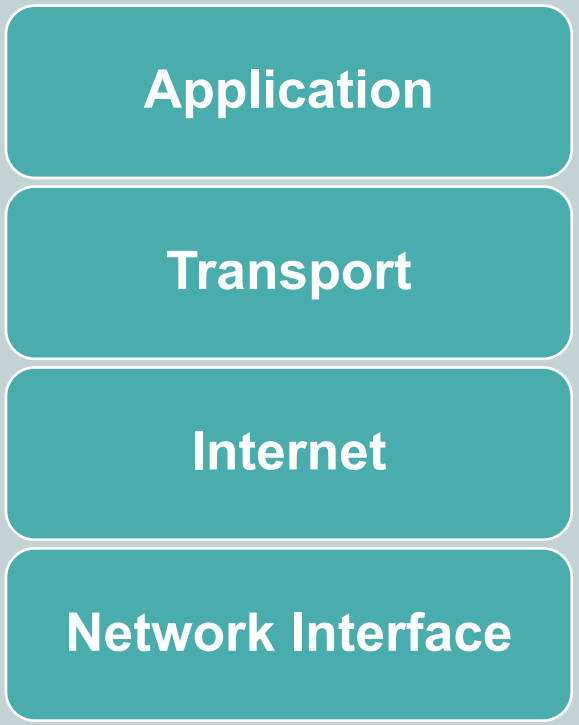
TCP/IP Model

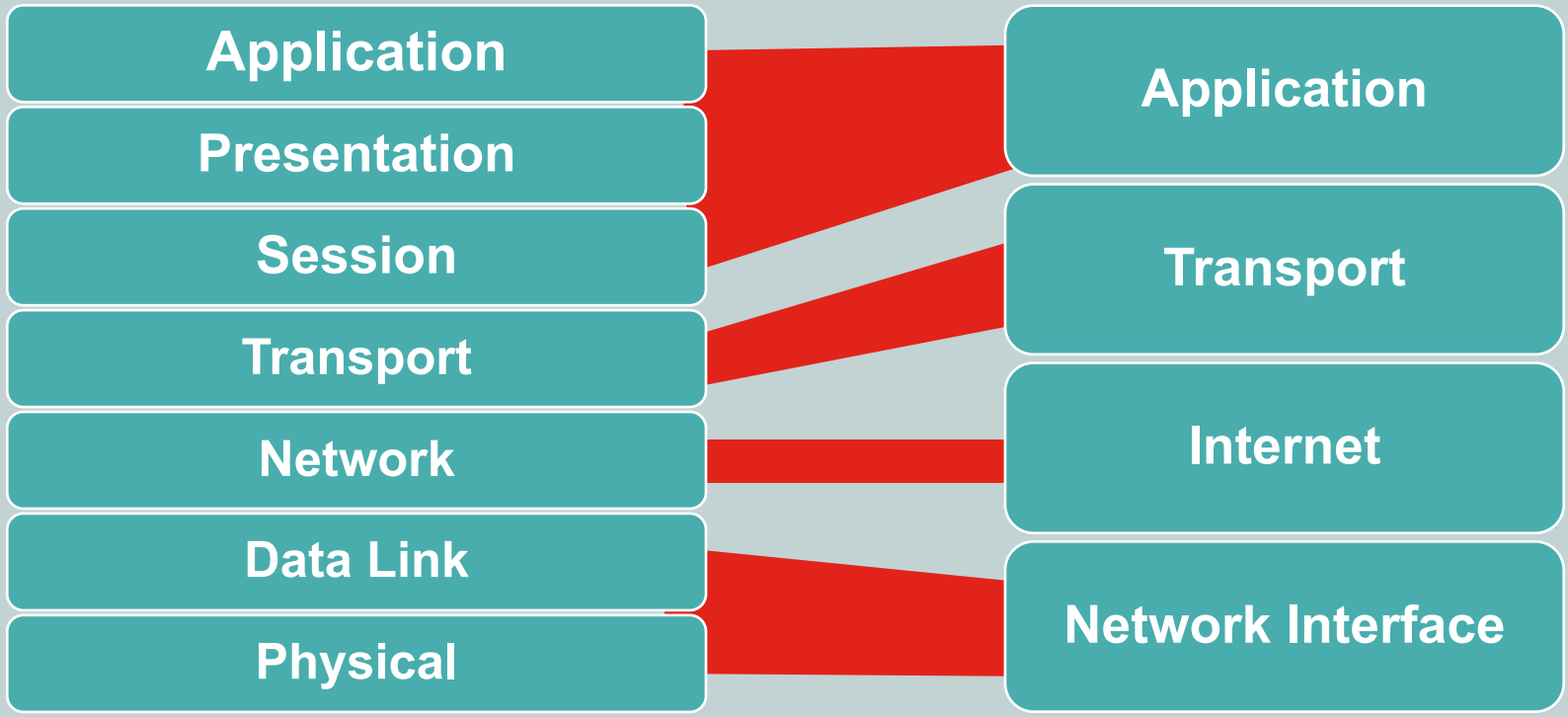
CompTIA Network+ (N10-007)

TCP/IP Model

- Also known as TCP/IP stack or the DoD Model
- Alternative to the OSI Model
- More relevant model for network designers since it's based on TCP/IP
- Only a 4 layer model



