agent** - a host that relays DHCP requests and responses between a remote DHCP server and the client

**Dial-ups** - use of telephone networks to dial-up and connect to an Internet Service Provider

**Differential Backup** - backing up only the data that has changed since the last full backup; see also Backup (Differential)

**Differentiated Services Code Point (DSCP) value** - the value assigned to the Diffserv field of an IP packet header to prioritize it in a Diffserv protocol

**Diffserv (Differentiated Services)** - a QoS architecture protocol that prioritizes and forwards data packets based on a DSCP value

**Dig** - command line tool to query and troubleshoot DNS problems

**Direct** - a link between two devices via a single cable/connection, or when a (routing) packet source and destination are in the same physical network

**Distributed DoS (DDoS)** - a DoS attack created by using Zombie computers that makes it difficult to trace the origin of an attack

**DNS** - Domain Name System, a directory system to convert website names to IP addresses

**DNS Poisoning** - a TCP/IP attack, where the DNS of a legit site is changed by an attacker, thereby redirecting users trying to access that site to another website

**Domain** - names used in URLs to identify IP addresses; ex. Google.com

**Dumpster diving**- the process of searching for sensitive information in the trash

**Dynamic DNS (DDNS)** - dynamically updating the name server in the DNS when IP addresses are changed

**Dynamic Host Configuration Protocol (DHCP)** - a network protocol which automatically configures devices on networks

**Dynamic IP** - an IP address that changes and is assigned by network

## E

**Eavesdropping** - unauthorized listening to sensitive information

**Electronic Penetration** - a penetration testing where the tester

attacks the organization's computer systems and data

**Encryption** - the process of transforming data into a secured code based on an algorithm or established rules

**Error checking** - techniques used to detect errors in data transmission, such as Parity check, CRC, checksum

**Error codes** - a numeric code used to identify the type of error in data transmission or any other system errors

**Error Correcting** - detecting errors and reconstructing original data in transmission

**EtherChannel** - a port channel architecture to group several physical Ethernet links into one logical link for fast and fault-tolerant connection between network devices

**Ethernet** - connecting devices together in a network as per the IEEE 8023 standard

**Ethernet (568A/B)** - wiring standards used for creating straight-through cables

**Ethernet (Cat 5)** - unshielded cable, max speed 10/100 Mbps, max bandwidth 100 MHz

**Ethernet (Cat 5e)** - unshielded cable, max speed 1000Mbps/1 Gbps, max bandwidth 100 MHz

**Ethernet (Cat 6)** - shielded/unshielded cable, max speed 1000Mbps/1 Gbps, max bandwidth 250 MHz

**Ethernet (Cat 6a)** - shielded cable, max speed 10000Mbps/10 Gbps, max bandwidth 500 MHz

**Ethernet (Cat 7)** - shielded cable, max speed 10000 Mbps/10 Gbps, max bandwidth 600 MHz

**Ethernet (Plenum)** - ethernet cable rated to run in the plenum space of a building

**Ethernet (RJ11)** - used in twisted pair cables for telephone wiring, has 4 connectors

**Ethernet (RJ45)** - used in twisted pair cables, has 8 connectors

**Ethernet (Shielded Twisted Pair)** - copper wiring twisted together and coated with electromagnetic insulation

**Ethernet (Unshielded Twisted Pair)** - Ethernet wiring twisted together to avoid cross-talk or noise

**Ethernet over Power** - used to connect devices with no built Wi-Fi connectivity to the internet

**Ethical Hackers** - refer to White-hat hackers

**Extranet** - an Intranet that allows outside users with partial access

## **F**

**Failover** – a backup operational mode that automatically switches to a standby database, server, or network if the primary system fails or is shut down for servicing

**False Negative** - when a user who should be allowed access is declined access while authentication

**False Positive** - when a user who shouldn't be allowed access is allowed access while authentication

**Fiber** - use of fiber strands to transmit/receive optical signals in a cable

**Fiber (LC Connector)** - Lift-and-click/Little connector, half the size; see also LC Connector Fiber

**Fiber (MT-RJ Connector)** - plastic connector with locking tab, used for single and multi-mode; see also MT-RJ Connector Fiber

**Fiber (Multi-mode)** - cables that transfer data using multiple light paths, cable core is 50-100 microns; see also Multi-mode Fiber

