Management Protocols

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)

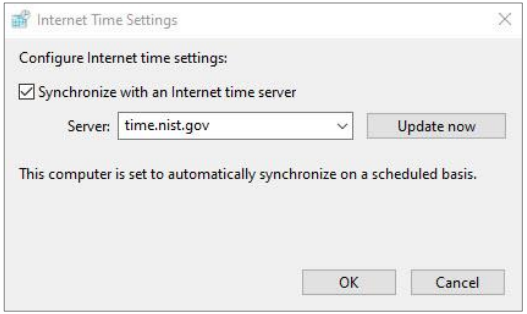
Ports: 67, 68 **Transport Layer Protocol:** UDP

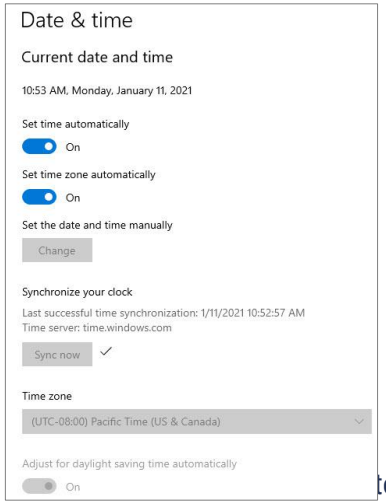
- Protocol that automatically assigns IP address configurations to devices on a network:
  - IP Address
  - Subnet Mask
  - Default Gateway
  - DNS Server
- We'll be discussing how DHCP works in detail in the **Assigning IP Addresses** section of this course
- Uses two UDP ports 67 and 68 by default

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.





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

Remote Communication Protocols

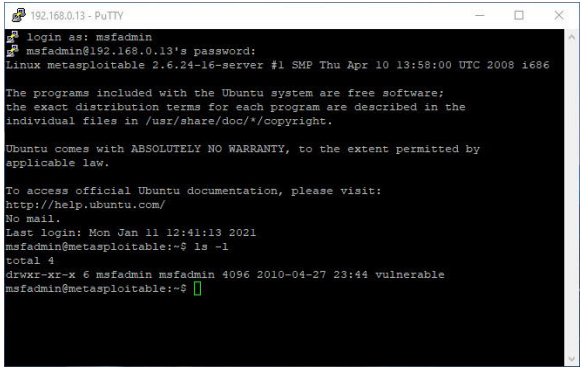
Application Layer Remote Communication Protocols

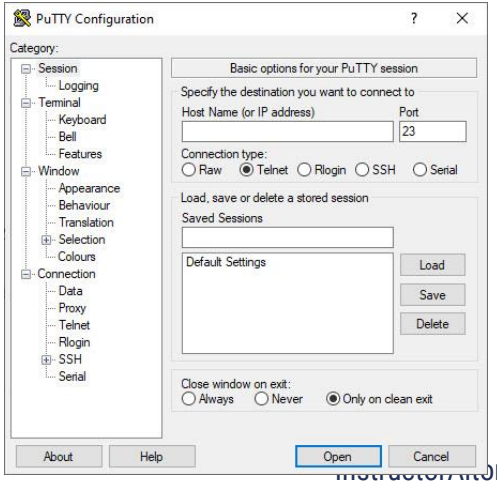
- Telnet
- Secure Shell (SSH)
- Remote Desktop Protocol (RDP)