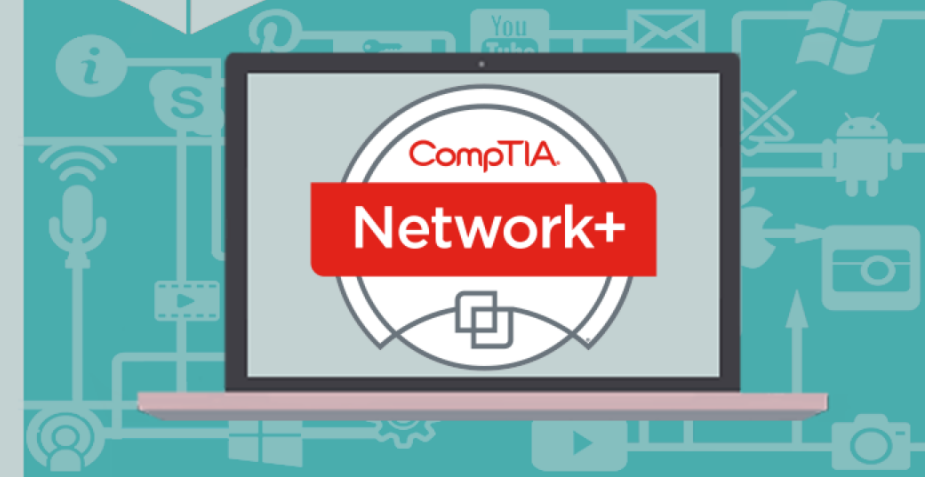
OSI Model to TCP/IP Model



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Network Interface (Layer 1)

- Physical and electrical characteristics
- Describes how to transmit bits across the network (1's and 0's)
- Determines how interface uses network medium
  - Coaxial, Optical fiber, or Twisted-pair copper cabling
- Examples:
  - Ethernet, Token Ring, FDDI, RS-232

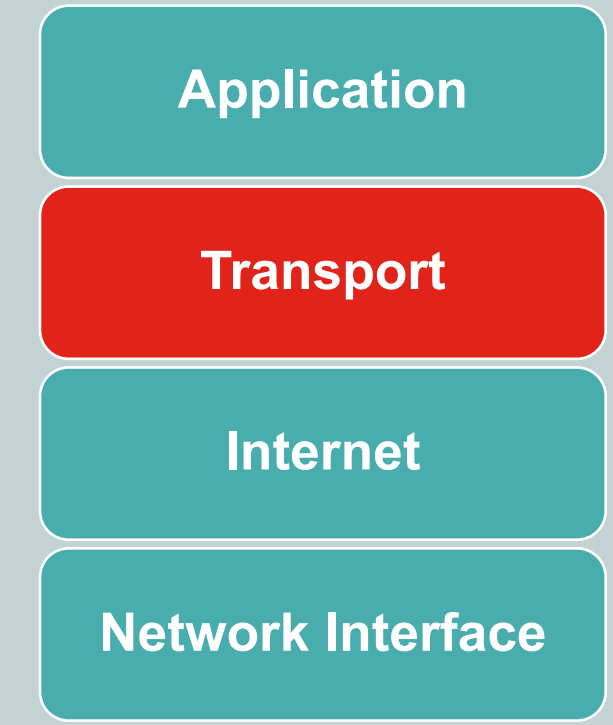


Internet (Layer 2)

- Packages data into IP datagrams
  - Contains source and destination IPs
  - Forwards datagrams between hosts across the networks
- Routes IP datagrams across networks
- Connectivity occurs externally
- Examples:
  - IP, ICMP, ARP, RARP

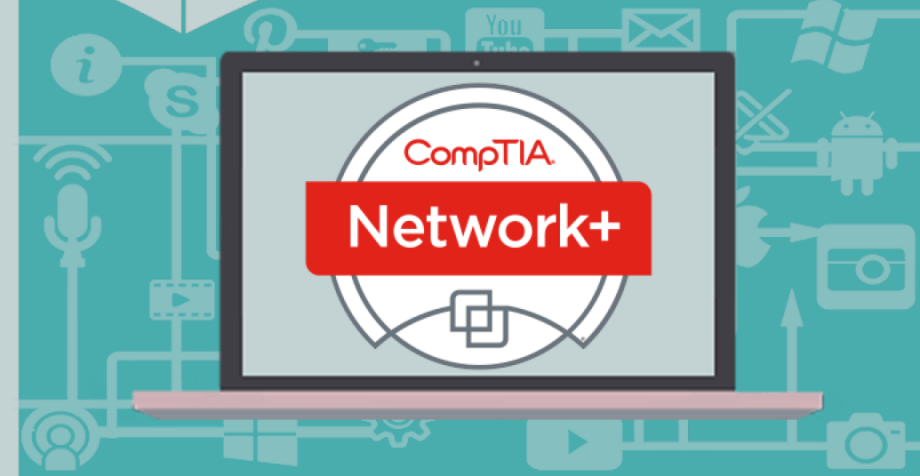
Transport (Layer 3)

- Provides communication session management between hosts
- Defines level of service and status of connection used for transport
- Examples:
  - TCP
  - UDP
  - RTP