**Fiber (SC Connector)** - Set-and-click/square connector uses a ceramic ferrule for core alignment and prevents light ray deflection; see also SC Connector Fiber

**Fiber (Single-mode)** - cables that transfer data using a single light path, cable core is 8-105 microns; see also Single-mode Fiber

**Fiber (ST Connector)** - push-in and twist/set-and-twist/straight tip connector, used in single and multi-mode cabling; see also ST Connector Fiber

**File Transfer Protocol (FTP)** - used to transfer files over a network

**File Transfer Protocol Secure (FTPS)** - adds Transport layer security to the FTP

**Fingerprinting** - a pre-attack phase where an intruder gathers computer system information such as OS, apps, services, etc.; also known as Footprinting

**Firewall** - a device/network security system to monitor and manage incoming and outgoing traffic

**Forensic investigation** - gather evidence and identify the methods used in an incident/attack

**Frame relay** – a protocol that defines how frames are routed through a fast-packet network based on the address field in the frame

**Full Backup** - backing up all the data, new as well as old; see also Backup (Full)

**Fully Qualified Domain Name (FQDN)** - hostname and domain names separated by periods

## G

**Gigabit Interface Converter (GBIC) Transceiver** - a large transceiver used for Gigabit media; see also Transceiver GigaBit Interface Converter (GBIC)

**Grayware** - a legitimate software that also contains malicious content that a user might be unaware of

**Grey-Box Testing** - when the tester has partial knowledge of the target system prior to the test; see also Testing (Grey-Box)

**Grey-Hat hackers** - an unauthorized hacker who intrudes into

systems, but without malicious intent, often to disclose system vulnerabilities to authorities or law enforcement

## H

**Hacker** - a person who breaks into another person's computer or network with a malicious intent

**Hacking** - unauthorized intrusions into a computer or network system

**Hardware locks (1)** - device required to make certain software operable on a computer, i.e. dongles

**Hardware locks (2)** - locks, locked cases, cabinet locks, cable locks, etc. used to prevent device theft

**Hexadecimal Numbering System** - a number system with base 16, uses digits 0-9, A; see also Numbering System (Hexadecimal)

**Homegroup** - a group of computers connected to share files, printers, or data

**Honeynet** - a network of honeypots

**Honeypot** - a device that attracts intruders by displaying vulnerabilities

**Hot Site Recovery** - a recovery site with complete duplication of original site resources, ensures the fastest disaster recovery; see also Recovery (Hot Site)

**HTTPS** – an extension of HTTP, used for secure communications

**Hub** - a network device to connect devices, operates on a physical layer level

**Hybrid topology** - a network structure that combines two or more different types of topologies to take advantage of their strengths and minimize their weaknesses. Ex. Star Ring, Mesh

**HyperText Transfer Protocol (HTTP)** - an application layer protocol to transfer hypertext messages between clients and servers

## **I**

**ifconfig** - command line tool used to manage IP addresses and control network connections

**Incident response** - actions taken to deal with an incident during and after the incident

**Incremental Backup** - backing up only the data that has changed since the last full or incremental backup; see also Backup (Incremental)

**Indirect** - (routing) data packet goes from router to router to reach the destination

**Intellectual Property** - creations/inventions owned by a copyright holder

**Internet** - a collection of different networks that collectively connect and exchange information

**Internet Control Message Protocol (ICMP)** - an Internet layer protocol used to detect errors in network communications

**Internet Message Access Protocol (IMAP/IMAP4)** - used to access emails over the internet from email servers

**Intranet** - a local or private network created using WWW for communication within an organization

**Intruder Detection System (IDS)** - a network device that detects any suspicious activity on the network

**Intrusion Prevention System (IPS)** - a device/system that prevents an attack before it penetrates the rest of the network

**IP address** - a numeric label assigned to a device that uses Internet Protocol for connections/communications Ex 12326523

**Ipconfig** - a Windows command line utility used to manage network connections on devices, usually displays current TCP/IP network configurations

## **K**

**Keepalive Signal** - a signal that devices transmit over a network medium to check if the link is alive or active

**Kerberos** - a free authentication protocol for client/server applications

**Key fob** - a small device used for two-factor authentication, can be attached to a key chain

## **L**



**LC Connector Fiber** - Lift-and-click/Little connector, half the size; see also Fiber (LC Connector)

**Lightweight Directory Access Protocol (LDAPS)** - a network services protocol that uses TCP port 636

**Load Balancing** - the process of distributing network traffic across a group of servers (also known as server farms)

**Load Tester** - a server tool used to test and estimate the load on the server or service

**Local** - software/storage or anything on-site or on-device

**Local area network (LAN)** - a small area network of devices that connects users and applications in close geographical proximity such as in the same building

**Local backup** - a data backup done on a storage device maintained closer to the device or connected through the LAN

**Log file** - a file that documents details of specific activities performed on a system, i.e. backlogs, repair logs, etc.

