- Identify the Transmission Control Protocol/Internet Protocol TCP/IP model
- Identify the Open Systems Interconnection (OSI) model
- Describe the relationship between the OSI layers and the TCP/IP layers
- Describe the data flow in the OSI model
- Identify the types of basic network media
- Describe the types of wired and wireless devices for networking
- Explain distance limits of wireless media
- Identify common networking commands
- Identify various network types
- Describe various network topologies
- Describe diagrams of various network topologies
- Describe various types of network architecture
- Explain the differences between peer-to-peer and client/server architecture
- Describe the fundamentals of cloud computing
- Explain the role of virtualization in cloud computing
- Describe how cloud computing supports high availability

Unit 2 Overview

This unit introduces working with TCP/IP and OSI models. The TCP/IP model is the common set of protocol standards that permit the appropriate transmission of data. The TCP/IP model consists of an application layer, transport layer, network layer, and network interface layer. The OSI model is used to enable the efficient transmission of data among hosts on a network. The model was developed by the International Organization for

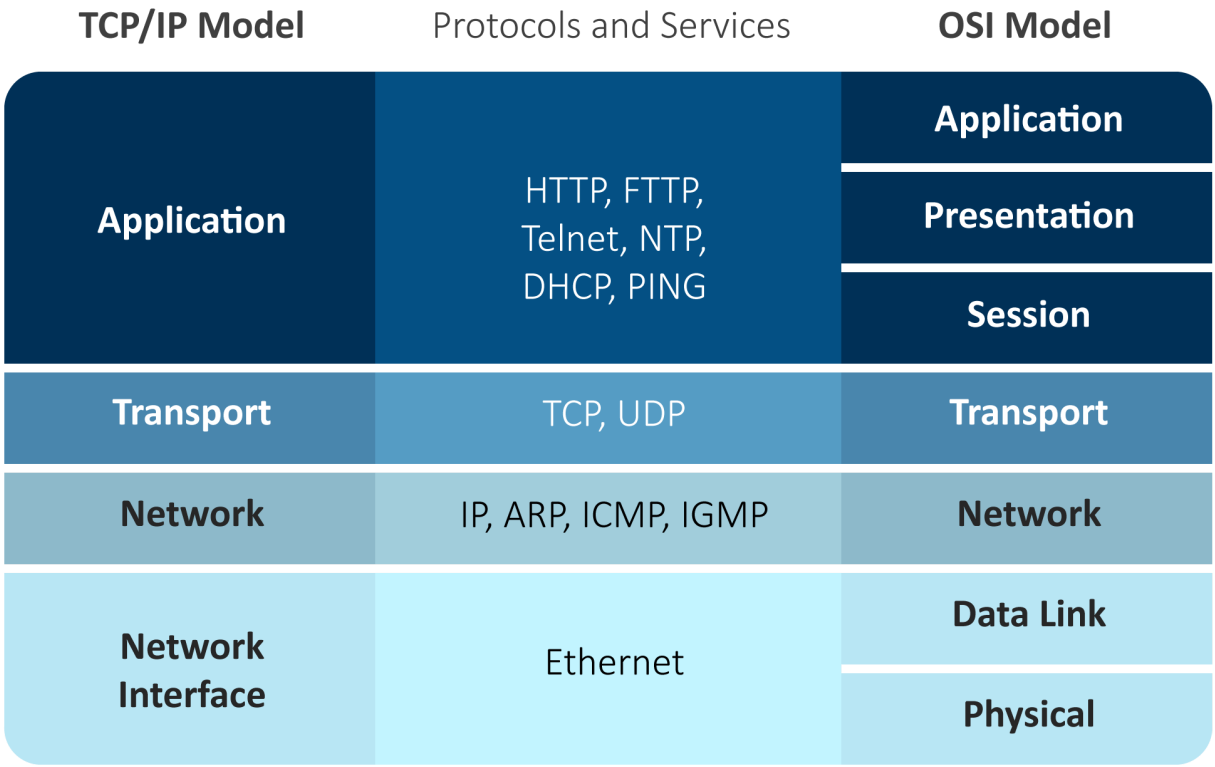
Standardization. The OSI model consists of an application layer, presentation layer, session layer, transport layer, network layer, data link layer, and physical layer.