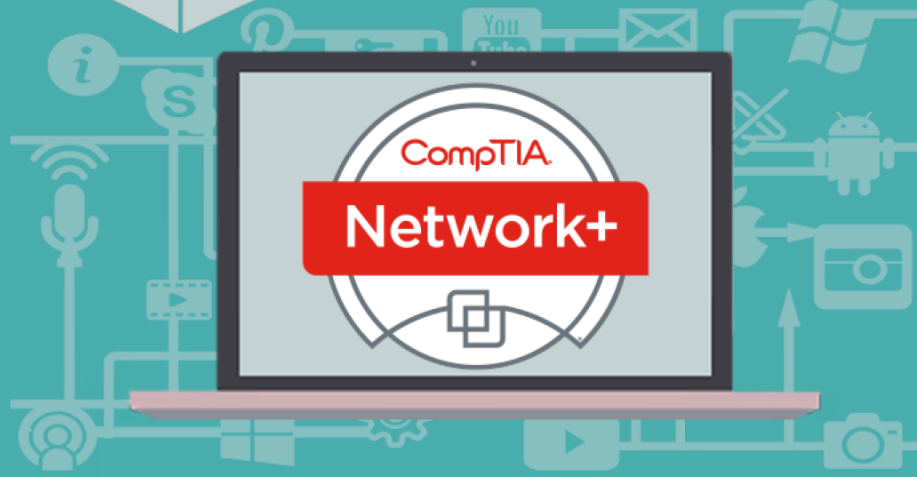


Application (Layer 4)

- Defines TCP/IP application protocols
- Defines how programs interface with the transport layer service
- Layer with which the user interacts
- Examples:
  - HTTP, TELNET, FTP, SNMP, DNS, SMTP, SSL, TLS, …



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE



Data Transfer Over Networks

CompTIA Network+ (N10-007)

Ports

- Port numbers can be 0 to 65,536
- “Well-known” & Reserved Ports
  - Ports 0 to 1024

- Ephemeral Ports
  - Short-lived transport port that is automatically selected from a predefined range
  - Ports 1025 to 65,536

Data Transfer

Client

192.168.1.24

Website

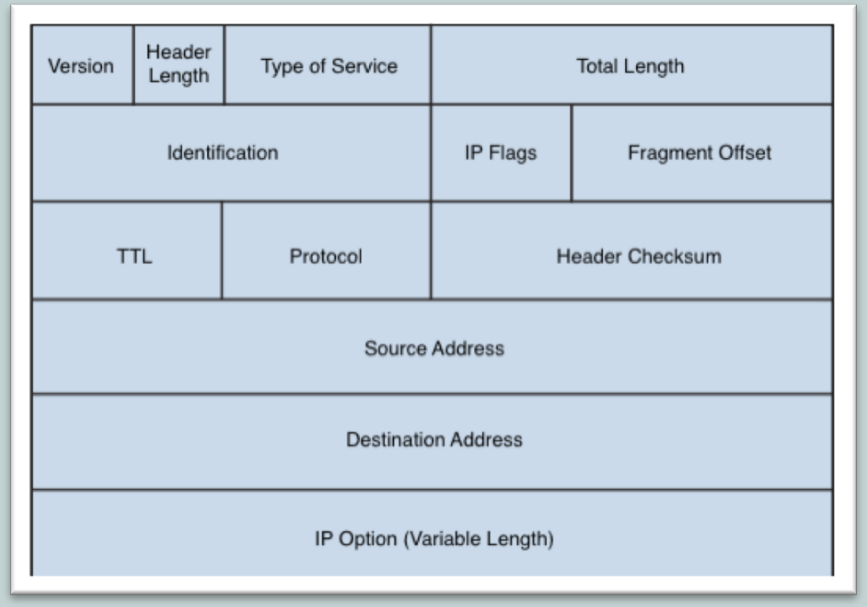
64.82.46.21

Source IP: 192.168.1.24
Source Port: 49163
Destination IP: 64.82.46.21
Destination Port: 80

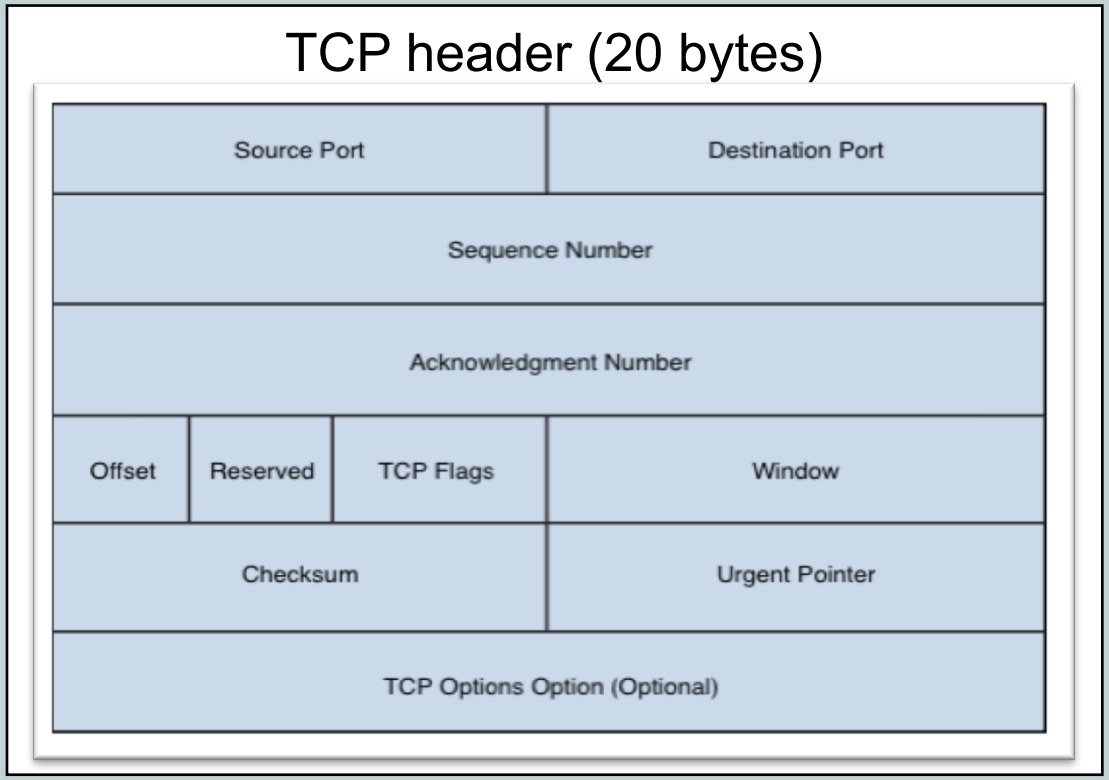
Source IP: 64.82.46.21
Source Port: 80
Destination IP: 192.168.1.24
Destination Port: 49163

