Networking basics modules 16, 17 and Final Exam

Day 13/365

The term server refers to a host running a software application that provides information or services to other hosts that are connected to the network, such as a web server. An example of client software is a web browser, like Chrome or Firefox. A single computer can also run multiple types of client software. A crucial factor to enable these complex interactions to function is that they all use agreed upon standards and protocols.

The key characteristic of client/server systems is that the client sends a request to a server, and the server responds by carrying out a function, such as sending the requested document back to the client. The combination of a web browser and a web server is perhaps the most commonly used instance of a client/server system.

A URI is a string of characters that identifies a specific network resource. The parts of a URI are protocol/scheme, hostname, path and file name, and fragment. A URI has two specializations:

- **URN** - This identifies only the namespace of the resource without reference to the protocol.
- **URL** - This defines the network location of a specific resource on the network. HTTP or HTTPS URLs are typically used with web browsers. Other protocols such as FTP, SFTP, SSH, and others can be used as a URL.

Common services include: DNS, SSH, SMTP, POP, IMAP, DHCP, HTTP, and FTP.

The DNS provides a way for hosts to request the IP address of a specific server. DNS names are registered and organized on the internet within specific high-level groups, or domains. Some of the most common high-level domains on the internet are .com, .edu, and .net.

When the DNS server receives the request from a host, it checks its table to determine the IP address associated with that web server. If the local DNS server does not have an entry for the requested name, it queries another DNS server within the domain. When the DNS server learns the IP address, that information is sent back to the host.

When a web client receives the IP address of a web server, the client browser uses that IP address and port 80 to request web services. This request is sent to the server using HTTP. The HTTP protocol is not a secure protocol; information could easily be intercepted by other users as data is sent over the network. To provide security for the data, HTTP can be used with secure transport protocols. Requests

for secure HTTP are sent to port 443. These requests use https in the site address in the browser, rather than http.

When the server receives a port 80 request, the server responds to the client request and sends the web page to the client. The information content of a web page is encoded using HTML. HTML coding tells the browser how to format the web page and what graphics and fonts to use.

FTP provides an easy method to transfer files from one computer to another (possibly deprecated today)

Telnet provides a standard method of emulating text-based terminal devices over the data network. Both the protocol itself and the client software that implements the protocol are commonly referred to as Telnet. Telnet servers listen for client requests on TCP port 23. A connection using Telnet is called a vty session, or connection. Rather than using a physical device to connect to the server, Telnet uses software to create a virtual device that provides the same features of a terminal session with access to the server's CLI.

Telnet is not considered to be a secure protocol. Although the Telnet protocol can require a user to login, it does not support transporting encrypted data. All data exchanged during Telnet sessions is transported as plaintext across the network. This means that the data can be easily intercepted and understood.

SSH provides the structure for secure remote login and other secure network services. It also provides stronger authentication than Telnet and supports transporting session data using encryption. Network professionals should always use SSH in place of Telnet, whenever possible.

Each mail server receives and stores mail for users who have mailboxes configured on the mail server. Each user with a mailbox must then use an email client to access the mail server and read these messages. Many internet messaging systems use a web-based client to access email including Microsoft 365, Yahoo, and Gmail. Application protocols used in processing email include SMTP, POP3, and IMAP4.

SMTP is used by an email client to send messages to its local email server. The local server then decides if the message is destined for a local mailbox or if the message is addressed to a mailbox on another server. If the server must send the message to a different server, SMTP is used between those two servers. SMTP requests are sent to port 25. A server that supports POP clients receives and stores messages addressed to its users. When the client connects to the email server, the messages are downloaded to the client. By default, messages are not kept on the server after they have been accessed by the client. Clients contact POP3 servers on port 110.

A server that supports IMAP clients also receives and stores messages addressed to its users. However, unlike POP, IMAP keeps the messages in the mailboxes on the server, unless they are deleted by the user. The most current version of IMAP is IMAP4 which listens for client requests on port 143.

Text messages may be called instant messages, direct messages, private messages, and chat messages. Text messaging enables users to chat over the internet in real-time. Text messaging services on a computer are usually accessed through a web-based client that is integrated into a social media or information sharing site. These clients usually only connect to other users of the same site.