**Logical Topologies** - the ways a network is set up physically, but the messages are sent out in a different logical topology manner; see also Physical Topologies

## **M**

**Malware** - a software created to perform malicious activities

**Managed Switch** - a switch with advanced control features such as managing, and controlling LAN settings; see also Switches (managed/unmanaged)

**Management Information Base (MIB)** - a database of network elements that are managed by SNMP protocol in a complex network

**Man-in-the-Middle (MitM)** – when an attacker intercepts communication between two systems and uses it to gain access or falsify/edit the communications

**Mantrap** - a secured entrance with two doors, where once a user enters the first door, they can access the second door only after authentication

**Masquerading** - pretending to be an authorized user to gain access

**Media Access Control (MAC) Address** - a unique identifier embedded permanently into a NIC

**Mesh Physical Topology** - a topology where all devices connect, like a Point-to-point setup; see also Physical Topologies (mesh)

**Metropolitan Area Network (MAN)** - a collection of networks within a Metropolitan area

**Modem** - A modulator/demodulator is a device that connects devices, and converts computer signals to/from audio signals

**MT-RJ Connector Fiber** - plastic connector with locking tab, used for single and multi-mode; see also Fiber (MT-RJ Connector)

**Multicast** - one-to-many devices or many-to-many devices data transmission in a network

**Multilayer Switch** - refer to Content Switch

**Multiprotocol Label Switching (MPLS)** – a networking technology that routes traffic using the shortest path based on “labels,” rather than network addresses, to handle forwarding over private wide area networks

**Multi-factor authentication (MFA)** – authentication that requires users to verify multiple factors before they can access a service, also known as 2FA

**Multi-mode Fiber** - cables that transfer data using multiple light paths, cable core is 50-100 microns; see also Fiber (Multi-mode)

## **N**

**Name Server Lookup (Nslookup)** - a command line utility used to see the DNS records for a domain

**Nbtstat** - a command line utility used to diagnose NetBIOS name resolution issues

**Netiquette** - the appropriate way to act over the internet

**NETstat** - a command line utility used to see TCP connections, routing tables, and other network interface information

**Network Access Protection (NAP)** - a set of components that administrators use to regulate network access

**Network Address Translation (NAT)** - used on a router to map private IP addresses to a public IP address

**Network Attached Storage (NAS)** - a dedicated file storage used to store and retrieve data for a network’s user group

**Network Basic Input/Output System (NetBIOS)** - operates as the Session layer for applications on different devices to communicate over a LAN

**Network Cards** – allow a computer to exchange data with a network

**Network ID** - an identifier for the network an IP address belongs to (32-bit in IPv4)

**Network interface card (NIC)** - necessary for internet connection - wired or wireless

**Network monitor** - a system of consistent monitoring of a network and informing network administrators of any issues

**Network Settings** - the settings used to view and manage the network connections on a device

**Network Topology** – the physical and logical arrangement of nodes and connections in a network

**NIC Teaming** - Ethernet Bonding, the grouping of two or more physical connections logically to the same network for faster data transmission

**Nonrepudiation** – prevents users from denying their participation in a transaction or communication and ensures no entity can claim a transaction didn’t happen when it did, or vice versa

**Numbering System (Binary)** - a number system with base 2, or only two values 0/1; also see Binary Numbering System

**Numbering System (Decimal)** - a number system with base 10, uses digits 0-9; see also Decimal Numbering System

**Numbering System (Hexadecimal)** - a number system with base 16, uses digits 0-9, A-F; see also Hexadecimal Numbering System

**Numbering System (Octal)** - a number system with base 8, uses digits 0-7; see also Octal Numbering System

## **O**

**Octal Numbering System** - a number system with base 8, uses digits 0-7; see also Numbering System (Octal)

**Open Systems Interconnection (OSI) Model** - an ISO framework created to explain network system communications

**Operations Penetration** - a penetration testing where an authorized attacker tries to gather information through phishing attacks