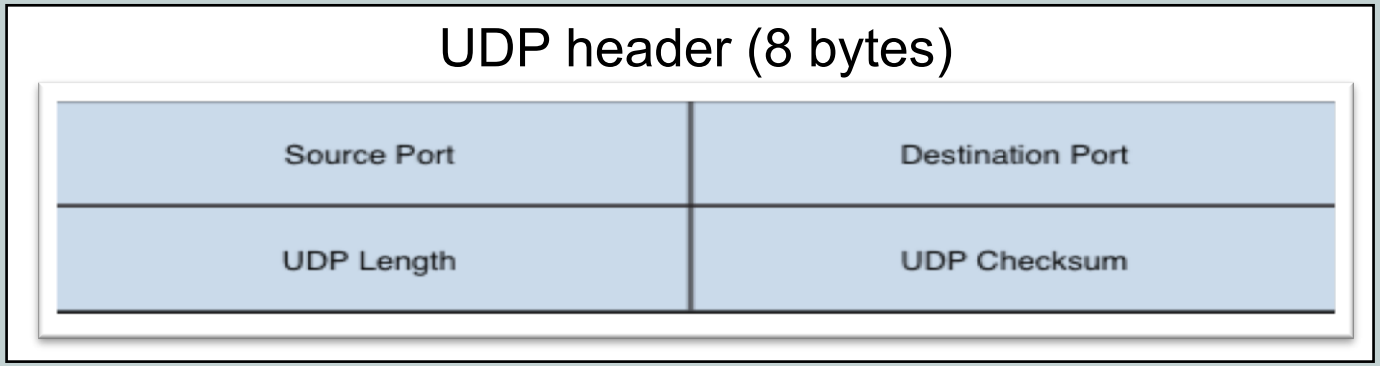
IPv4 Packets

- Source Address
  - IP of sender
- Destination Address
  - IP of receiver
- IP Flags
  - Allows packet fragmentation
- Protocol
  - Is this packet using TCP or UDP?



Overhead of TCP and UDP





Ports and Protocols

CompTIA Network+ (N10-007)

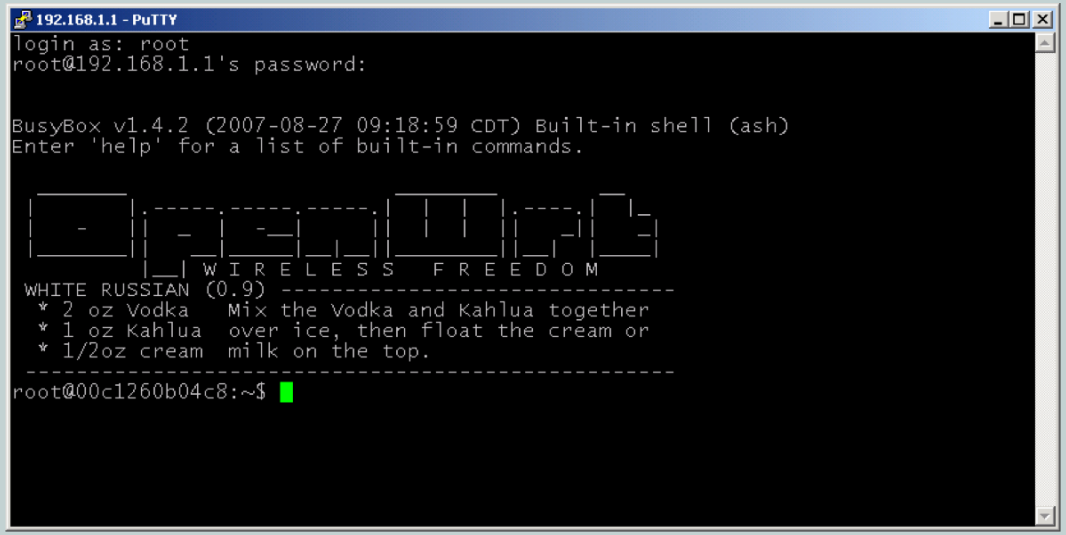
File Transfer Protocol
FTP (Port 20, 21)

- Transfers computer files between a client and server on a computer network
- Unsecure method
- Data transferred in the clear

Secure Shell
SSH (Port 22)

- Cryptographic network protocol for operating network services securely over an unsecured network

