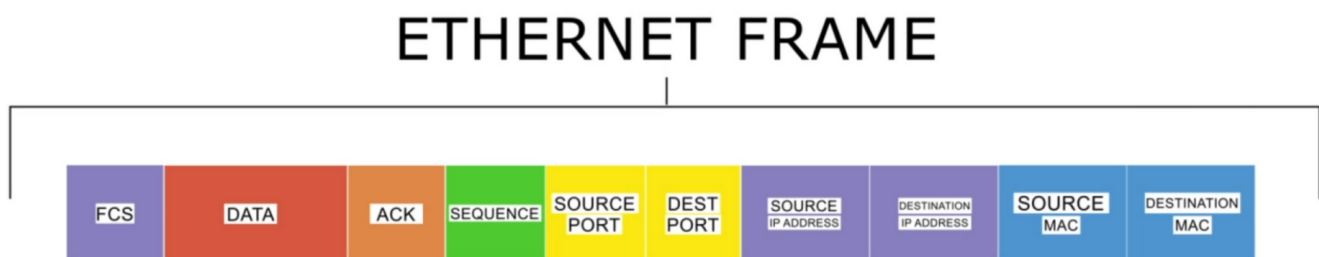


# Section 9: TCP/IP Applications

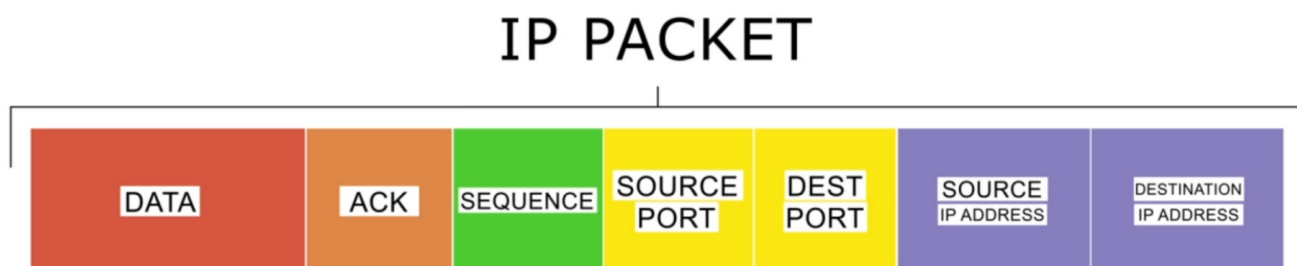
## 59. TCP and UDP

PDU (Protocol Data Units):

PDU in an Ethernet Frame:



PDU in an IP Packet:



PDU in a TCP and UDP:

TCP is connection based and called the "TCP Segment"

UDP is connectionless and calle the "UDP Datagram"

## TCP & UDP



UDP:

- Send a frame. No talk no response no communications
- TFTP*-Trivial File Transfer protocol - used for connectionless file transfer

TCP:

- TCP 3-way handshake
- 1.client sends Syn packet goes to the server
- 2.sends a syn/ack back to the client
- 3.client sends an ack back to the server

---

### 60. ICMP and IGMP

ICMP (Internet Control Message Protocol)

- Works at the IP layer of the OSI

ICMP Packet:



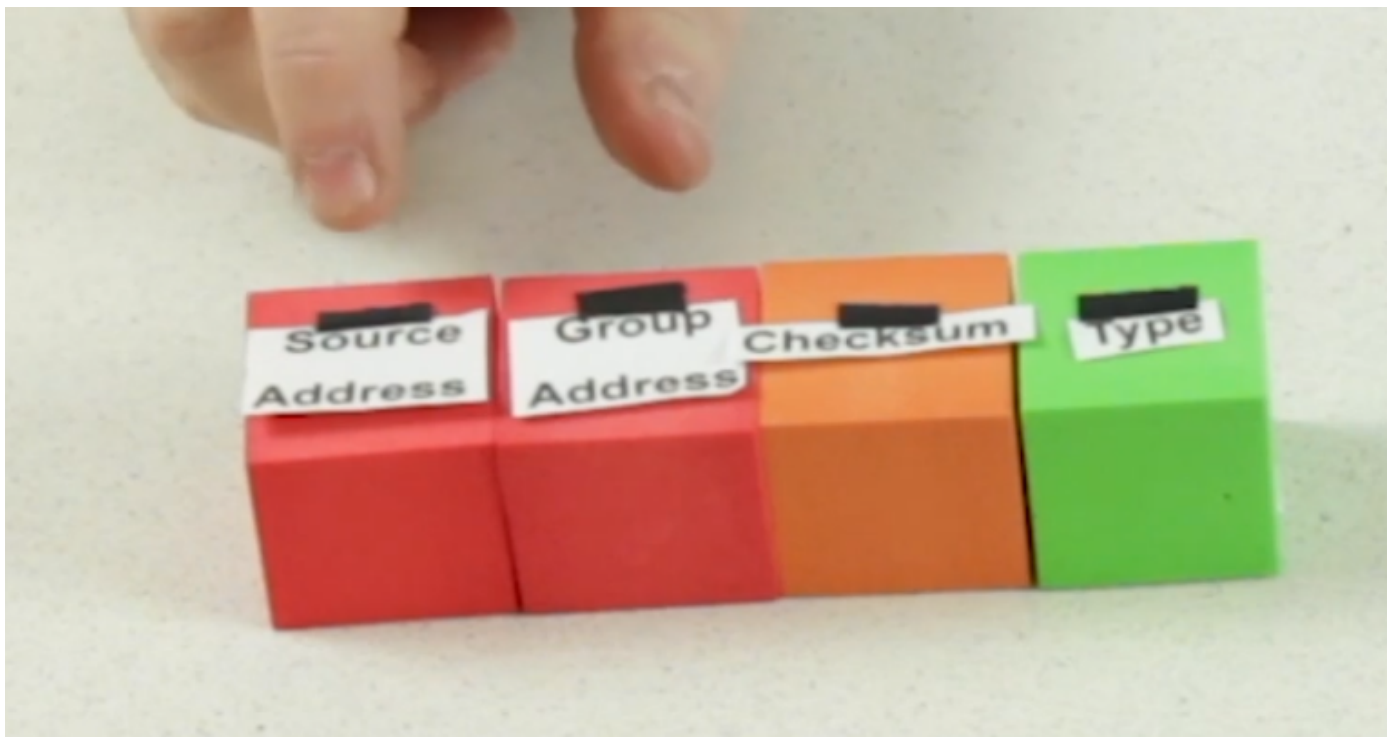
Example: "Ping" no data. Just looking for a response

"Type" has all kinds of responses

Example: ARP

IGMP (Internet Group Management Protocol)

IGMP Packet:



Multicast address (224.anything)

Group address: multicast address

Source address: the video server so everyone knows where it came from.

## For Exam Remember:

\*IGMP and ICMP are on the internet(2) layer of the TCP/IP model and the network (3) layer in the OSI model