**Organizationally unique identifier (OUI)** – a 24-bit number that uniquely identifies a vendor, manufacturer, or other organization

## **P**

**Packet Sniffer** - a software or hardware tool used to record or analyze packets transmitted over a network

**Passive** - a type of security attack where network traffic and data are monitored, recorded, and analyzed, and no changes are made to them

**Passphrase** – a sequence of words or other text used to control access to data or a computer system or program

**Passphrase generator** – uses complex algorithms to create nonsensical combinations of characters which are difficult even for sophisticated software to break

**Patch** - a change done to a software or application to fix bugs, vulnerabilities, or enhance performance

**Patch management** - the process of creating, installing, and testing patches on systems to address bugs, vulnerabilities, and errors

**Patch panel** - a hardware device that organizes/joins networks or devices together with its multiple ports/jacks

**Patent** - a license that ensures inventors complete ownership of their invention

**Penetration Testing** - a simulated attack to test the security system and detect vulnerabilities of a network or organization

**Phishing** - a malicious attack that looks legitimate, used to trick users into providing sensitive information or installing malware

**Physical Penetration** - a penetration testing where an authorized physical attacker tries to enter or break into the organization's perimeter, access systems, and network

**Physical Topologies** - the connection infrastructure and cables used to connect physical devices in a network; see also Logical Topologies

**Physical Topologies (Bus)** - a topology with a single cable that connects all the devices, and has two endpoints, it's also called linear topology; see also Bus Physical Topology

**Physical Topologies (Mesh)** - a topology where all devices connect, like a Point-2-point setup; see also Mesh Physical Topology

**Physical Topologies (Ring)** - a ring-like connection where each device has two neighboring connections; see also Ring Physical Topology

**Physical Topologies (Star)** - a topology where each device connects to a central node/hub; see also Star Physical Topology

**Piggybacking** - entering a secured area by following an authorized user

**Ping** - a command line utility that tests the reachability or connectivity of the host to an IP address

**Piracy** - the crime of using/copying/distributing someone else's intellectual property

**POP3** - the commonly used version of POP

**Port Aggregation Protocol (PAGP)** - a Cisco proprietary network protocol to aggregate Ethernet ports on network devices

**Port forwarding** – a technique that redirects network traffic from one address and port number combination to another; also known as port mapping

**Post Office Protocol (POP)** - an application layer protocol that is used for email retrieval from an email server

**Power over Ethernet (Injectors/switch)** - a switch that is used to inject power to a PoE cabling for the devices connected to it

**Power over Ethernet (PoE)** - systems that pass over electric and digital data on a single Ethernet cable to devices such as WAPs, VoIP phones, etc.

**Principle of Least Privilege** - level of access provided to users only based on need

**Privacy** - the ability of an individual or organization to choose what data or information is shared with third parties

**Protocol** - set of rules or standards for network systems and communications

## Q

**Quad (SFP) or QSFP Transceiver** - used for data communication applications; see also Transceiver (QSFP)

**Quality of Service (QoS)** - a network feature that ensures data delivery and high-priority applications run smoothly even under limited capacity

## R

**Radio Frequency Interference (RFI)** - signals caused by devices such as cordless phones, and microwave ovens that interfere with the network

**Ransomware** - a malware that denies access to infected systems and demands a ransom to remove restricted access

**Recovery (Cold Site)** - recovery site with limited resources and lesser initial cost, but higher time to get the site up and running; see also Cold Site Recovery

**Recovery (Hot Site)** - a recovery site with complete duplication of original site resources, ensures the fastest disaster recovery; see also Hot Site Recovery

**Recovery (Warm Site)** - a recovery site with only the critical hardware and data; see also Warm Site Recovery

**Recovery Site** - a site or location that can be relied upon in case the main site faces issues or failures

**Red Team**- a team of cybersecurity professionals that attacks a system externally to detect vulnerabilities and is defended by a blue team

**Remote backup** - the process of backing up data and files on a remote location such as the cloud through an online connection

**Repeater** - a replicating network device that simply regenerates and relays signals to avoid transmission loss

**Replay** - similar to MitM attack, but used to record the intercepted information and replay it back to the destination devices