- Best known for remote login to computer systems by users

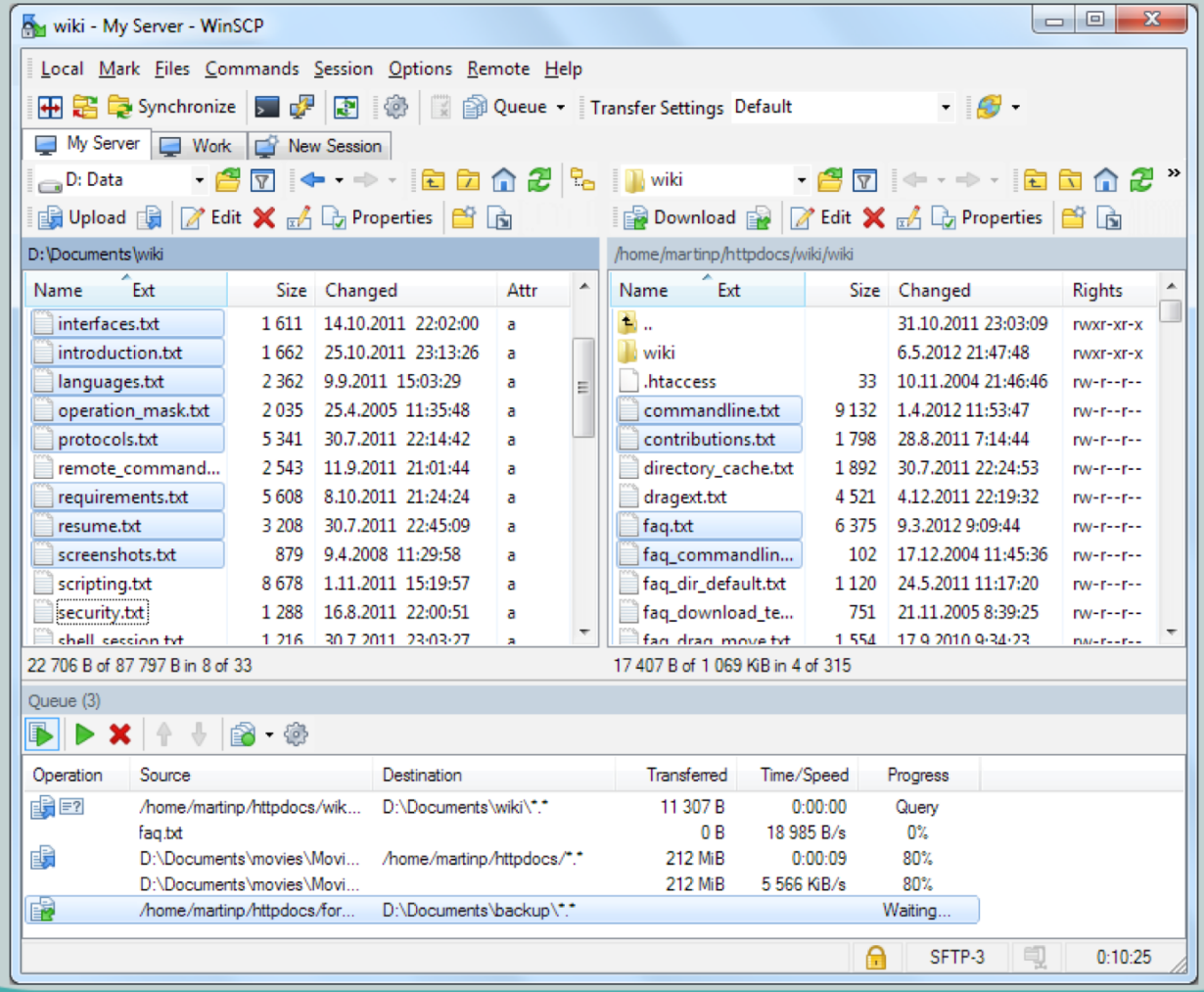


JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

CompTIA
Network+

SSH File Transfer Protocol SFTP (Port 22)

- Provides file access, file transfer, and file management over any reliable data stream



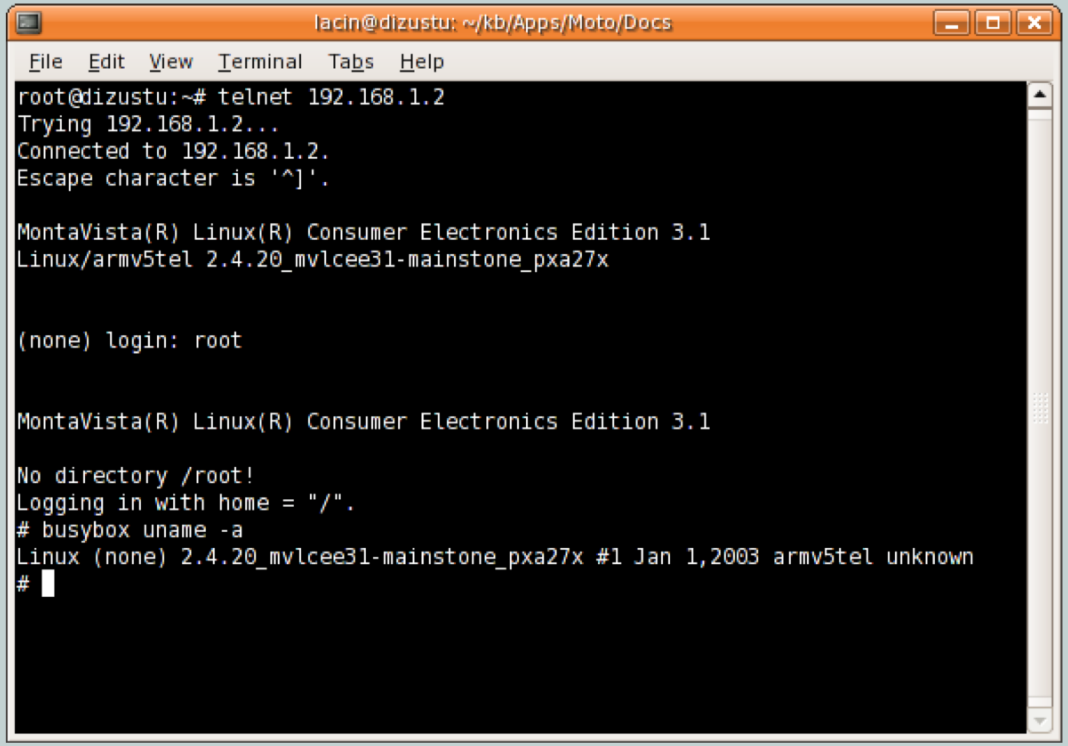
JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