An internet telephony client uses peer-to-peer technology similar to that used by instant messaging. IP telephony uses VoIP, which converts analog voice signals into digital data. The voice data is encapsulated into IP packets which carry the phone call through the network.

Troubleshooting Commands

A number of software utility programs are available that can help identify network problems. Most of these utilities are provided by the operating system as CLI commands.

Some of the available utilities include:

- **ipconfig** - Displays IP configuration information.
- **ping** - Tests connections to other IP hosts.
- **netstat** - Displays network connections.
- **tracert** - Displays the route taken to the destination.
- **nslookup** - Directly queries the name server for information on a destination domain.

The **ipconfig** command is used to display the current IP configuration information for a host. Issuing this command from the command prompt will display the basic configuration information including IP address, subnet mask, and default gateway.

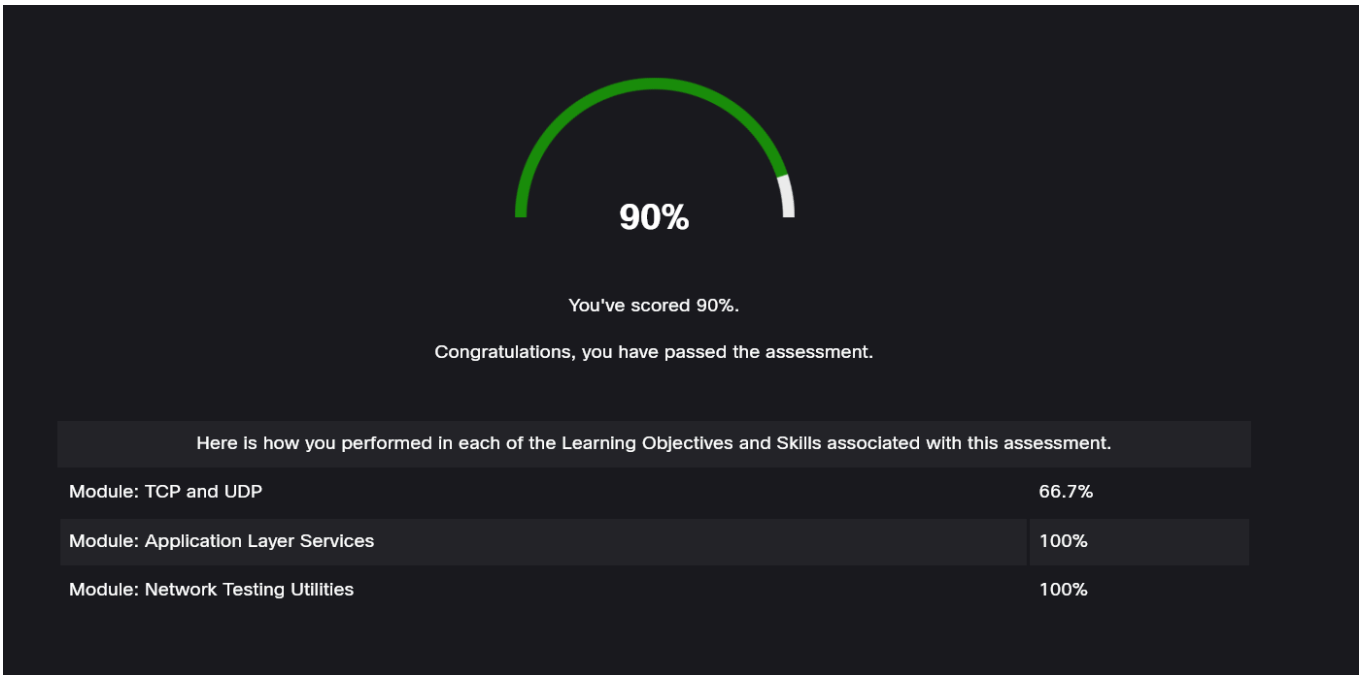
The command **ipconfig /all** displays additional information including the MAC address, IP addresses of the default gateway, and the DNS servers. It also indicates if DHCP is enabled, the DHCP server address, and lease information.