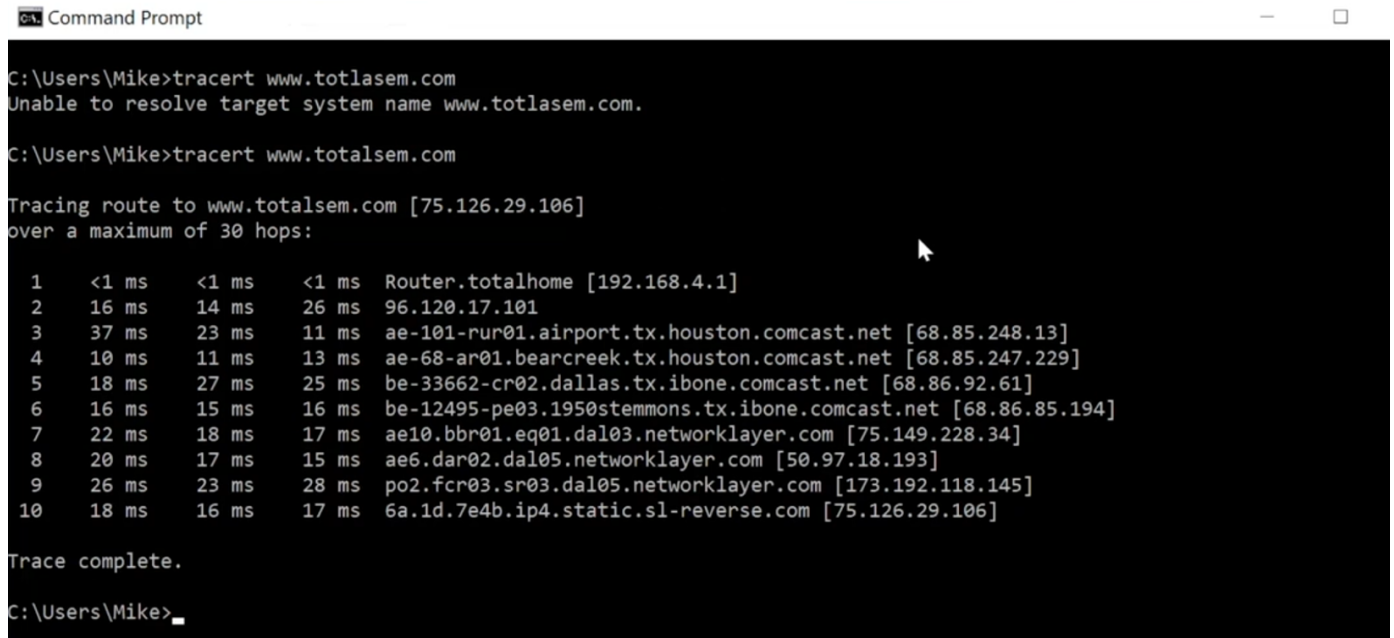
\*IGMP provides multicast support

\*Multicast addresses always start with 224

---

## 61. Handy Tools

1. Trace Route: a command that allows you to check all the hops  
tracert (Windows) = traceroute (Linux)



```
Command Prompt

C:\Users\Mike>tracert www.totlasem.com
Unable to resolve target system name www.totlasem.com.

C:\Users\Mike>tracert www.totalsem.com

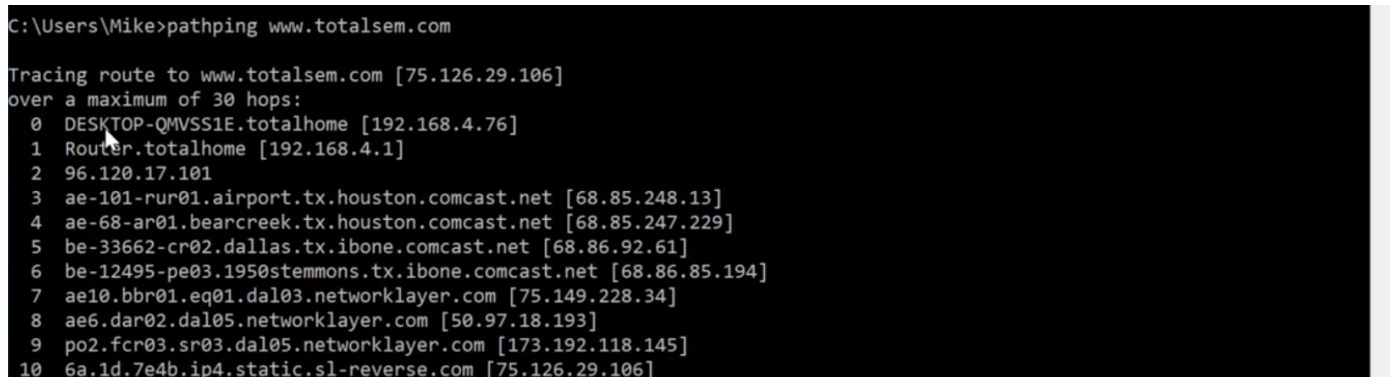
Tracing route to www.totalsem.com [75.126.29.106]
over a maximum of 30 hops:

  0  <1 ms    <1 ms    <1 ms  Router.totalhome [192.168.4.1]
  1  16 ms    14 ms    26 ms  96.120.17.101
  2  37 ms    23 ms    11 ms  ae-101-rur01.airport.tx.houston.comcast.net [68.85.248.13]
  3  10 ms    11 ms    13 ms  ae-68-ar01.bearcreek.tx.houston.comcast.net [68.85.247.229]
  4  18 ms    27 ms    25 ms  be-33662-cr02.dallas.tx.ibone.comcast.net [68.86.92.61]
  5  16 ms    15 ms    16 ms  be-12495-pe03.1950stemmons.tx.ibone.comcast.net [68.86.85.194]
  6  22 ms    18 ms    17 ms  ae10.bbr01.eq01.dal03.networklayer.com [75.149.228.34]
  7  20 ms    17 ms    15 ms  ae6.dar02.dal05.networklayer.com [50.97.18.193]
  8  26 ms    23 ms    28 ms  po2.fcr03.sr03.dal05.networklayer.com [173.192.118.145]
  9  18 ms    16 ms    17 ms  6a.1d.7e4b.ip4.static.sl-reverse.com [75.126.29.106]

Trace complete.

C:\Users\Mike>
```

