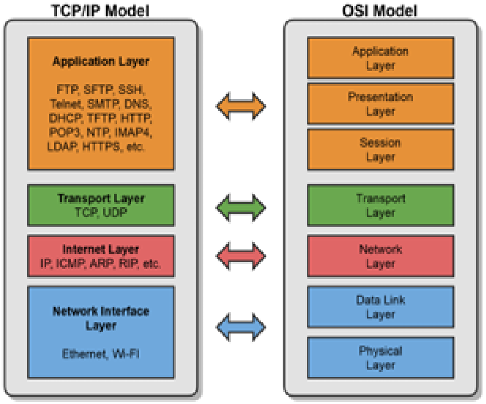
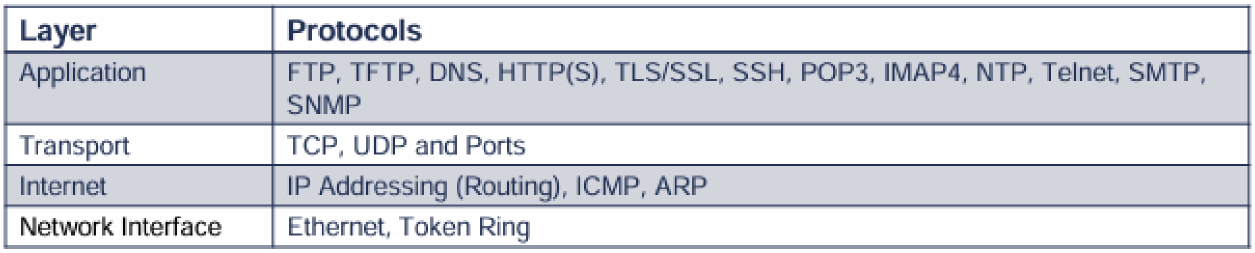
Networking Protocols

What is Tcp/ Ip?

- Transmission Control Protocol/Internet Protocol
- Commonly called the Internet Protocol suite because it was designed for the Internet, but LANs use it too.
- First Two Protocols Defined in the Suite Were:
  - TCP & IP, hence TCP/IP
- Similar to the OSI Model, but Simpler:
  - OSI is Conceptual
  - TCP/IP was Implemented



Tcp/Ip Protocol:



Layer	Protocols
Application	FTP, TFTP, DNS, HTTP(S), TLS/SSL, SSH, POP3, IMAP4, NTP, Telnet, SMTP, SNMP
Transport	TCP, UDP and Ports
Internet	IP Addressing (Routing), ICMP, ARP
Network Interface	Ethernet, Token Ring

These protocols work together to provide communication, management, diagnostics, and troubleshooting for a TCP/IP network.

Understanding Protocols, Ports, and Sockets

Protocols:

- Computers communicate with each other with network protocols.
- Protocols are rules governing how machines exchange data and enable effective communication.
- In an operating system (OS), a protocol runs as a process or service.

Ports:

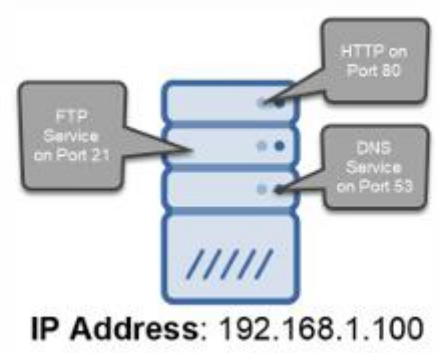
- Ports **are logical constructs that bind a unique port number to a protocol process or service.**

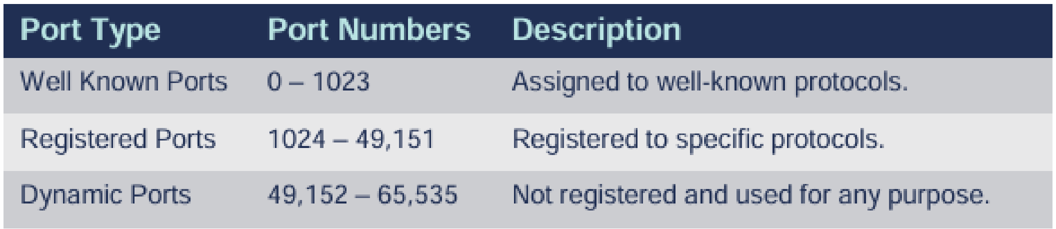
Sockets:

- Sockets are a combination of an IP address and a port number, for example, 192.168.1.1:80.

Why We Need Ports and Sockets?

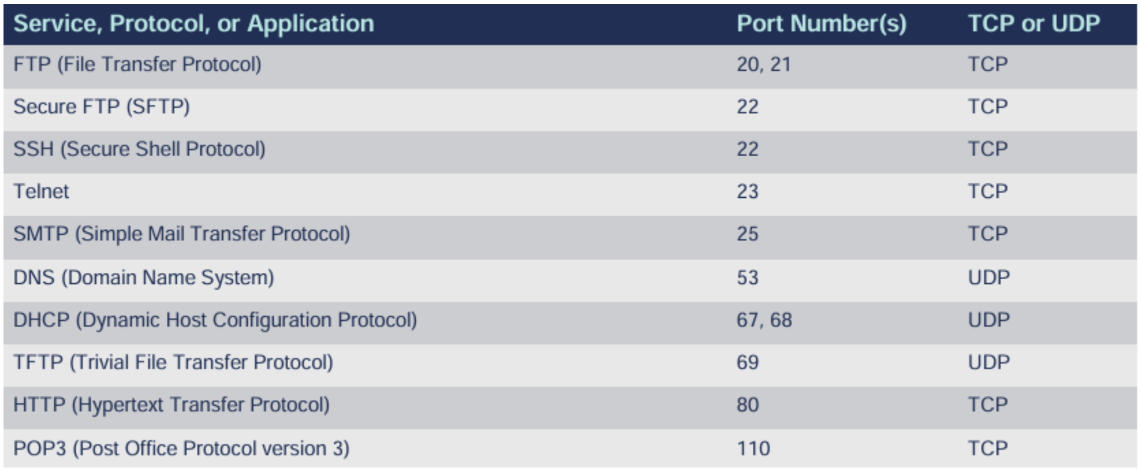
- Computers require ports because of network application multitasking.
- Because a computer may have only one IP address, it needs ports to differentiate network protocols and services running on it.
- TCP/IP has 65,536 ports available