This section will allow you to further explore and compare the TCP/IP and OSI models. You will gain a detailed understanding of each model's applications and uses. You will apply these models to basic network components, network types and topologies, and network architectures as well as to virtual and cloud computing platforms.

TCP/IP and OSI

The **TCP/IP** and **OSI** models describe a set of procedures that sends data from one host to another. This can be done over the internet, a network, or any other form of communication.

The image below is a comparison chart showing aspects of the two models.



The TCP/IP model covers the same networking aspects found in the OSI model but in fewer layers. The OSI model was developed as a standard set by ISO (International Standard Organization) and provides greater granularity of networking assignments within the model. TCP/IP was developed by the Department of Defense (DoD). OSI Model 1. Physical 2. Data Link 3. Network 4. Transport 5. Session 6. Presentation 7. Application TCP/IP Model 1. Network Interface a. OSI Layer 1 (Physical) b. OSI Layer 2 (Data Link) 2. Network a. OSI Layer 3 (Network) 3. Transport a. OSI Layer 4 (Transport) 4. Application a. OSI Layer 5 (Session) b. OSI Layer 6 (Presentation) c. OSI Layer 7 (Application)

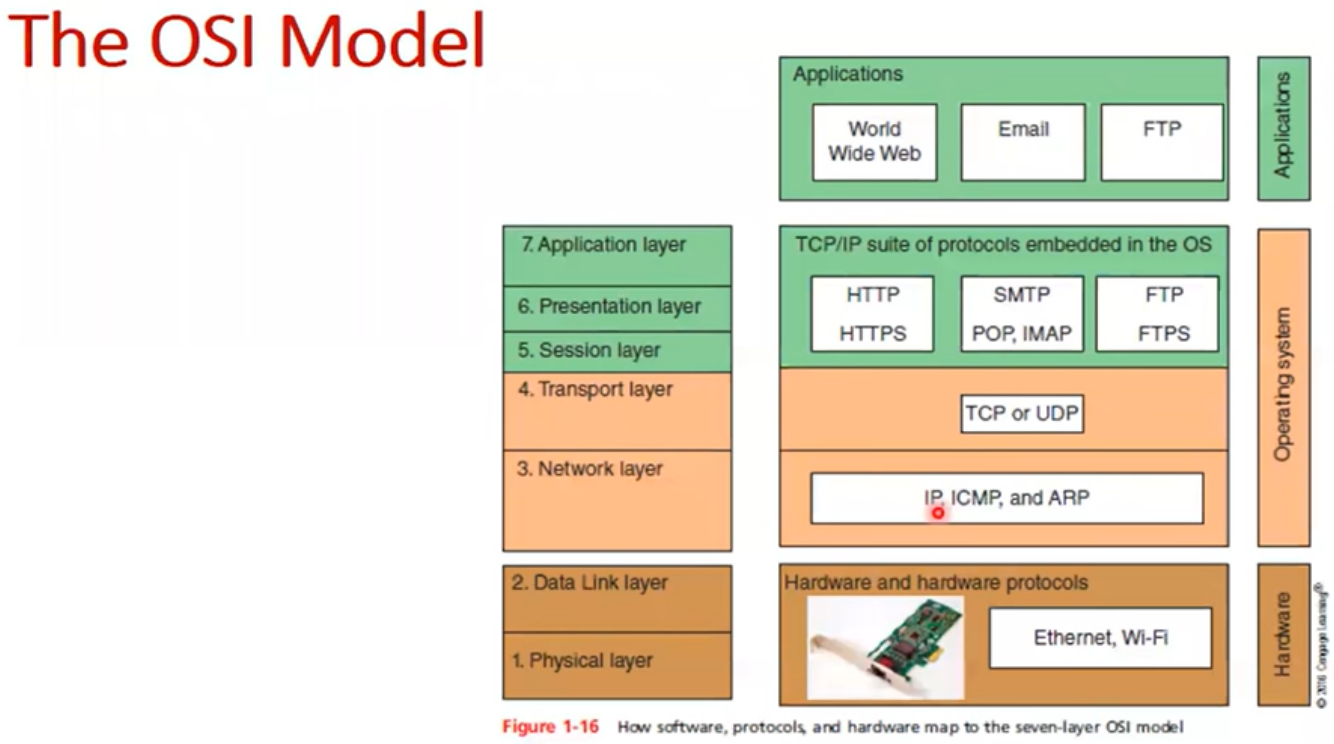
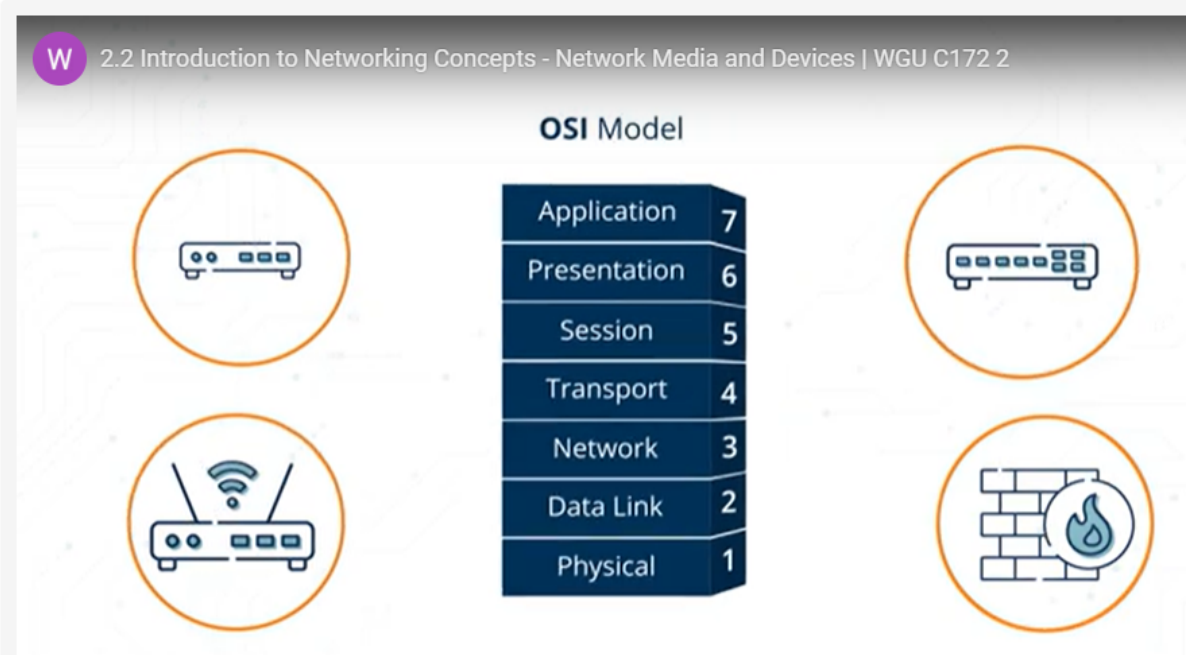
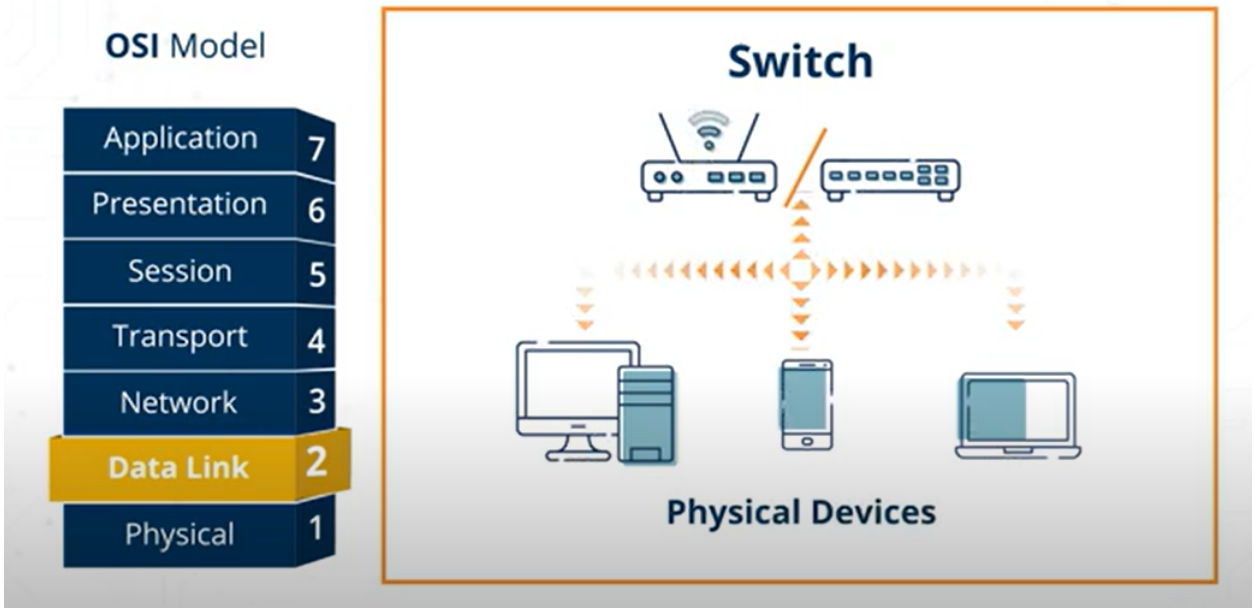