2. Alternative to Trace Route called "pathping



```
C:\Users\Mike>pathping www.totalsem.com

Tracing route to www.totalsem.com [75.126.29.106]
over a maximum of 30 hops:
  0  DESKTOP-QMVSS1E.totalhome [192.168.4.76]
  1  Router.totalhome [192.168.4.1]
  2  96.120.17.101
  3  ae-101-rur01.airport.tx.houston.comcast.net [68.85.248.13]
  4  ae-68-ar01.bearcreek.tx.houston.comcast.net [68.85.247.229]
  5  be-33662-cr02.dallas.tx.ibone.comcast.net [68.86.92.61]
  6  be-12495-pe03.1950stemmons.tx.ibone.comcast.net [68.86.85.194]
  7  ae10.bbr01.eq01.dal03.networklayer.com [75.149.228.34]
  8  ae6.dar02.dal05.networklayer.com [50.97.18.193]
  9  po2.fcr03.sr03.dal05.networklayer.com [173.192.118.145]
 10  6a.1d.7e4b.ip4.static.sl-reverse.com [75.126.29.106]
```

3. Bandwidth Speed Tester:

These are 3rd party.

- Are you being ripped off by your ISP
- Bad cheap routers can destroy our speeds

---

## 62. Introduction to Wireshark

\*Wireshark is a protocol analyzer that comes with a frame capture tool \*On the exam

\*Wireshark displays the traffic flow of Ethernet frames, and can drill down into the frame-viewing various protocols, ports, timelines, and services

-Wireshark can segment and organized the data into consumable information to help in troubleshooting

Grabs data and allows us to pull a packet apart

DHCP = bootp

*wireshark is the best protocol analyzer out there. Need to know wireshark*

The capture tool for wireshark is notorious for missing packets so people use alternative capture tools such as:

TCP dump

"sudo tcpdump"

---

## 62. Introduction to netstat

netstat lists all the open ports and connections on your computer.

netstat -n shows the results numerically

netstat -b shows the executable for every connection

netstat -o shows the PID (windows)

netstat -a shows all active ports

netstat -r shows the local routing table

### On the exam

-Netstat keeps track of all our connections

-shows us the ports

run netstat command at the command prompt

Know netstat switches above

---

## 63. Web Servers

\*A server is just software

\*You can run a web server on any computer

Two types of servers on the internet:

1. Microsoft ISS (Internet Information Services)

2. Apache

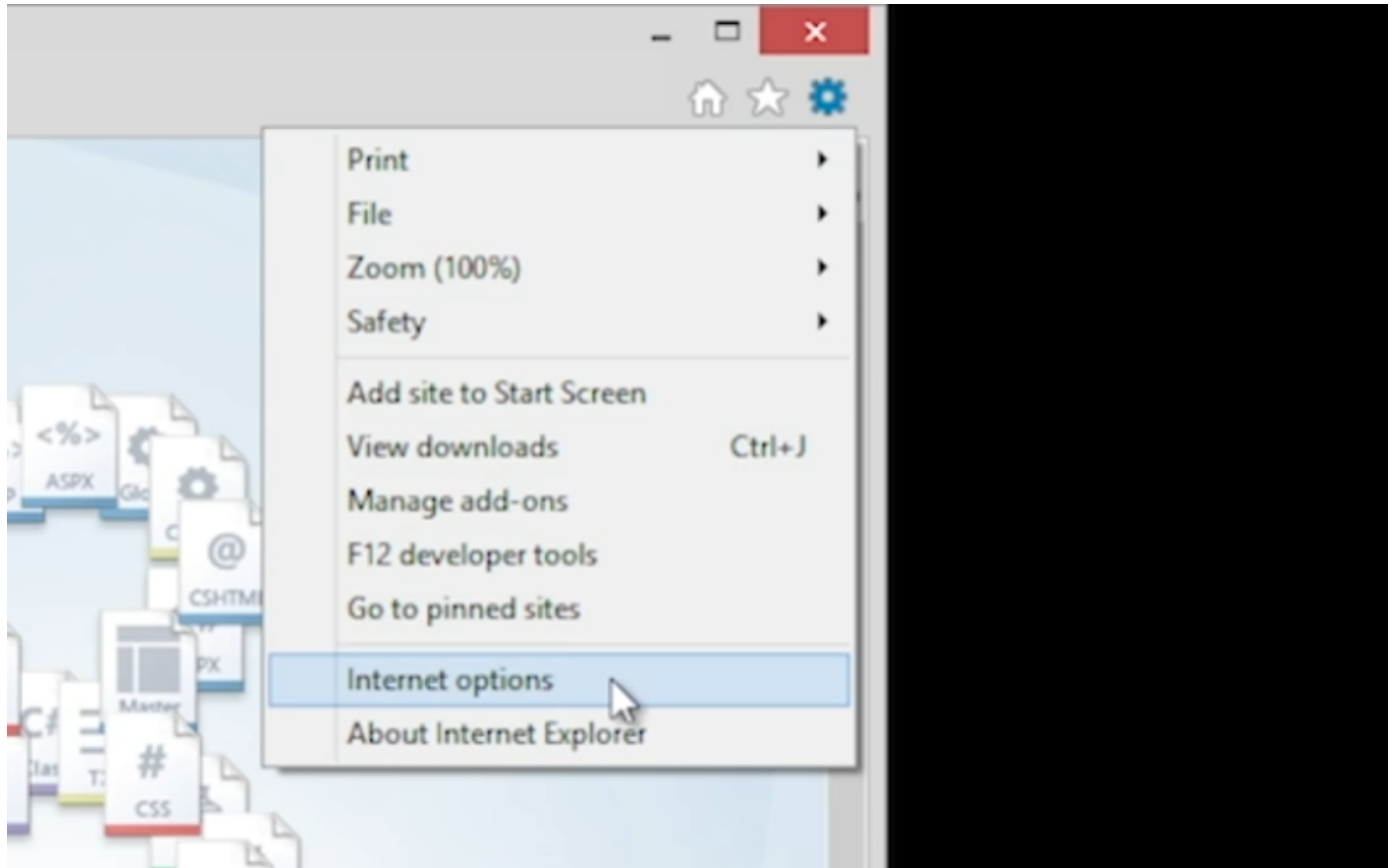
Run netstat -a to check if a web server is running

Net+ focuses on the client side.

Most questions will focus on microsofts internet explorer

-Asks pathing questions about how to get to stuff from a web server

**\*\*Tools>Internet Options\*\*** is the answer



**\*\*http (Hyper Text Transfer Protocol) listens on port 80**

**\*\*https (secure http)- encrypts traffic (port 443)**

Review:

-Web servers host web sites: web clients access web servers

- HTTP uses TCP port 80 by default
- HTTPs uses TCP port 443 as default

---

## 65. FTP

(File Transfer Protocol)

FTP uses ports 21 and 20

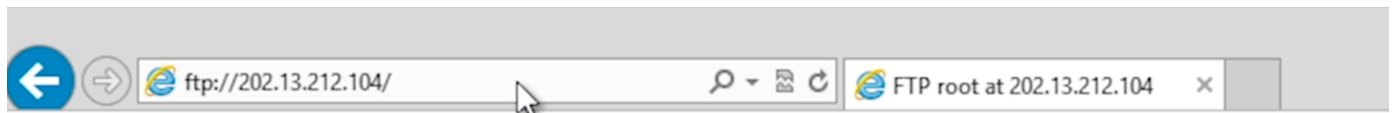
anonymous accounts enable public access to FTP servers

Lots of things have an FTP client built in.