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



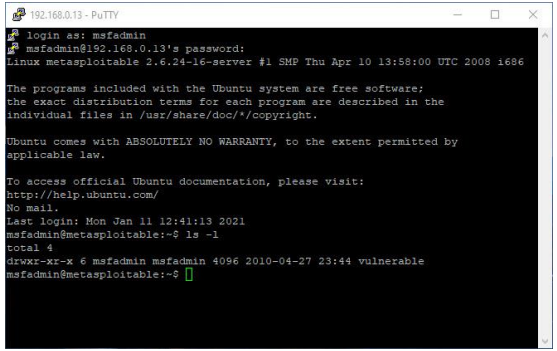


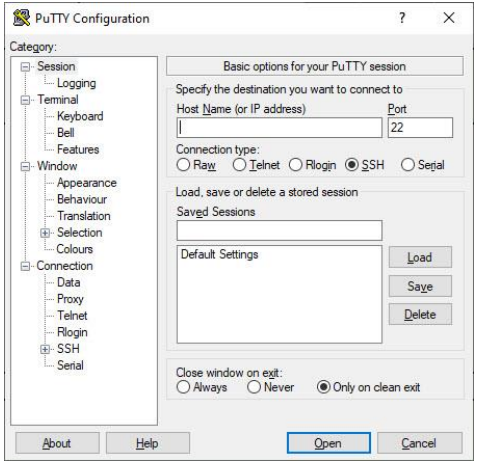
INSTRUCTOR ALTON

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



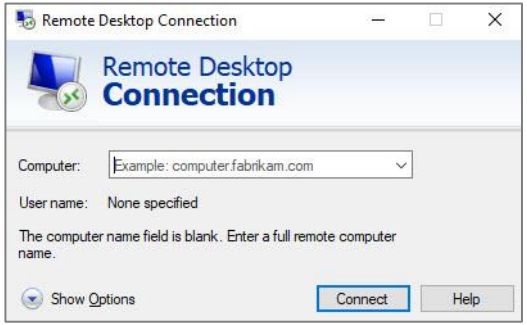


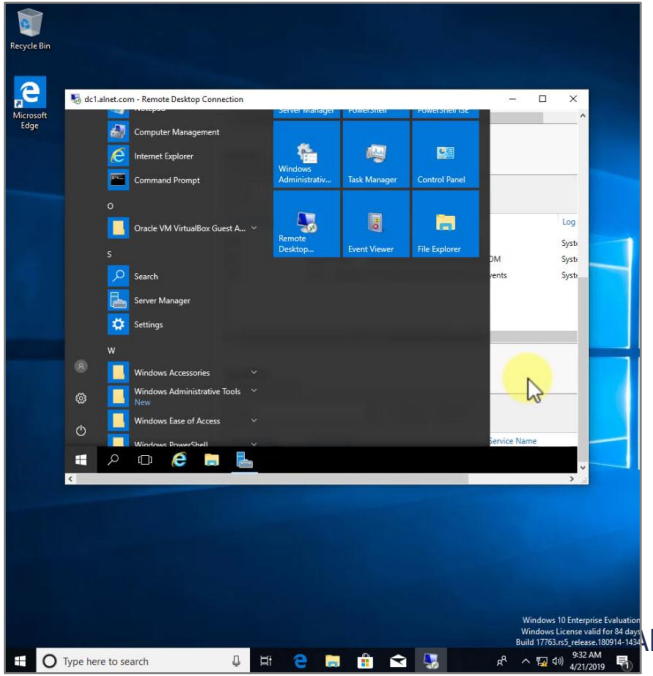
INSTRUCTOR ALTON

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





File Transfer Protocols

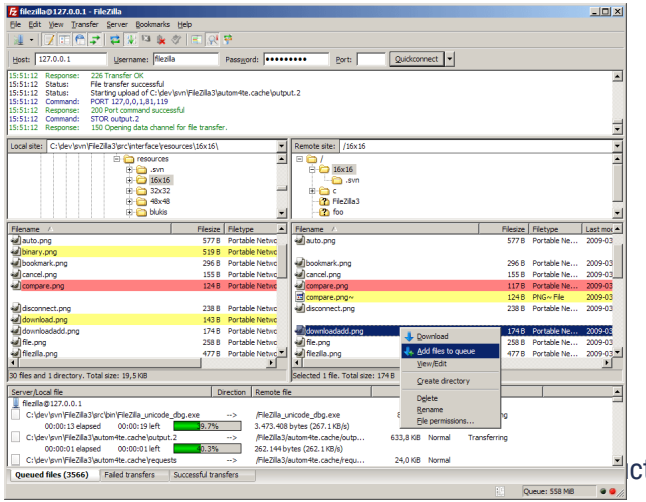
Application Layer File Transfer Protocols

- 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

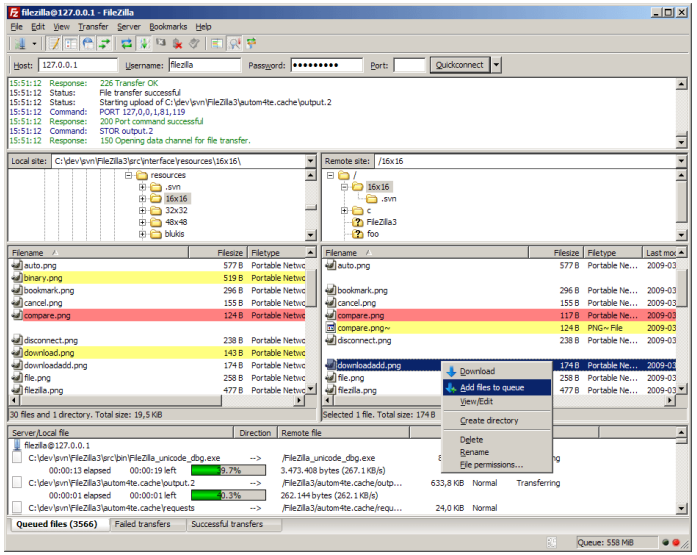
- Legacy protocol used to transfer files between systems
  - Slowly being replaced by Secure FTP (SFTP)
- Can authenticate with a username and password or utilize anonymous logins
- Data is transferred in clear text, so it's considered insecure
- Full-featured functionality:
  - View, list, add, delete,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