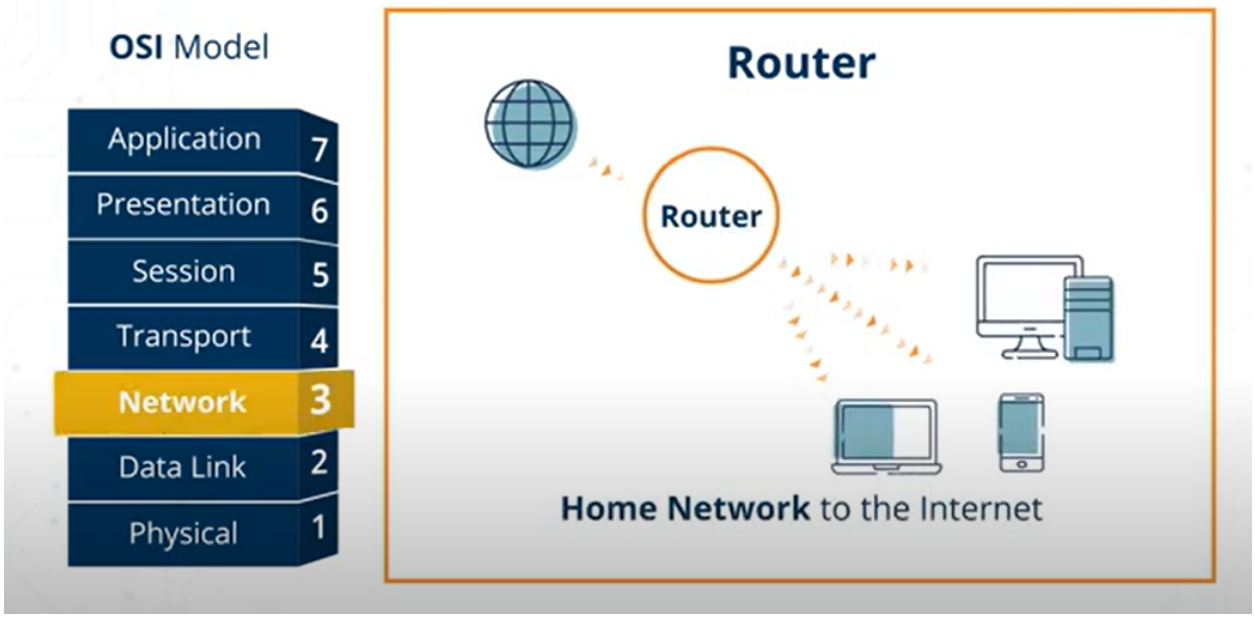
Figure 1-16 How software, protocols, and hardware map to the seven-layer OSI model