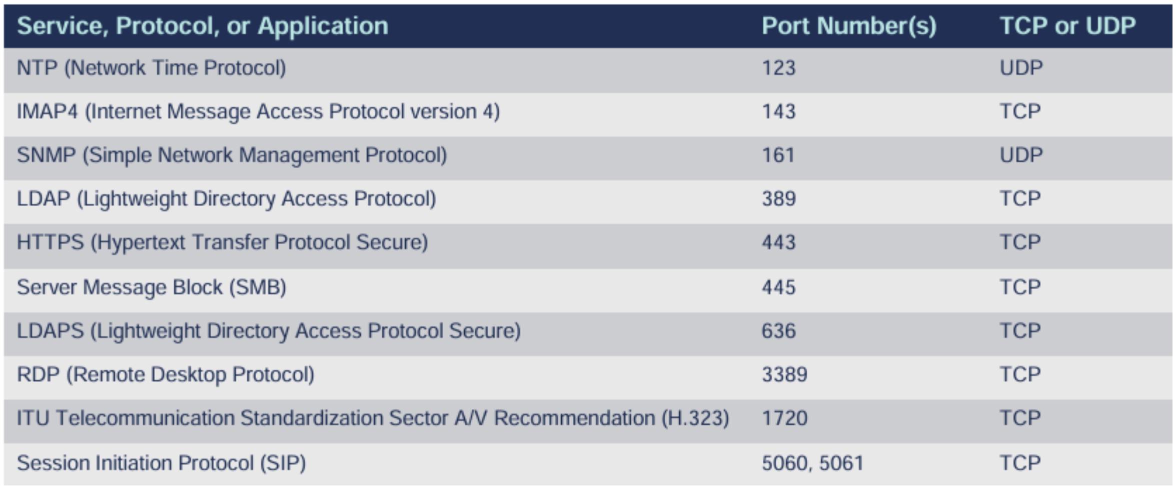


Port Type	Port Numbers	Description
Well Known Ports	0 – 1023	Assigned to well-known protocols.
Registered Ports	1024 – 49,151	Registered to specific protocols.
Dynamic Ports	49,152 – 65,535	Not registered and used for any purpose.

Protocols & Port Numbers:



Service, Protocol, or Application	Port Number(s)	TCP or UDP
FTP (File Transfer Protocol)	20, 21	TCP
Secure FTP (SFTP)	22	TCP
SSH (Secure Shell Protocol)	22	TCP
Telnet	23	TCP
SMTP (Simple Mail Transfer Protocol)	25	TCP
DNS (Domain Name System)	53	UDP
DHCP (Dynamic Host Configuration Protocol)	67, 68	UDP
TFTP (Trivial File Transfer Protocol)	69	UDP
HTTP (Hypertext Transfer Protocol)	80	TCP
POP3 (Post Office Protocol version 3)	110	TCP



Service, Protocol, or Application	Port Number(s)	TCP or UDP
NTP (Network Time Protocol)	123	UDP
IMAP4 (Internet Message Access Protocol version 4)	143	TCP
SNMP (Simple Network Management Protocol)	161	UDP
LDAP (Lightweight Directory Access Protocol)	389	TCP
HTTPS (Hypertext Transfer Protocol Secure)	443	TCP
Server Message Block (SMB)	445	TCP
LDAPS (Lightweight Directory Access Protocol Secure)	636	TCP
RDP (Remote Desktop Protocol)	3389	TCP
ITU Telecommunication Standardization Sector A/V Recommendation (H.323)	1720	TCP
Session Initiation Protocol (SIP)	5060, 5061	TCP

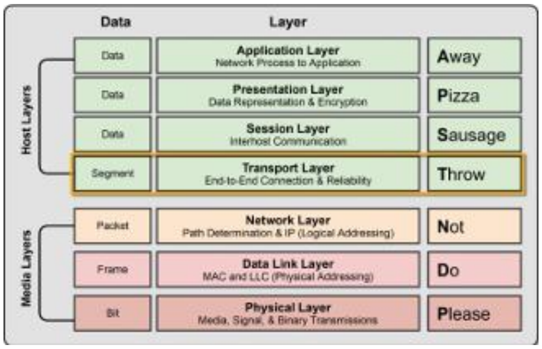
TCP vs. UDP

Transport Layer Protocols:

- **TCP** (Transmission Control Protocol): Connection-Oriented
- **UDP** (User Datagram Protocol): Connectionless

TCP is the most widely used Transport Layer protocol because it is connection-oriented, which provides packet delivery reliability, i.e., guaranteed delivery.

UDP, being connectionless, is considered to be unreliable; however, it is more lightweight than TCP and often used for streaming or real-time data.



	Data	Layer	
Host Layers	Data	**Application Layer** Network Process to Application	Away
	Data	**Presentation Layer** Data Representation & Encryption	Pizza
	Data	**Session Layer** Interhost Communication	Sausage
	Segment	**Transport Layer** End-to-End Connection & Reliability	Throw
Media Layers	Packet	**Network Layer** Path Determination & IP (Logical Addressing)	Not
	Frame	**Data Link Layer** MAC and LLC (Physical Addressing)	Do
	Bit	**Physical Layer** Media, Signal, & Binary Transmissions	Please

TCP Reliability:

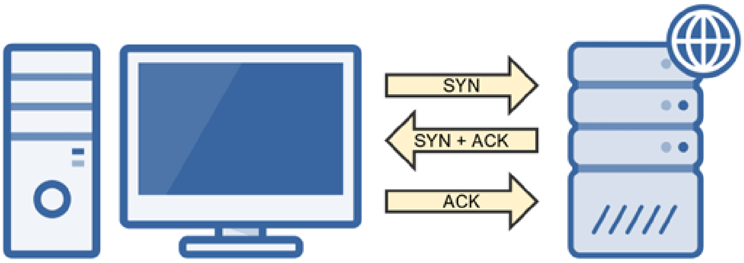
TCP utilizes the following features to ensure reliable delivery of data.