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)



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

Email Protocols

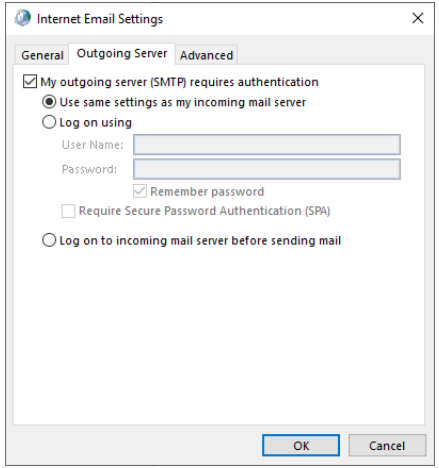
Application Layer Email Protocols

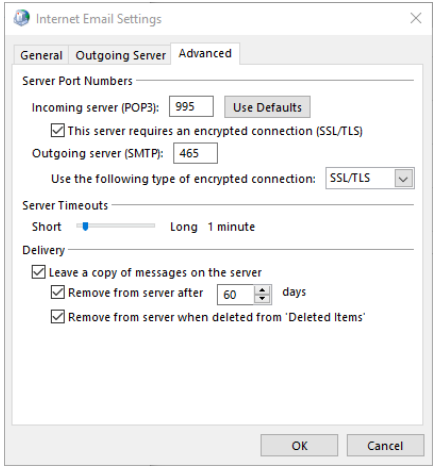
- Simple Mail Transfer Protocol (SMTP)
- Post Office Protocol Version 3 (POP3)
- Internet Message Access Protocol (IMAP)

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

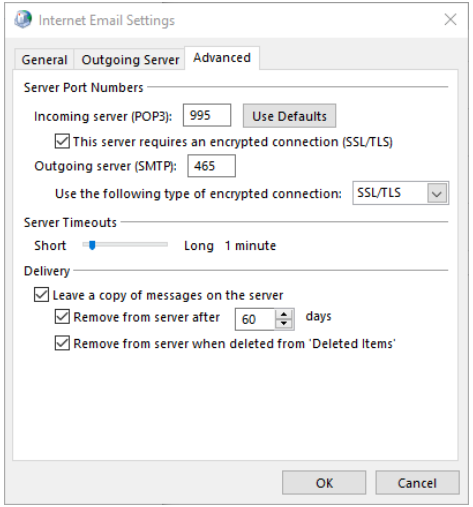




Post Office Protocol Version 3 (POP3)

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



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

Web Browser Application Protocols

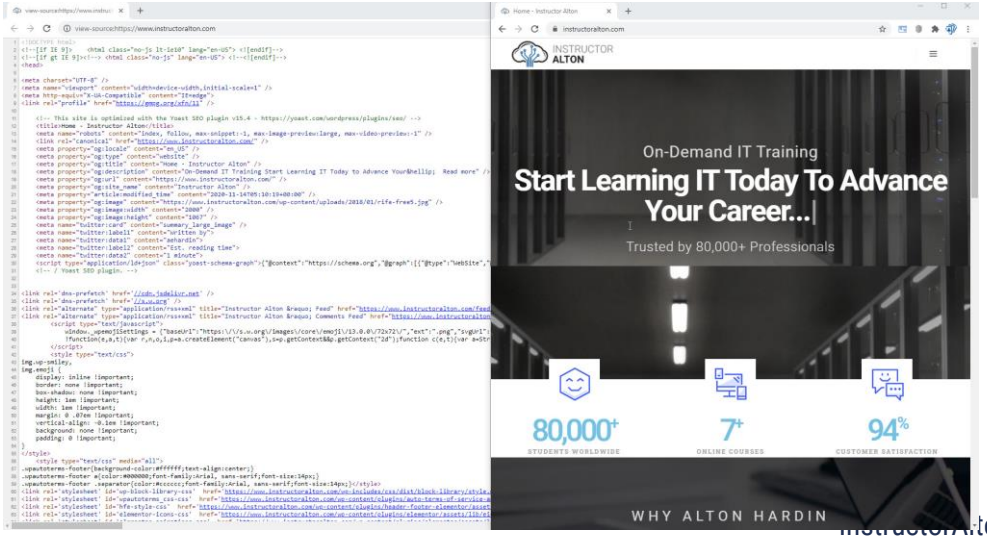
Application Layer Web Browser Protocols

- 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



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