CompTIA Network+

Telnet (Port 23)

- Provides bidirectional interactive text-oriented communication facility using a virtual terminal connection

- Like SSH, but insecure



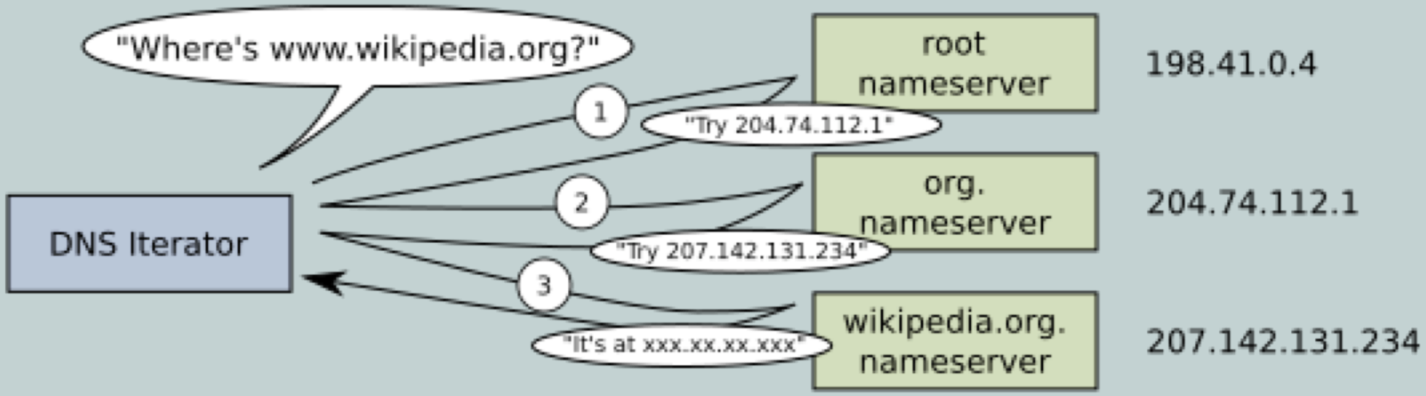
Simple Mail Transfer Protocol SMTP (Port 25)

- Internet standard for sending electronic mail
- RFC 821 was defined originally in 1982
- RFC 5321 developed in 2008 (current version)

Domain Name Service
DNS (Port 53)

- Hierarchical decentralized naming system for computers, services, or other resources connected to the Internet or a private network

- Converts domain names to IP addresses

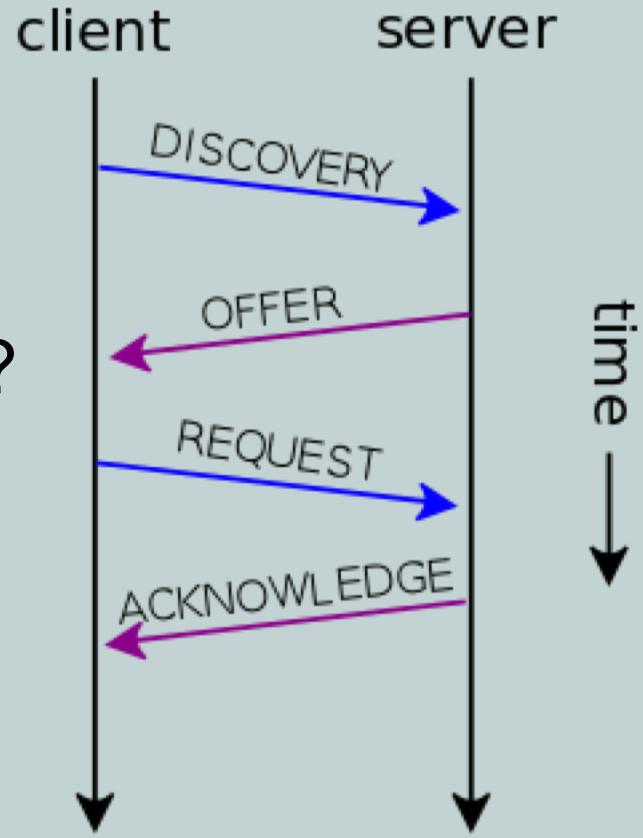


JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

CompTIA Network+

Dynamic Host Control
DHCP (Port 67, 68)

- DHCP server dynamically assigns an IP address and other network configuration parameters to a client
- Enables computers to request IP addresses and networking parameters automatically?
- Reduces burden on network administrators



Trivial File Transfer TFTP (Port 69)

- Transmits files in both directions of a client-server application
- Used for booting an operating system from a local area network file server
- Doesn't provide user authentication or directory visibility
- Essentially a stripped down version of FTP

Hyper Text Transfer HTTP (Port 80)

- Foundation of data communication for WWW
- Designed for distributed, collaborative, and hypermedia presentation across many devices