- **3-Way Handshake** creates a virtual connection between the source and destination before data is sent.
- **Acknowledgment** is required before the next segment is sent.
- **Checksum** that detects corrupted data.
- **Sequence Numbers** that detect missing data and reassemble them in the correct order.
- **Retransmission** that will retransmit lost or corrupt data.

Note: TCP header is 20 bytes in size, whereas the UDP header is only 8 bytes.

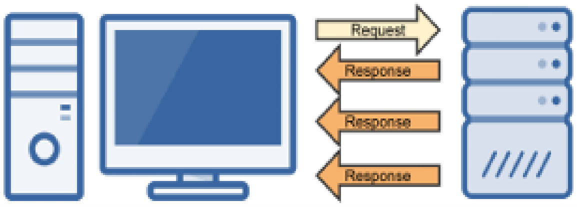
TCP Three-Way Handshake

- A connection must be established before data is transmitted, called the three-way handshake.
  SYN →SYN / ACK →ACK
- Creates a Virtual Connection Between 2 Devices



“Best Efforts” UDP

- A scaled-down, economic version of TCP
  - Connectionless & Unreliable
  - No Data Retransmissions
  - “Best Effort”
- Faster than TCP
  - Smaller Header & Connectionless
- Primarily used for protocols that favor:
  - Low-Latency, i.e., Faster Speeds
  - Can Tolerate Data Loss
- Example UDP Use-Cases:
  - VoIP Phone Calls
  - Live Video Streams
  - Live Audio Streams
  - Online Gaming
  - Certain Network Management Protocols
    - DNS
    - DHCP
    - NTP

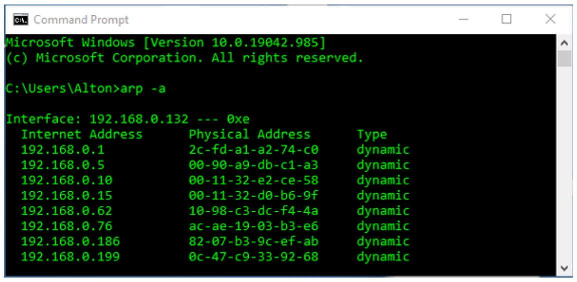


Protocols:

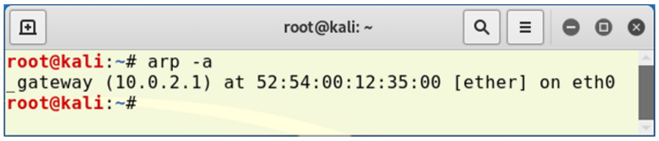
Address Resolution Protocol (ARP)

- Resolves IP address to MAC Addresses
- Finds the hardware address of a host from a known IP address.
    - And vice versa (RARP)

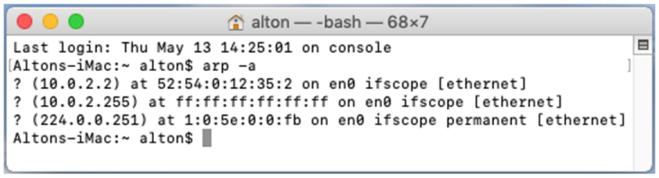
ARP Command: arp-a



```
Microsoft Windows [Version 10.0.19042.985]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Alton>arp -a

Interface: 192.168.0.132 --- 0xe
  Internet Address      Physical Address      Type
  192.168.0.1           2c-fd-a1-a2-74-c0     dynamic
  192.168.0.5           00-90-a9-db-c1-a3     dynamic
  192.168.0.10          00-11-32-e2-ce-58     dynamic
  192.168.0.15          00-11-32-d0-b6-9f     dynamic
  192.168.0.62          10-98-c3-dc-f4-4a     dynamic
  192.168.0.76          ac-ae-19-03-b3-e6     dynamic
  192.168.0.186         82-07-b3-9c-ef-ab     dynamic
  192.168.0.199         0c-47-c9-33-92-68     dynamic
```

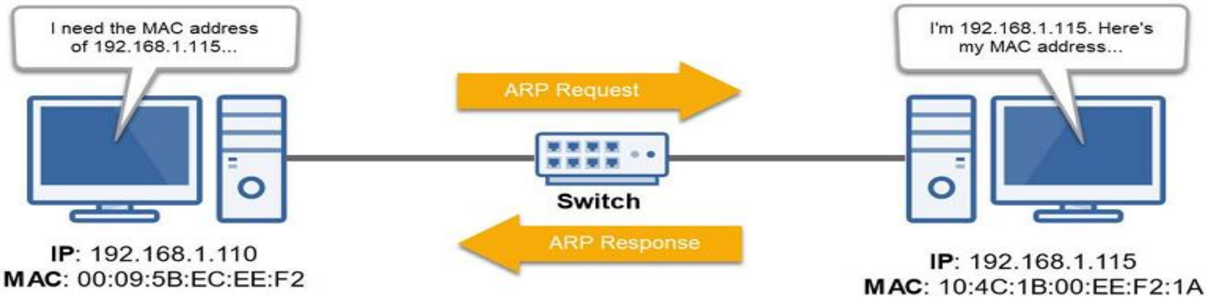


```
root@kali:~# arp -a
_gateway (10.0.2.1) at 52:54:00:12:35:00 [ether] on eth0
root@kali:~#
```



```
Last login: Thu May 13 14:25:01 on console
Altons-iMac:~ alton$ arp -a
? (10.0.2.2) at 52:54:0:12:35:2 on en0 ifscope [ethernet]
? (10.0.2.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
? (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
Altons-iMac:~ alton$
```

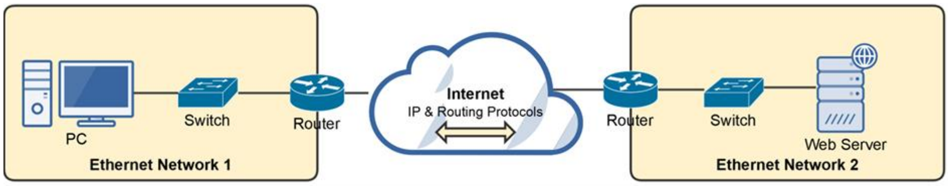
ARP Diagram:


I need the MAC address of 192.168.1.115...
I'm 192.168.1.115. Here's my MAC address...
ARP Request
Switch
ARP Response
IP: 192.168.1.110
MAC: 00:09:5B:EC:EE:F2
IP: 192.168.1.115
MAC: 10:4C:1B:00:EE:F2:1A

If a computer knows a device's IP address but not its MAC address, it'll send a broadcast message to all devices on the LAN asking which device is assigned that MAC address.