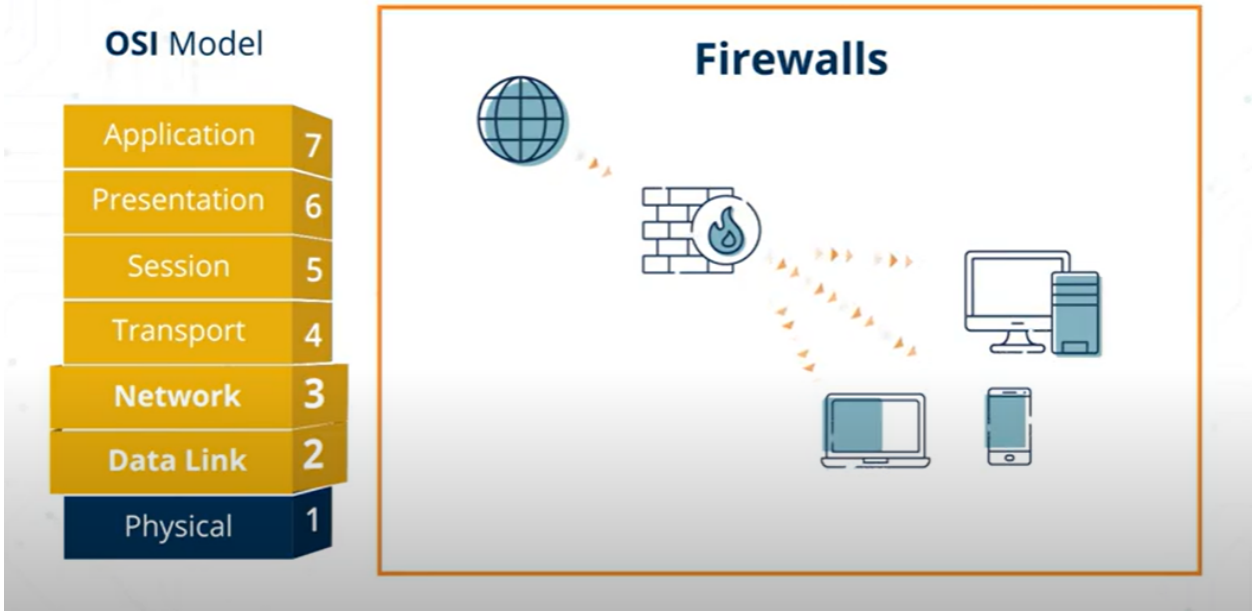
Devices in Network

Network Media and Devices

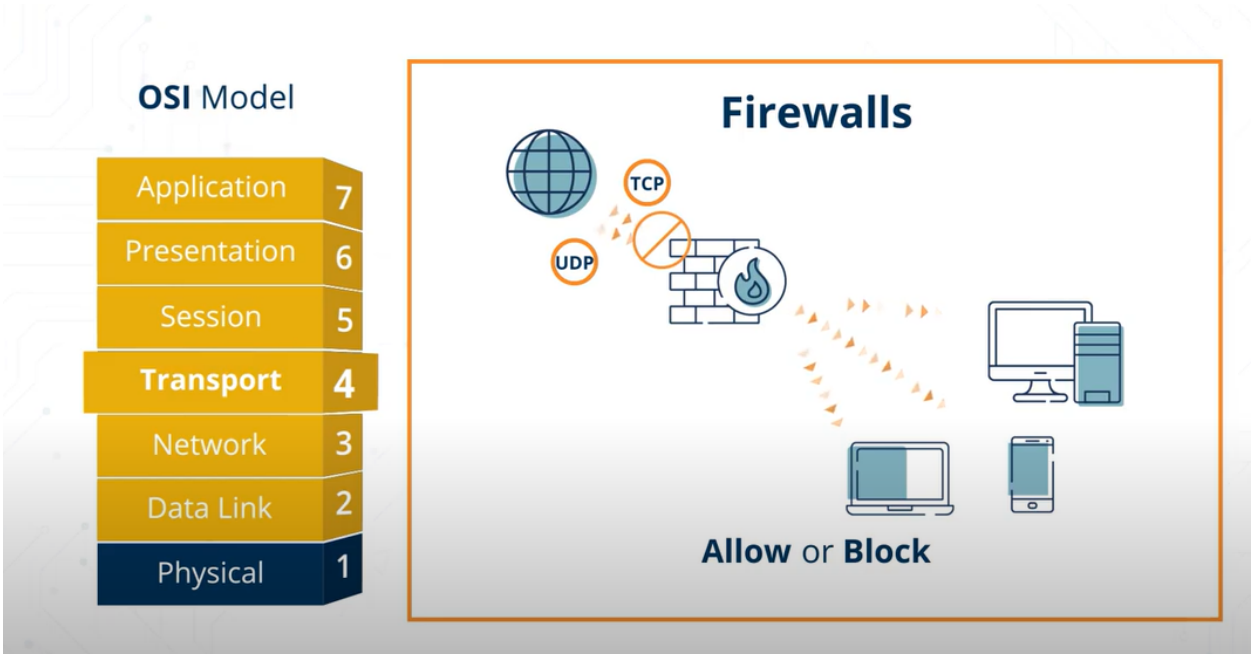








Can be in those layers



Firewall Rule
ACL
Firewall check in Windows

S/w
H/w firewall FortiGate , F5

Basic Network Commands

Basic Network Commands

Basic Network Commands

Watch the following videos to learn more about basic network commands.

Networking Commands (6:06)

Basic Network Commands (4:32)

Networking Commands

0:00 / 6:07

Press UP to enter the speed menu then use the UP and DOWN arrow keys to navigate the different speeds, then press ENTER to change to the selected

Basic Network Commands

Ping

Ping is one of the most basic tools for testing connectivity to other hosts. It sends an Internet Control Message Protocol (ICMP) echo request to a host and listens for the reply. If a reply is received, it will display the time it took and the time to live (TTL) left. Ping has many options for setting attributes of the request, like the maximum TTL, IPv4/IPv6, and the number of requests to send. Ping is useful in troubleshooting connectivity with other devices. If a

reply is not received, you will receive a timeout message, which could indicate connectivity issues, firewall issues, or both issues with the other device. In addition, due to the time to get a response, the latency between two devices can be measured, enabling a network engineer to troubleshoot performance problems or a network architect to determine where to place devices to minimize response time to other systems and users.

Traceroute/Tracert

Traceroute and ***Tracert*** are used to trace the route an IP packet takes to a destination. It displays each hop (next router) in a numerical list with the hop's IP address and the time it takes to receive the packet. The command traceroute is used for Linux systems and tracert is used for Windows systems. It can be useful in determining where a ping fails, troubleshooting performance issues, and other aspects regarding connectivity.