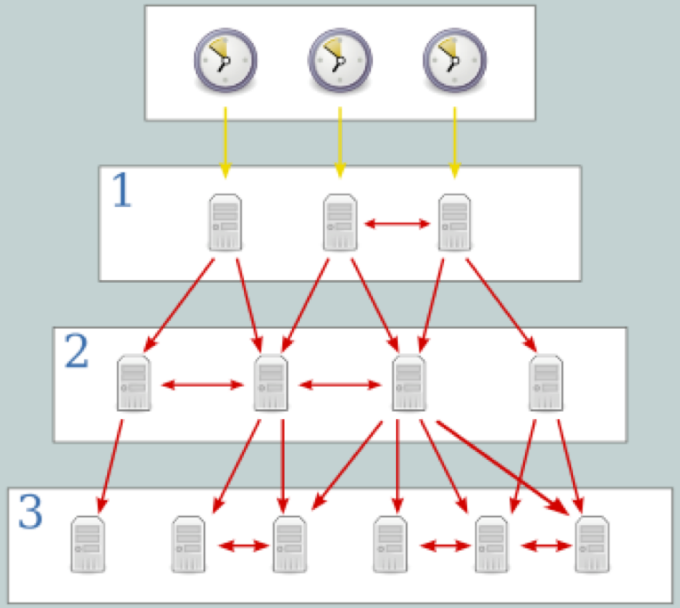
Post Office Protocol v3 POP3 (Port 110)

- Used by local e-mail clients to retrieve e-mail from a remote server over TCP/IP connection

Network Time Protocol
NTP (Port 123)

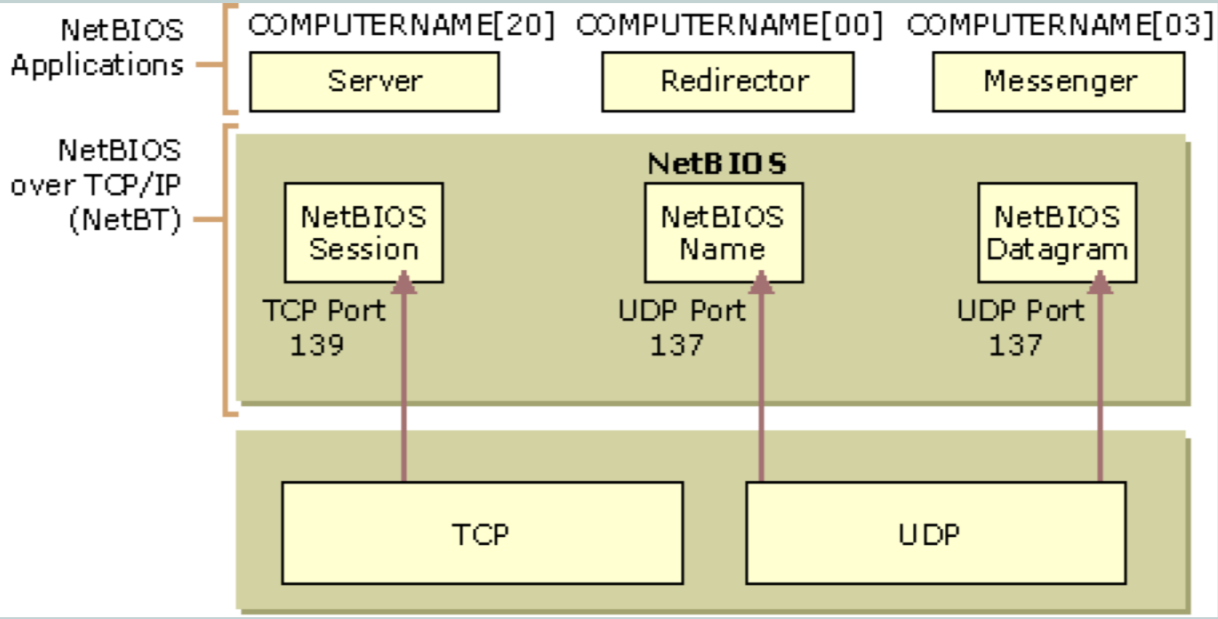
- Provides clock synchronization between computer systems over packet-switched, variable-latency data networks

- Created in 1985, one of the oldest Internet protocols in current use



NetBIOS (Port 139)

- Network Basic Input/Output System
- Provides services allowing applications on separate computers to communicate over a local area network for file and printer sharing



Internet Mail Application IMAP (Port 143)