Internet Protocol (IP)

- An OSI Layer 3 protocol that defines routing and logical addressing of packets that allow data to traverse WANs and the Internet.
- It specifies the formatting of packets and the logical addressing schema.
    - IP addresses: IPv4 and IPv6
- Its job is to connect different OSI Layer 2 (switched) networks together.
- Provides end-to-end connectivity from one Layer 2 network to another via routers.



- It's connectionless and, therefore, unreliable (similar to UDP).
    - No continued connection.
- Each packet sent is independent of each other packet.
    - TCP and other protocols provide a means to reassemble them properly.
- Packets don't always follow the same path to their destination.
    - They're sent via the most efficient route.
- Doesn't provide any error recovery or sequencing functionality.
    - That's the job of other protocols.

Internet Control Message Protocol (ICMP)

- OSI Layer 3 Internet Protocol (IP) companion "error reporting" protocol within the TCP/IP suite of protocols.
- Just like IP, it's connectionless.
- Used to generate error messages to the source IP address when network issues prevent the delivery of a packet.
- Typically used by routers to report packet delivery issues, and, most importantly, it can report errors but not correct them.
- Commonly used by IT administrators to troubleshoot network connections with command-line utilities, including ping, pathping, and traceroute.
- For IPv6, it is also used for:
    - Neighbor Solicitation and Advertisement Messages (Similar to ARP)
    - Router Solicitation and Advertisement Messages

Some ICMP Massage Type:

- **Echo Request, Echo Reply:** Tests destination accessibility and status. A host sends an Echo Request and listens for a corresponding Echo Reply. Commonly done using the ping command.
- **Destination Unreachable:** Sent by a router when it can't deliver an IP packet.
- **Source Quench:** Sent by a host or router if it's receiving too much data than it can handle. The message requests that the source reduces its rate of data transmission.
- **Redirect Message:** Sent by a router if it receives a packet that should have been sent to a different router. The message includes the IP address to which future packets should be sent and is used to optimize the routing.
- **Time Exceeded:** Sent by a router if a packet has reached the maximum limit of routers through which it can travel.
- **Router Advertisement, Router Solicitation (IPv6):** Allow hosts to discover the existence of routers. Routers periodically multicast their IP addresses via Router

Advertisement messages. Hosts may also request a router IP address by broadcasting a Router Solicitation message, then wait for a router to reply with a Router Advertisement.

Application Layer Management Protocols:

- Domain Name System (DNS)
- Dynamic Host Configuration Protocol (DHCP)
- Network Time Protocol (NTP)
- Simple Network Management Protocol (SNMP)
- Lightweight Directory Access Protocol (LDAP)
- LDAP Secure (LDAPS)
- Server Message Block (SMB)

Domain Name System (DNS)

Port: 53 Transport Layer Protocol: UDP

- Protocol that is used to resolve a domain name to its corresponding IP address.
    - InstructorAlton.com → 162.0.232.236
- Uses TCP port 53 by default.
- We'll be discussing DNS in detail in the DNS Network Services section of this course:
    - DNS Hierarchy
    - DNS Record Types
    - Name Resolution

Dynamic Host Configuration Protocol (DHCP)

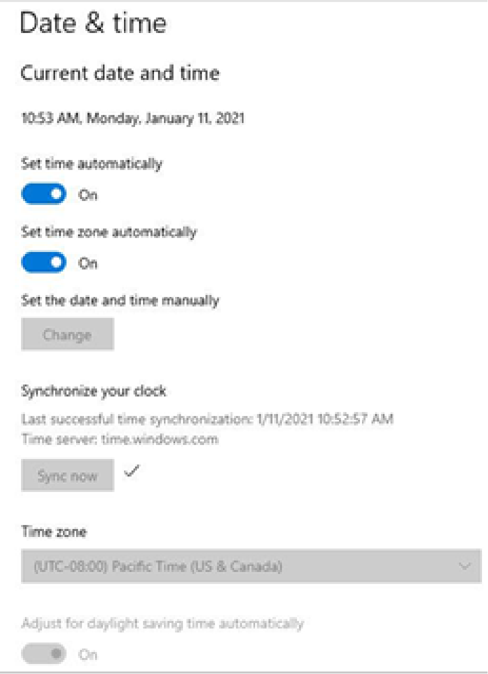
Ports: 67, 68 Transport Layer Protocol: UDP

- Protocol that automatically assigns IP address configurations to devices on a network:
    - IP Address
    - Subnet Mask
    - Default Gateway
    - DNS Server
- We'll be discussing how DHCP works in detail in the Assigning IP Addresses section of this course.
- Uses two UDP ports 67 and 68 by default.

Network Time Protocol (NTP)

Port: 123 Transport Layer Protocol: TCP

- Protocol that automatically synchronizes a system's time with a network time server.
    - Important for time-dependent network applications and protocols.
    - If a system is configured with the incorrect time, it may not be able to access network services.
    - Authentication will often fail if time isn't properly synchronized between devices.
- Uses TCP port 123 by default.