WSFTPLe - Free FTP client

FTP clients send requests out (servers listen) on port 21, but send back information to the client on port 20.

Any web browser makes a good FTP client



## FTP root at 202.13.212.104

To view this FTP site in File Explorer: press Alt, click View, and then click **Open FTP Site in File Explorer**.

|                    |           |  |
|--------------------|-----------|--|
| 11/28/2012 11:15AM | 282       | <a href="#">desktop.ini</a>            |
| 09/05/2012 12:00AM | 1,007     | <a href="#">Dropbox.lnk</a>            |
| 12/03/2012 05:25PM | 2,479     | <a href="#">Google Chrome.lnk</a>      |
| 12/11/2012 10:34AM | Directory | <a href="#">Imag</a>                   |
| 08/22/2012 12:00AM | 1,168     | <a href="#">OpenOffice.org 3.4.lnk</a> |
| 08/22/2012 12:00AM | 947       | <a href="#">ApTorrent.lnk</a>          |

<ftp.microsoft.com/products>

Windows command prompt has an FTP client **on the exam**

site in File Explorer: press Alt, click View, and then click **Open FTP Site in File Explorer**.

```
C:\Users\Miketohlian>cd\
C:\>ftp
ftp> open 202.13.212.104
Connected to 202.13.212.104.
220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
User (202.13.212.104:(none)): dave
331 Password required for dave
Password:
230 Logged on
ftp> ?
Commands may be abbreviated.  Commands are:
?          delete          literal          prompt          send
?          debug            ls              put             status
append     dir                mdelete         pwd             trace
ascii     disconnect        mdir            quit            type
bell      get               mget            quote           user
binary    glob              nkdir           recv            verbose
bye       hash              nls             remotehelp
cd        help              nput            rename
close    lcd               open            rmdir
ftp> _
```

The GET command Downloads

The PUT command uploads

FTP is not an encrypted protocol.

**\*\*to do secure things you need to use SFTP (Secure FTP)**

(TFPT) Trivial FTP - a lightweight UDP protocol that works on port 69

## 66. Email Servers and Clients

SMTP (Simple Mail Transfer Protocol) - Port 25

POP3 (Post Office Protocol Version3) - Port 110

IMAP (Internet Message Access Protocol V4) - Port 143

**Need to memorize port for the Network+ Exam**

\*Email is based on domain names

\*Netplus needs us to understand the older way of doing Email.

POP vs IMAP

Pop anything on the server is copied down to the client and you can set up folders on the client

IMAP copies of emails are done online and you can set up folders online as well

**For the exams know the port numbers**

---

## **67. Securing E-Mail**

-SMTP, IMAP, POP3 are not encrypted

-All mail servers have the capability to encrypt email

**Very important for the exam**

*Real email (Not web based)*

\*Traditional TLS (OLD)

IMAP 143 -> 993 ENCRYPTED

POP 110 -> 995 ENCRYPTED

SMTP 25 -> 465 ENCRYPTED

Problem: Realized bad guys might be monitoring and doing a MIM attack

\*Start TLS

IMAP, POP3, SMTP - PORT 465

Problem: TLS/STARTTLS conflicted with port 465

Solution: STARTTLS changed to port 587

when configuring email servers and email clients there are a lot of variants.

On the client side it can be more frustration.

**\*\*for the exam you MUST know that there were two different protocols:**

1st version TLS started unencrypted and then went encrypted.

**\*\*IMAP 143 UNENCRYPTED -> 993 ENCRYPTED\*\***

**\*\*POP 110 UNENCRYPTED -> 995 ENCRYPTED\*\***

**\*\*SMTP 25 UNENCRYPTED -> 465 ENCRYPTED\*\***

2nd version was STARTTLS which was port 465 but caused issues between TLS and STARTTLS so start TLS went to Port 587

**START TLS extension uses only one port (587) for encrypted communication**

---

## **68. Telnet and SSH**

Telnet is a remote command prompt to a far away computer.