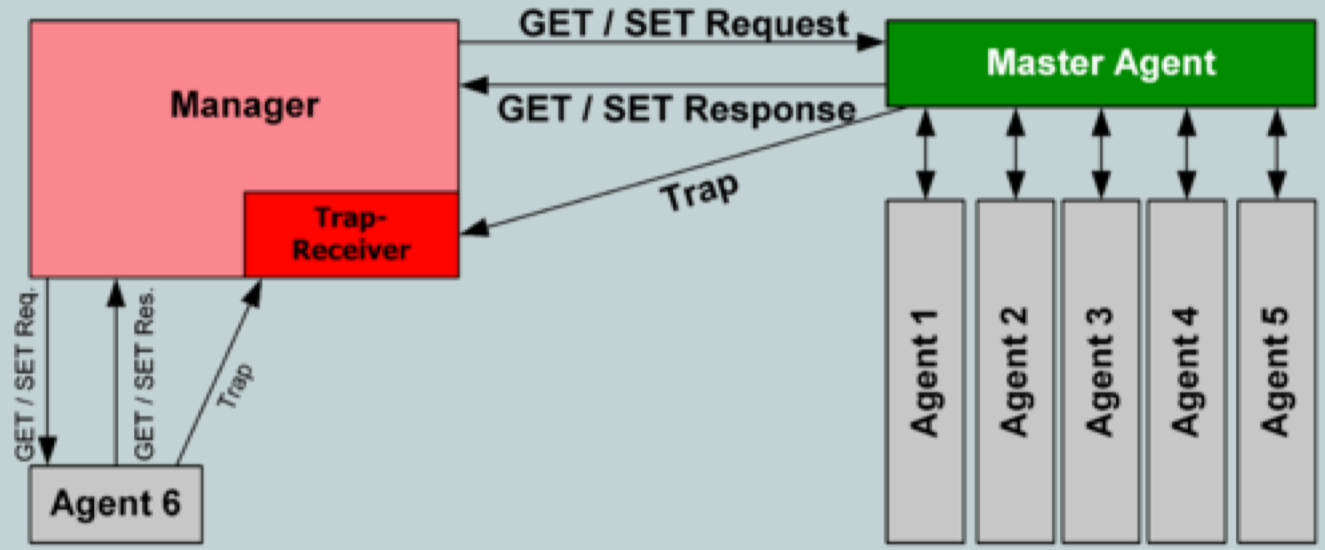
- Provides e-mail clients to retrieve e-mail messages from a mail server over a TCP/IP connection

- Allows the end user to view and manipulate the messages as if they're stored locally

Simple Network Management SNMP (Port 161)

- Provides collection and organization of information about managed devices on IP networks

- Can modify that information to change device behavior, commonly used in network devices



Lightweight Directory Access LDAP (Port 389)

- Open, vendor-neutral, industry standard for accessing and maintaining distributed directory information services

- LDAP and Active Directory use this port

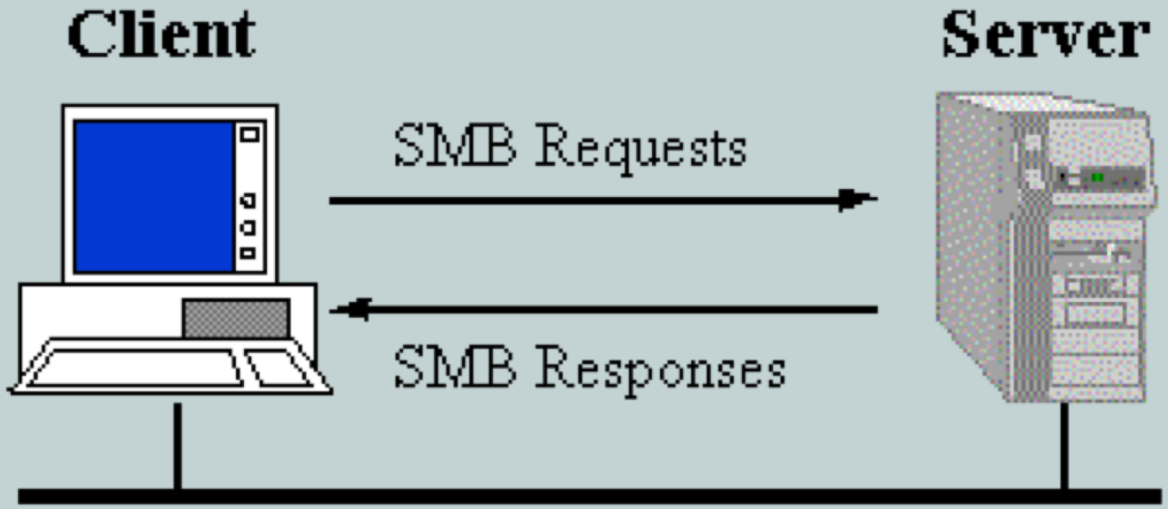
HTTP Secure
HTTPS (Port 443)

- Foundation of ecommerce on WWW

- Designed for adding security to the insecure HTTP protocol

Server Message Block SMB (Port 445)

- Provides shared access to files, printers, and miscellaneous communications between devices on a network



LDAP Secure
LDAPS (Port 636)

- Open, vendor-neutral, industry standard for accessing and maintaining distributed directory information services

- LDAP and Active Directory use this port

Remote Desktop Protocol RDP (Port 3389)

- Proprietary protocol developed by Microsoft
- Provides a user with a graphical interface to connect to another computer over a network connection
- User employs RDP client software for this purpose and the other computer must run RDP server software

Session Initiation Protocol SIP (Port 5060, 5061)

- Provides signaling and controlling multimedia communication sessions in applications

- Used for Internet telephony for voice and video calls, VOIP, and instant messaging

Ports to Remember

Service	Description	Port Number
FTP	File Transfer	20, 21
SSH	Secure Remote Access	22
SFTP	Secure File Transfer Protocol	22
Telnet	Unsecure Remote Access	23
SMTP	Sending Emails	25
DNS	Domain Name Service	53
DHCP	Dynamic Host Control Protocol	67, 68
TFTP	Trivial File Transfer	69
HTTP	Web Browsing	80
POP3	Receiving Emails	110

Ports to Remember

Service	Description	Port Number
NTP	Network Time Protocol	123
NETBIOS	Windows File Sharing	139
IMAP	Receiving Emails	143
SNMP	Network Management	161
LDAP	Directory Services	389
HTTPS	Secure Web Browsing	443
SMB	Windows File Sharing	445
LDAPS	LDAPS	636
RDP	Remote Desktop	3389
SIP	Real-time Audio (VOIP)	5060, 5061