**Reverse Address Resolution Protocol (RARP)** - process of finding the IP address using the MAC address

**Ring Physical Topology** - a ring-like connection where each device has two neighboring connections; see also Physical Topologies (Ring)

**RJ11** - a type of 4-wire connector used in twisted pair cabling for telephone connections

**RJ45** - a type of 8-wire connector used in twisted pair cabling for Ethernet and Ring token connections

**Rollback** - the process of reverting a system to its previous or original version

**Rootkits** - a malware program used by hackers to gain administrative-level access to a device

**Routers** - a data/packet forwarding network device that navigates a path for the packets

## **S**

**SC Connector Fiber** - set-and-click/square connector uses a ceramic ferrule for core alignment and prevents light ray deflection; see also Fiber (SC Connector)

**Scareware** - to make users believe that they have malware with the intent to make them purchase fake antivirus software

**Secure Copy (SCP)** - a file transfer protocol that uses SSH to transfer files securely

**Secure File Transfer Protocol (SFTP)** - a file transfer protocol that uses SSH for secure data transfer

**Secure Shell (SSH)** - a network protocol used for secured access and communication over an unsecured network

**Secure Sockets Layer (SSL)** - a security protocol to provide encrypted links over network/internet connections

**Server** - any computer providing services to other computers, but usually the term server implies a powerful computer that supports a number of users simultaneously in a network

**Service pack** - a group of updates to software including patches, bug-fixes, and enhancements released together

**Shoulder surfing** - looking over the shoulder of someone's device for information

**Simple Mail Transfer Protocol (SMTP)** - a standard protocol for email communication

**Simple Network Management Protocol (SNMP)** - a protocol to manage complex networks

**Single-mode Fiber** - cables that transfer data using a single light path, cable core is 8-105 microns; see also Fiber Single-mode

**Small Form-factor Pluggable (SFP) Transceiver** - a mini-GBIC; see also Transceiver Small Form-factor Pluggable (SFP)

**Social Engineer** - an attacker who uses social engineering techniques such as phishing, spamming, or tailgating to gain access

**Social Engineering** - when an attacker tries to gain access to a system by tricking users into providing access information

**Software-Defined Wide Area Network (SD-WAN)** – separates networking hardware from its control mechanism and uses a centralized interface to deliver virtualized resources to WAN connections

**Spam** - a junk email used for advertising, or sending malicious contents

**Spanning Tree Protocol (STP)** - a network protocol that runs on layer 2 devices (switch, bridge) to ensure loop-free communications

**Spear-Phishing** - the act of creating phishing attacks targeted towards a specific target or individual in an organization

**Spoofing** - an attack where a computer pretends to be another device to gain resource access, usually by forging MAC or IP addresses

**Spoofing (ARP)** - uses spoofed ARP messages, mostly to create DoS attacks; also known as ARP poisoning,

**Spoofing (DNS)** - an attacker resolves a domain to a fake or invalid IP address; also known as DNS spoofing

**Spoofing (IP)** - attacking device spoofs the IP address of the IP packet

**Spoofing (MAC)** - attacking device spoofs the MAC address of a valid host

**Spyware** - a malware similar to adware, but collects and sends browsing or sensitive user data to the attacker without the user's knowledge

**Star topology** – a network topology where all devices connect to a central node or hub and act as clients to the central node which acts as a server

**ST Connector Fiber** - push-in and twist/set-and-twist/straight tip connector, used in single and multi-mode cabling; see also Fiber (ST Connector)

**Star Physical Topology** - a topology where each device connects to a central node/hub; see also Physical Topologies (star)

**Stateful Protocol** - a protocol that requires the server to save status and session information

**Stateless Protocol** – a protocol that does not require the server to retain information or session details

**Static IP** - an IP address that is assigned permanently to a device

**Subnet** - a subnetwork or a logical division of an IP network

**Subnet Mask** - a numeric pattern that separates the network ID from the host address

**Subnetting** - the process of creating logical divisions of an IP network to increase routing efficiency and privacy

**Supernetting** - coming two or more networks into one

**Switches (managed/unmanaged)** - a network device that connects systems and redirects data on a network; see also Managed Switch and Unmanaged Switch