A Telnet server is not built into windows.

Telnet clients are most times built into windows

Telnet runs on Port 23

\*PuTTY - is a telnet client with a GUI

You don't transfer files, you just get to a command prompt

Telnet is unencrypted.

**Telnet - Unencrypted Terminal Emulator TCP Port 23 (Used Locally)**

**rlogin - Unencrypted Terminal Emulator TCP port 513 - Replaced with SSH (Not used)**

**SSH(Secure Shell) - Encrypted Terminal Emulator TCP Port 22 (Used over the web)**

SSH uses an authentication Key

---

## **69. (NTP) Network Time Protocol**

Runs on port 123 - Manages applications that need to check the time

Hundreds of protocols rely on NTP.

A system with NTP may cause networking issues

There are hundreds of NTP servers worldwide

---

## **70 Network Service Scenarios**

### **1. DHCP Issues:**

1. IP Reservations: (ex. reserved address for NETWORK ID or Broadcast or for a file server) Reduce DHCP Scope and then do your reservations.

2. MAC Reservation (ex. a Camera):

REAL SCENARIO: John has a system and he can't get on the web. checks his ip address and finds that he has an APIPA address which means he is not getting an IP address. However, the file server will get to the web, a camera has access to web, some other computers have addresses. Biggest mistake with DHCP scope is they set really long leases. (Issue: Exhausted the DHCP scope) (solution: Add more addresses to the scope, or shorten the DHCP lease time)

DHCP Servers alone are not the perfect tool that we want them to be.

IPAM (IP Address Management) tools - very power full tool for managing your IP address.

REVIEW:

-DHCP Scope ranges need to consider gateway, printers, and other types of hosts to provide the IP reservations

-MAC reservations can be used to define devices that have top priority for address assignment

-IPAM tools track and manage allotted IP addresses, keeping address requirement available for server and VM farms

## **QUIZ**

1. Which characteristic is true of TCP?
  - a. TCP is connectionless
  - b. The TCP three-way handshake begins with a SYN message, followed by an ACK response followed by an ACK SYN message
  - c. TCP uses the FIN message to close a connection**
  - d. TCP uses the END message to close a connection
2. Ping uses which IP layer Protocol
  - a. ICMP**
  - b. ARP
  - c. RIP
  - d. FTP
3. Which of the following is not a network information or troubleshooting utility?
  - a. tracert
  - b. pathping
  - c. FTP**
  - d. Bandwidth tester
4. Which choice is not true about protocol analyzers such as Wireshark?
  - a. Protocol analyzers can capture packets and frames
  - b. Protocol analyzers can show the contents of packets and frames
  - c. Protocol analyzers can filter the contents of packet frames
  - d. Protocol analyzers can generate packets and frames
5. What is the primary purpose of netstat?
  - a. Captures frames and packets for later review
  - b. Shows your computer's connection(s) to a web server(s)
  - c. Graphical utility that charts amount of network data entering and leaving a host
  - d. Displays all connections to and from a host computer**
6. FTP uses TCP port 20 and TCP port 21. Which choice describes how the ports are used?
  - a. FTP servers listen for commands on port 20 and respond with data on port 21
  - b. FTP servers listen for commands on port 21 and respond with data on port 20**
  - c. FTP clients send requests on port 21 and receive data on port 21
  - d. FTP clients send requests on port 202 and receive data on port 20
7. Which of the following is a secure email protocol?
  - a. SMTP
  - b. STLS**
  - c. POP
  - d. IMAP
8. Which choice describes a significant difference between Telnet and SSH?
  - a. Telnet is an Internet Telephony protocol, SSH is a Secure Sharing protocol
  - b. Telnet runs on a client, SSH runs on a server
  - c. Telnet runs on a server, SSH runs on a client
  - d. Telnet is unencrypted, SSH is encrypted**

9. Which is the default port for NTP?

a. 321

**b. 123**

c. 132

d. 231

10. Which of the following is not a network service program?

a. Duplicate IP address in DHCP scope

b. Not enough IP addresses in the DHCP scope

c. Overlong DHCP lease periods

**d. Exclusions in the DHCP scope**