Date & time

Current date and time

10:53 AM, Monday, January 11, 2021

Set time automatically: On

Set time zone automatically: On

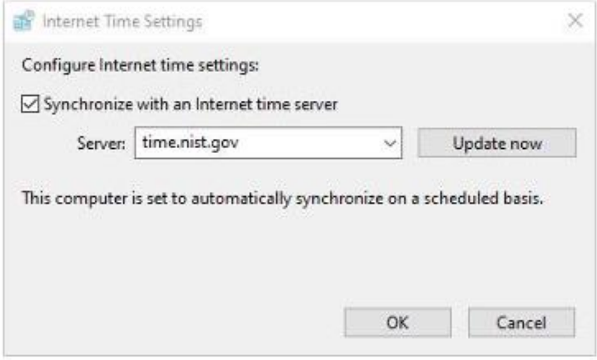
Set the date and time manually

Synchronize your clock

Last successful time synchronization: 1/11/2021 10:52:57 AM
Time server: time.windows.com

Time zone: (UTC-08:00) Pacific Time (US & Canada)

Adjust for daylight saving time automatically: On



Internet Time Settings

Configure Internet time settings:

☑ Synchronize with an Internet time server

Server: time.nist.gov

This computer is set to automatically synchronize on a scheduled basis.

Simple Network Management Protocol (SNMP)

Port: 161 Transport Layer Protocol: TCP

- Protocol used to monitor and manage network devices.
- Allows admins to monitor and manage network devices and traffic.
- Allows network devices to communicate information about their state:
    - Memory
    - CPU
    - Bandwidth
- Uses TCP port 161 by default

Lightweight Directory Access Protocol (LDAP)

Port: 389 Transport Layer Protocol: TCP

- Protocol that provides a means to access and query directory service systems:
    - Usernames, Passwords, Computer Accounts, etc.
- Typically Unix/Linux-based or Microsoft Active Directory-based.
- Uses TCP 389 by default.

LDAP Secure (LDAPS)

Port: 636 Transport Layer Protocol: TCP

- LDAP over SSL
- A secure version of LDAP that utilizes SSL to encrypt LDAP network traffic.
- Uses TCP port 636 by default

Server Message Block (SMB)

Port: 445 Transport Layer Protocol: TCP

- Network and file sharing protocol commonly used in Microsoft environments.
- Allows systems to share their files and printers with other systems
- Uses TCP port 445 by default.

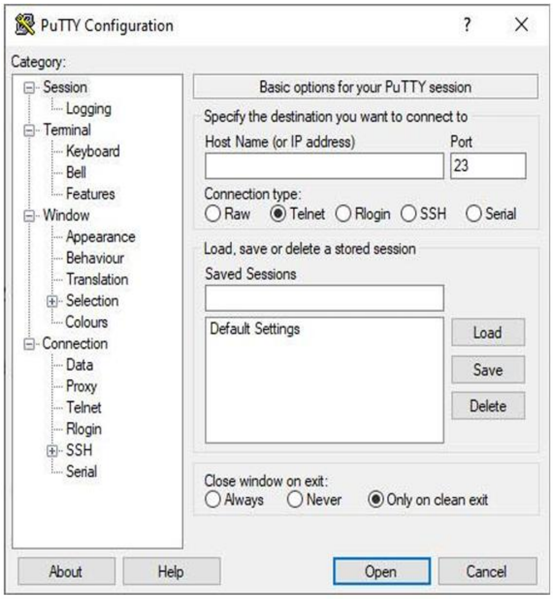
Application Layer Remote Communication Protocols

- Telnet
- Secure Shell (SSH)
- Remote Desktop Protocol (RDP)

Telnet

Port: 23 Transport Layer Protocol: TCP

- Legacy protocol used to “insecurely” connect to a remote host.
  - Data is transferred in clear text, so it’s considered insecure
  - Largely replaced by SSH
- Today it’s primarily used to access managed network devices, such as routers via a serial connection.
- Use TCP Port 23 by default

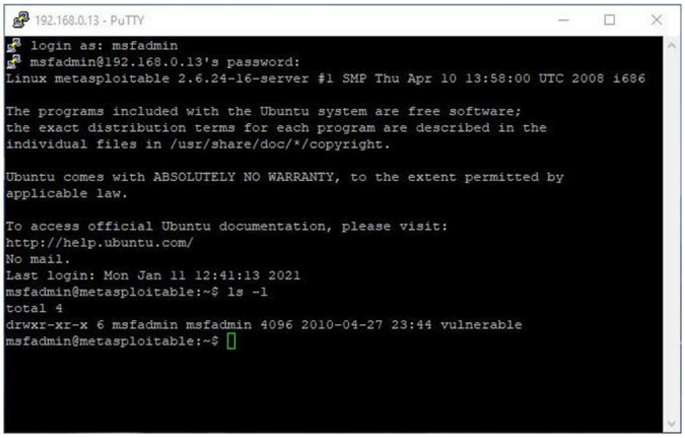


Host Name (or IP address)

Port: 23

Connection type: ○ Raw ● Telnet ○ Rlogin ○ SSH ○ Serial

Close window on exit: ○ Always ○ Never ● Only on clean exit

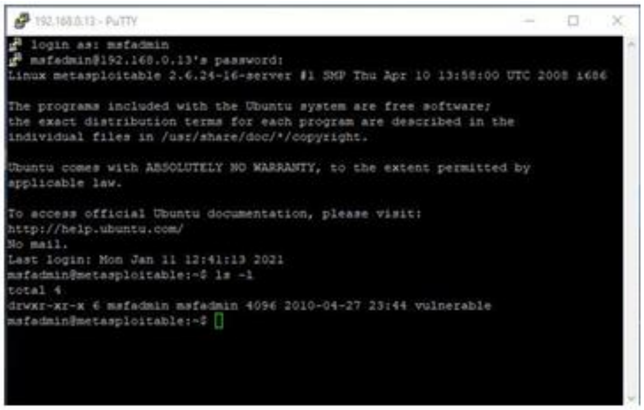


```
login as: msfadmin
msfadmin@192.168.0.13's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Mon Jan 11 12:41:13 2021
msfadmin@metasploitable:~$ ls -l
total 4
drwxr-xr-x 6 msfadmin msfadmin 4096 2010-04-27 23:44 vulnerable
msfadmin@metasploitable:~$
```

Secure Shell (SSH)