If IP addressing information is assigned dynamically, the command **ipconfig /release** will release the current DHCP bindings. **ipconfig /renew** will request fresh configuration information from the DHCP server. A host may contain faulty or outdated IP configuration information and a simple renewal of this information is all that is required to regain connectivity.

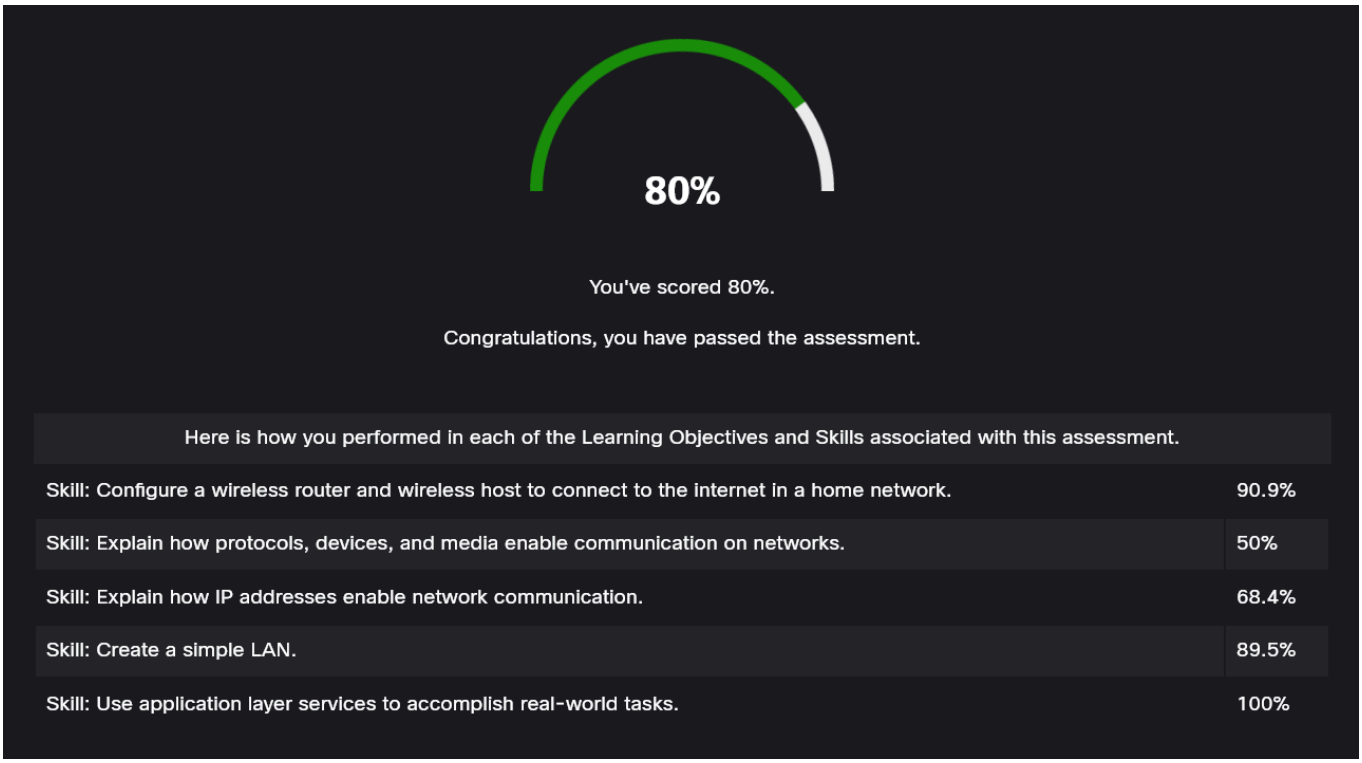
Probably the most commonly used network utility is ping. Most IP enabled devices support some form of the **ping** command in order to test whether or not network devices are reachable through the IP network. When a ping is sent to an IP address, a packet known as an echo request is sent across the network to the IP address specified. If the destination host receives the echo request, it responds with

a packet known as an echo reply. If the source receives the echo reply, connectivity is verified by the reply from the specific IP address.

Finished all modules



Last checkpoint exam first try



Final exam first try

Reviewed and corrected mistakes