**Syn Flood** - an attack where multiple SYN requests flood a web server, thereby denying TCP sessions to valid users

**SYN request** - initial request sent to request a TCP session with a web server

## **T**

**Tailgating** - an act of gaining access to restricted areas and systems by following an authorized user

**Tarpit** - a device that attracts attackers and makes them 'stuck' for a duration of time; also known as a sticky honeypot

**Telnet** - a client-server protocol to start a bidirectional/command line text interaction over a LAN or Internet

**Temporal Key Integrity Protocol (TKIP)** - an IEEE 80211 WLAN security/encryption protocol

**Terminator** - endpoints on the main cable of a Bus topology that absorbs signals preventing back-and-forth relay

**Testing (Black-Box)** - when the tester has zero knowledge of the target system prior to the test; see also Black-Box Testing

**Testing (Grey-Box)** - when the tester has partial knowledge of the target system prior to the test; see also Grey-Box Testing

**Testing (White-Box)** - when the tester has full knowledge of the target system prior to the test; see also White-Box Testing

**Thick client** - a fully functional computer system that can operate independently

**Thin client** - an optimized computer system that depends on remote servers for major functions such as data storage

**Throughput Tester** - a tool used to measure the amount of data that can be transmitted through a network in a given duration

**Time-to-Live (TTL)** - a counter or duration set on an IP packet or DNS record before it is discarded; i.e. maximum router-hops a packet can make

**Token** - a physical or logical authentication device

**Tombstone** - a marker that relays to the servers to delete their copies of any data that has been deleted from a local directory

**Top Down Approach** – an approach based on starting a network design beginning from the topmost layer and moving down

**Top-Level Domain (TDL)** - the last part of a domain name; i.e. com, net, gov, etc.

**Topology** - the physical or logical layout of a network, usually the way devices are connected; i.e. Bus, Ring, Star, etc.

**Topology Table** - a table with information about all the routers in a network and their routes, like a network roadmap

**Traceroute** - another name for the tracert command

**Tracert** - a command line command that shows the path a packet follows to reach from a source to a destination

**Traffic Shaper** - a network device capable of traffic shaping

**Traffic Shaping** - a bandwidth management technique, used to slow low-priority network packets to transmit high-priority traffic; also known as Packet Shaping

**Transceiver** - a device that transmits and receives data

**Transceiver (XFP)** - similar to SFP, used for 10 GB networks; see also XFP Transceiver

**Transceiver GigaBit Interface Converter (GBIC)** - a large transceiver used for Gigabit media; see also GigaBit Interface Converter (GBIC) Transceiver

**Transceiver Quad (SFP) or QSFP** - used for data communication applications; see also QSFP Transceiver

**Transceiver Small Form-factor Pluggable (SFP)** - a mini-GBIC; see also Small Form-factor Pluggable (SFP) Transceiver

**Transmission Control Protocol (TCP)** - a standard for establishing network connections for data transmission

**Transmission Control Protocol/Internet Protocol (TCP/IP)** – a suite of protocols to connect and transmit data over the Internet

**Transmission Media** - the medium through which data transmits from one device to another; i.e. cables, fiber optic, etc.

**Transport Layer** - the 4th layer of the OSI model responsible for reliable network communications

**Transport Layer Security (TLS)** - a security protocol that provides secured and tamper-proof message transmission

**Transport Protocol** - standards or protocols that provide data communication between systems; i.e. TCP/IP

**Transport Rules** - policies or guidelines that filter, process, and modify all emails in an exchange/corporate organization

**Trivial File Transfer Protocol (TFTP)** - a simple file transfer protocol between two TCP/IP devices, initially used for reading/writing files using a remote server

**Trojan Horse** - a malware program that looks useful but is malicious

**Trolling** - the act of provoking users online often through offensive posts, and arguments

**Trunk cable** - the main cable that connects to all the nodes/ devices on a physical Bus topology



**Trust (one-way/two-way)** - permission granted to accounts in one domain to access resources of another domain (one-way) and vice-versa (two-way)

**Tunnel** - a logical link created through encryption protocols to transfer private data over public networks safely

**Tunneling** - a communication protocol used to transfer private network data through a public network Ex. VPN

**Two-step authentication** – see Multi-Factor Authentication

## U

**Unicast** - a network transmission from a source host to a single destination host

**Uniform Resource Locator (URL)** - a combination of domain name and other necessary information that creates a web address to a page or a resource; i.e. <https://www.google.com>

**Universal Naming Convention (UNC)** - a naming convention for identifying network resources or servers; i.e. \\servername\path

**Universal Serial Bus (USB)** - a network media that connects a computer to external devices such as keyboards, mice, etc.