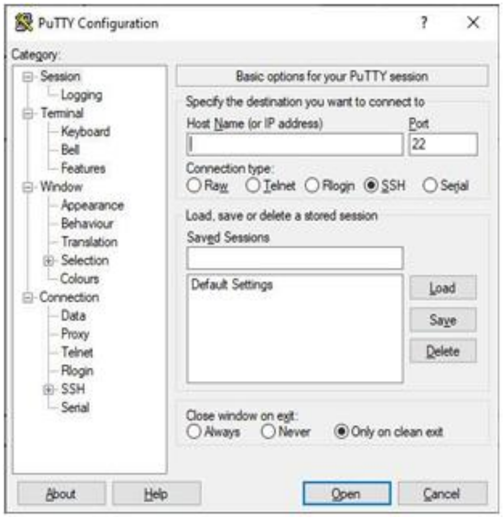
Port: 22 Transport Layer Protocol: TCP

- A cryptographic protocol that’s used to securely connect to a remote host.
  - Utilizes a terminal console
  - Typically Unix and Linux Machines, but also available on Windows and Mac OS
- Encrypts data with public key infrastructure (PKI), making it secure.
  - Considered secure replacement for Telnet.
- Uses TCP port 22 by default



192.168.0.13 - PuTTY

```
login as: msfadmin
msfadmin@192.168.0.13's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Mon Jan 11 12:41:13 2021
msfadmin@metasploitable:~$ ls -l
total 4
drwxr-xr-x 6 msfadmin msfadmin 4096 2010-04-27 23:44 vulnerable
msfadmin@metasploitable:~$
```



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address):

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

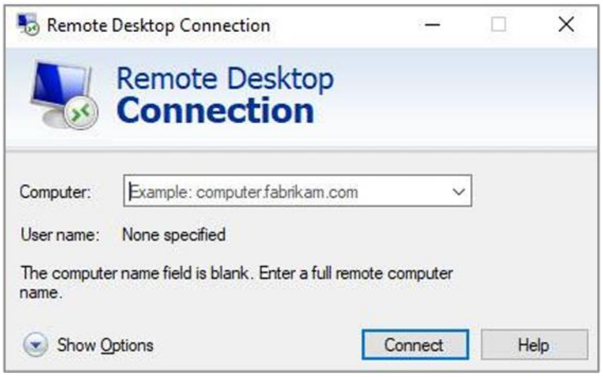
Saved Sessions: Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

Remote Desktop Protocol (RDP)

Port: 3389 Transport Layer Protocol: TCP

- A Microsoft protocol that allows users to remotely connect to, view, and control a remote computer from a Windows desktop.
- Built into the Microsoft operating system.
- Uses TCP port 3389 by default

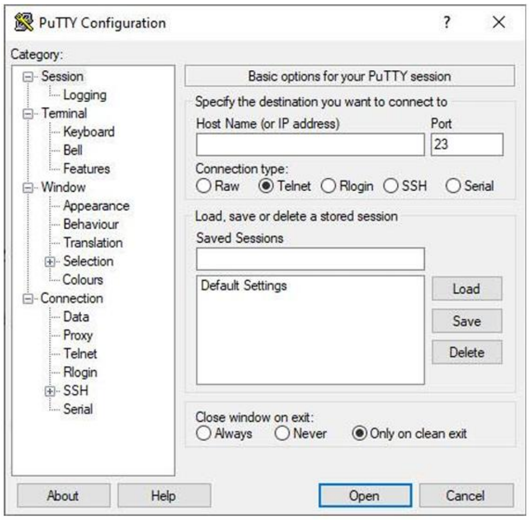


Remote Desktop Connection

Computer: Example: computer.fabrikam.com

User name: None specified

The computer name field is blank. Enter a full remote computer name.



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address):

Port: 23

Connection type: ○ Raw ● Telnet ○ Rlogin ○ SSH ○ Serial

Load, save or delete a stored session

Saved Sessions: Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

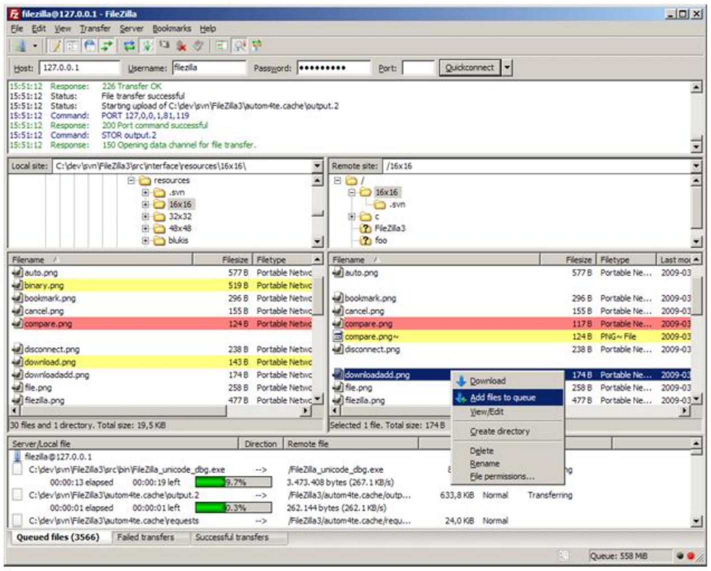
Application Layer File Transfer Protocols

- File Transfer Protocol (FTP)
- Secure File Transfer Protocol (SFTP)
- Trivial File Transfer Protocol (TFTP)

File Transfer Protocol (FTP)

Ports: 20, 21 Transport Layer Protocol: TCP

- Legacy protocol used to transfer files between systems.
  - Slowly being replaced by Secure FTP (SFTP)
- Can authenticate with a username and password or utilize anonymous logins.
- Data is transferred in clear text, so it's considered insecure.
- Full-featured functionality:
  - View, list, add, delete, etc. files and folders
- Uses two TCP ports by default:
  - **Port 20 for Data:** Data Transfers
  - **Port 21 for Control:** Commands