Tracepath

Tracepath is similar to traceroute or tracert in that it displays the path taken by a packet from its source to its destination. Tracepath is useful because it can be used by any user instead of needing superuser privileges. It is primarily used in Linux.

Ipconfig

Ipconfig (internet protocol configuration) provides the user with the IP, subnet mask, and default gateway for each network adapter by default with the /all option information, such as MAC address, DHCP status, and lease information. The command ipconfig/release can be used to release all connections and renew all adapters. It is primarily used in Windows.

Ifconfig

Similar to ipconfig, ***ifconfig*** is used to configure the kernel network interfaces. It is implemented at the time of booting to configure the necessary interfaces. Once the interfaces are configured, it is used for debugging or tuning the system. It is primarily used in Linux.

ARP

ARP (Address Resolution Protocol) displays the IP to physical (MAC) address mappings for hosts that have been discovered in the ARP cache. ARP can be used to add, remove, or modify entries in the ARP cache. The hosts need to be on the local network, as these addresses are discovered by broadcasting to everyone on the network and noting the reply from the owner; broadcast traffic is not allowed through a router so that the system will maintain the MAC address of the router.

Netstat

Netstat (network statistics) displays information about active ports and their state and can be useful in troubleshooting and capacity management. The command netstat -r displays routing information for network adapters. It is available in Windows, MacOS, and Linux.

Nslookup

Nslookup (name server lookup) displays information for displaying DNS information and troubleshooting DNS problems. It is useful in displaying names to IP address mappings.

DIG

DIG (domain information groper) is a command used to query the DNS name servers. It is helpful in troubleshooting DNS problems. It is also used for lookups and will display answers from the query. It is a replacement for nslookup.

Whois

Whois is a tool most often used to look up who owns a domain or block of IP addresses on the internet, including name, email address, and physical address. However, there are many privacy options that hide this information from being returned. It is primarily used in Linux.

Route

Route can be used to display the current route tables on a host. Route can also be used to add or remove routes. This is used by the local host to determine where to send traffic (0.0.0.0 means the default gateway, the router to send things to if not otherwise defined in the routing table).

SCP

The ***SCP (Secure Copy Protocol)*** command is used to securely copy files between servers, leveraging SSH (secure shell) for authentication and encryption.

FTP

FTP (File Transfer Protocol) copies the file from one host to another host. The data is unencrypted. If encryption is needed, FTPS uses SSL/TLS (Secure Sockets Layer, replaced by Transport Layer Security; the same encryption used in https). Transfer uses TCP (Transmission Control Protocol)

for reliability and is often used on the internet and other wide-area networks, where errors may be more common.

TFTP

TFTP (Trivial File Transfer Protocol) transfers a file from either a client to a server or from a server to a client using UDP (User Datagram Protocol) instead of TCP, and so it is usually used on reliable (local) networks.

Finger

Finger displays information about a user or users on a remote system, including things such as last login time and username. It is primarily used in Linux.

Nmap

Nmap (Network Mapper) scans networks to see what it can find in terms of hosts and open ports (including well known ones for many applications). It is commonly used to determine what is deployed on a network for vulnerability analysis, security scans, and related activities. Nmap is not native to either Linux or Windows but can be downloaded for free and used with both.

Tcpdump

Tcpdump displays TCP/IP packets and other network packets that are being transmitted over the network system. It is a form of protocol analyzer (sometimes called a sniffer) and is designed to show the contents of network packets in human-readable form for troubleshooting, security analysis, etc. Tcpdump is not native to either Linux or Windows but can be downloaded for free and used with both.

Telnet/ssh

Telnet and ***ssh*** allow a user to manage accounts and devices remotely. The main difference between the two is that ssh is encrypted, and thus all data is secure from eavesdropping, while telnet is unencrypted.