**Unmanaged Switch** - a basic switch with plug-n-play functionality; see also Switches (managed/unmanaged)

**Unshielded Twisted Pair (UTP)** - a type of copper cabling used in LANs and telephone networks

**Upgrading** - replacing a software or hardware product with a newer and better version of itself

**URL Hijacking** - a situation when an attacker buys domains that a user might hit due to a typo while reaching a valid website; also known as Typo squatting,

**User** - a network member provided with access to the components based on their account privilege

**User Datagram Protocol (UDP)** - a connectionless and unreliable Transport Layer protocol

**User profile** - a default (customizable) profile that holds the system components specific to a user, created when a user logs on to a system

**Username** - a name for a user or account that identifies them over a device or network group

## V

**Variable Length Subnet Masking (VLSM)** - creating custom subnets to divide IP addresses

**Vector-based Routing Protocol** - a routing standard that creates a routing table based on distance vectors (hop-count) from the nearest routers

**Virtual Device Driver (VDD)** - a software driver that provides a buffer between the hardware and software, and has direct access to the kernel; are also known as VxDs

**Virtual link** - an alternative USB-C link that will provide data, power, and graphics through a single connection to a VR headset

**Virtual Local Area Network (VLAN)** - a custom network that combines multiple wired/wireless networks into a single logical network

**Virtual Local Area Network (VLAN) Hopping** - an attack where an attempt is made to access traffic on a restricted VLAN

**Virtual Memory Manager (VMM)** - a Windows NT component that manages and allocates virtual or physical memory allocation to applications

**Virtual Private Network (VPN)** - used to create secured connections to other networks over the Internet

**Virtual Server** - creation of multiple virtual machines on a physical server

**Virtualization** - creation of virtual resources like operating system, storage, desktop, server, etc.

**Virus** - a malware that attacks a system by replicating when activated, transferred through email, USB drives, file transfer, etc.

**VoIP** - a technology that provides voice service over computer networks, compared to traditional telephony services

**Vmware** – software that allows a user to run a virtual computer on a physical computer as well as providing additional networking capabilities

## **W**

**Warm Site** - a backup work location that can be used to continue uninterrupted operation in case the primary site is compromised/affected for an organization

**Warm Site Recovery** - a recovery site with only the critical hardware and data; see also Recovery (Warm Site)

**White-Box Testing** - when the tester has full-knowledge of the target system prior to the test; see also Testing (White-Box)

**White-hat hacker** - an authorized hacker who works with an organization to help strengthen the latter's security system; also known as ethical hackers

**Wide Area Network (WAN)** - a network connecting users and applications in geographically dispersed locations (across the globe)

**WiFi Protected Access (WPA)** - a protocol for secured wireless networks

**WiFi Protected Access (WPA2)** - a protocol that adds security to WPA for stronger data protection and access control

**Wired** - uses an Ethernet port to connect to the internet (RJ 45)

**Wired Equivalent Protocol (WEP)** - a security protocol in IEEE standard 80211b, to provide security and privacy to WLAN

**Wireless** - uses Wi-Fi radio networking

**Wireless Application Protocol (WAP)** - a communication protocol used to access the internet by mobile or cellular devices

**Wireless Wide Area Network (WWAN)** - uses mobile telecommunication cellular network technologies such as 2G, 3G, 4G, 5G

**Workgroup** - a group of systems that share data over a network

**World Wide Web (WWW)** - a collection of hypertext documents/information that are accessible through the HTTP protocol; also known as the web

**Worm** - self-replicating malware, attacks network operations, and spreads by exploiting software vulnerabilities, doesn't need an activation mechanism

## **X**

**XFP Transceiver** - similar to SFP, used for 10 GB networks; see also Transceiver (XFP)

## **Z**

**Zero Configuration networking (Zeroconf)** - a technology where devices can automatically connect over a network, without any manual configuration

**Zero-Day attack** - an attack that exploits a system's vulnerabilities that the vendor is unaware of

**Zombie** - a device infected by a trojan, and controlled by a remote master

**Zone** - a part of DNS that is reserved for a specific server

**Zone Transfer** - the process of copying a zone file of a DNS server to another DNS server