Host: 127.0.0.1 Username: filezilla Password: ••••••••• Port:

```
15:51:12  Response:  226 Transfer OK
15:51:12  Status:    File transfer successful
15:51:12  Status:    Starting upload of C:\dev\svn\FileZilla3\autom4te.cache\output.2
15:51:12  Command:   PORT 127,0,0,1,81,119
15:51:12  Response:  200 Port command successful
15:51:12  Command:   STOR output.2
15:51:12  Response:  150 Opening data channel for file transfer.
```

Local site: C:\dev\svn\FileZilla3\src\interface\resources\16x16\

```
resources
  .svn
  16x16
  32x32
  48x48
  blukis
```

Remote site: /16x16

```
/
  16x16
    .svn
  c
  FileZilla3
  foo
```

Filename	Filesize	Filetype
auto.png	577 B	Portable Netwc
binary.png	519 B	Portable Netwc
bookmark.png	296 B	Portable Netwc
cancel.png	155 B	Portable Netwc
compare.png	124 B	Portable Netwc
disconnect.png	238 B	Portable Netwc
download.png	143 B	Portable Netwc
downloadadd.png	174 B	Portable Netwc
file.png	258 B	Portable Netwc
filezilla.png	477 B	Portable Netwc

30 files and 1 directory. Total size: 19,5 KiB

Filename	Filesize	Filetype	Last moc
auto.png	577 B	Portable Ne...	2009-03
bookmark.png	296 B	Portable Ne...	2009-03
cancel.png	155 B	Portable Ne...	2009-03
compare.png	117 B	Portable Ne...	2009-03
compare.png~	124 B	PNG~ File	2009-03
disconnect.png	238 B	Portable Ne...	2009-03
downloadadd.png	174 B	Portable Ne...	2009-03
file.png	258 B	Portable Ne...	2009-03
filezilla.png	477 B	Portable Ne...	2009-03

Selected 1 file. Total size: 174 B

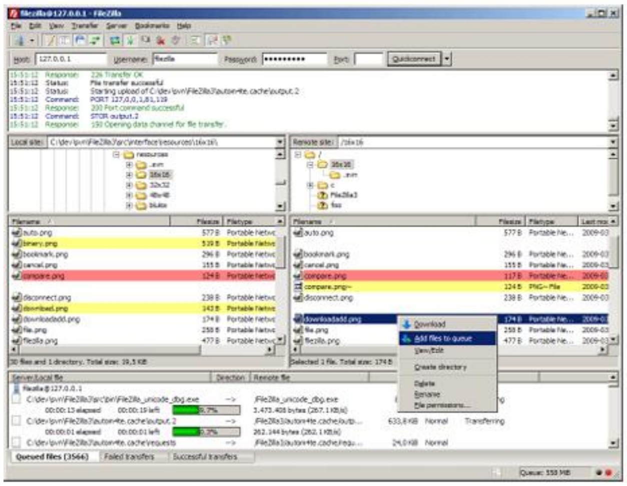
```
Server/Local file                                Direction  Remote file
filezilla@127.0.0.1
C:\dev\svn\FileZilla3\src\bin\FileZilla_unicode_dbg.exe  -->  /FileZilla_unicode_dbg.exe
    00:00:13 elapsed   00:00:19 left   9.7%     3.473.408 bytes (267.1 KB/s)
C:\dev\svn\FileZilla3\autom4te.cache\output.2     -->  /FileZilla3/autom4te.cache/outp...  633,8 KiB  Normal  Transferring
    00:00:01 elapsed   00:00:01 left   0.3%     262.144 bytes (262.1 KB/s)
C:\dev\svn\FileZilla3\autom4te.cache\requests     -->  /FileZilla3/autom4te.cache/requ...  24,0 KiB   Normal
```

Queue: 558 MiB

Secure File Transfer Protocol (SFTP)

Port: 22 Transport Layer Protocol: TCP

- A secure cryptographic version of FTP that uses SSH to provide encryption services.
  - Provides file transfer over SSH
- Uses TCP port 22 by default (same port as SSH)


Host: 127.0.0.1 Username: filezilla Password: ••••••••• Port:

```
15:51:12  Response:  226 Transfer OK
15:51:12  Status:    File transfer successful
15:51:12  Status:    Starting upload of C:\dev\svn\FileZilla3\autom4te.cache\output.2
15:51:12  Command:   PORT 127,0,0,1,81,119
15:51:12  Response:  200 Port command successful
15:51:12  Command:   STOR output.2
15:51:12  Response:  150 Opening data channel for file transfer.
```

Local site: C:\dev\svn\FileZilla3\src\interface\resources\16x16\

Remote site: /16x16

30 files and 1 directory. Total size: 19,5 KiB

Selected 1 file. Total size: 174 B

Queue: 558 MiB

Trivial File Transfer Protocol (TFTP)

Port: 69 Transport Layer Protocol: UDP

- A bare-bones version of FTP used for simple downloads,
    - Doesn’t support authentication,
    - Doesn’t support directory navigation.
- Requires that you request the exact file (and location).
- Often used to transfer software images for routers and switches during upgrades.
- Utilizes UDP port 69 by default.

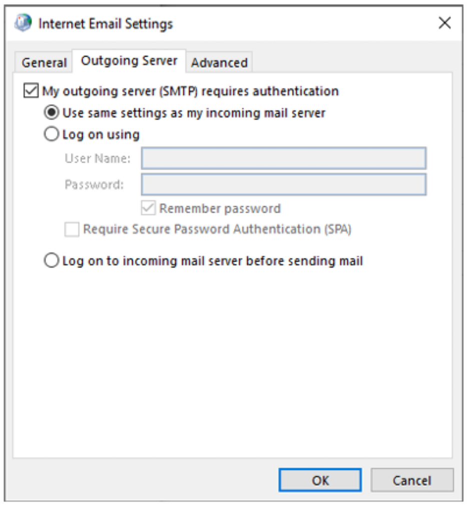
Application Layer Email Protocols

- Simple Mail Transfer Protocol (SMTP)
- Post Office Protocol Version 3 (POP3)
- Internet Message Access Protocol (IMAP)

Simple Mail Transfer Protocol (SMTP)

Port: 25 Transport Layer Protocol: TCP

- Email protocol that is used to deliver emails from an email client (Outlook) to a destination email server
- Can be configured to use encryption (recommended) or plain text
- Uses TCP Port 25 by default



☑ My outgoing server (SMTP) requires authentication

● Use same settings as my incoming mail server

○ Log on using

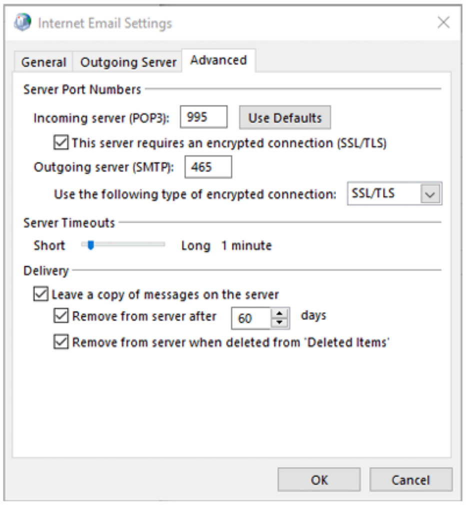
User Name:

Password:

☑ Remember password

☐ Require Secure Password Authentication (SPA)

○ Log on to incoming mail server before sending mail



Server Port Numbers

Incoming server (POP3): 995

☑ This server requires an encrypted connection (SSL/TLS)

Outgoing server (SMTP): 465

Use the following type of encrypted connection: SSL/TLS

Server Timeouts

Short Long 1 minute

Delivery

☑ Leave a copy of messages on the server

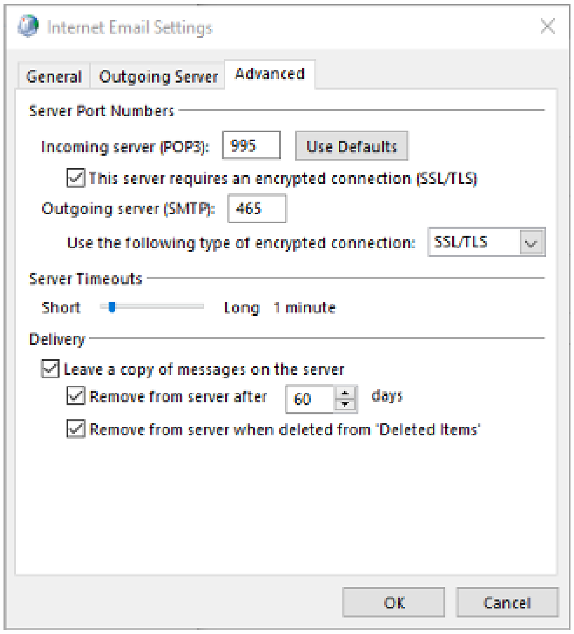
☑ Remove from server after 60 days

☑ Remove from server when deleted from 'Deleted Items'

Post Office Protocol Version 3 (POP3)

Port: 110 Transport Layer Protocol: TCP

- Email protocol that is used to retrieve emails from an email server
- Can be configured to use encryption (recommended) or plain text
- Uses TCP Port 110 by default



Server Port Numbers

Incoming server (POP3): 995

☑ This server requires an encrypted connection (SSL/TLS)

Outgoing server (SMTP): 465

Use the following type of encrypted connection: SSL/TLS

Server Timeouts

Short Long 1 minute

Delivery

☑ Leave a copy of messages on the server

☑ Remove from server after 60 days

☑ Remove from server when deleted from 'Deleted Items'

Internet Message Access Protocol (IMAP)

Port: 143 Transport Layer Protocol: TCP

- Another email protocol that is quickly replacing POP3.
- Allows users to access email on servers and either read the email on the server or download the email to the client machine.
- Popular when a user accesses email from multiple different devices.
- Web-based email clients, such as Gmail, use IMAP.
- Uses TCP port 143 by default.

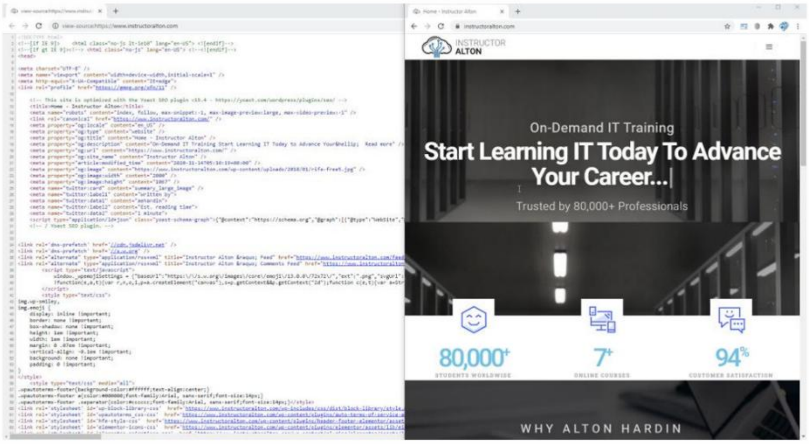
Application Layer Web Browser Protocol

- Hypertext Transfer Protocol (HTTP)
- HTTP Secure (HTTPS)

Hypertext Transfer Protocol (HTTP)

Port: 80 Transport Layer Protocol: TCP

- Protocol that provides browsing services for the World Wide Web (WWW)
  - Retrieves the content of a web page from a web server.
  - Requests are made in hypertext markup language (HTML) and returned to your browser in that format.
- Data is sent in plain text.
- Uses TCP Port 80 by default.


view-source:https://www.instructoralton.com
instructoralton.com
INSTRUCTOR ALTON
On-Demand IT Training
Start Learning IT Today To Advance Your Career...|
Trusted by 80,000+ Professionals
80,000+
7+
94%
WHY ALTON HARDIN

HTTP Secure (HTTPS)

Port: 443 Transport Layer Protocol: TCP

- HTTP over Secure Socket Layer (SSL) or Transport Layer Security (TLS)
- A secure version of HTTP that utilizes SSL/TLS to encrypts HTTP content
- Utilizes Public Key Infrastructure (PKI)
- Uses TCP Port 443 by default