CompTIA Network+ Exam N10-008

Lesson 9

Explaining Transport Layer Protocols

Objectives

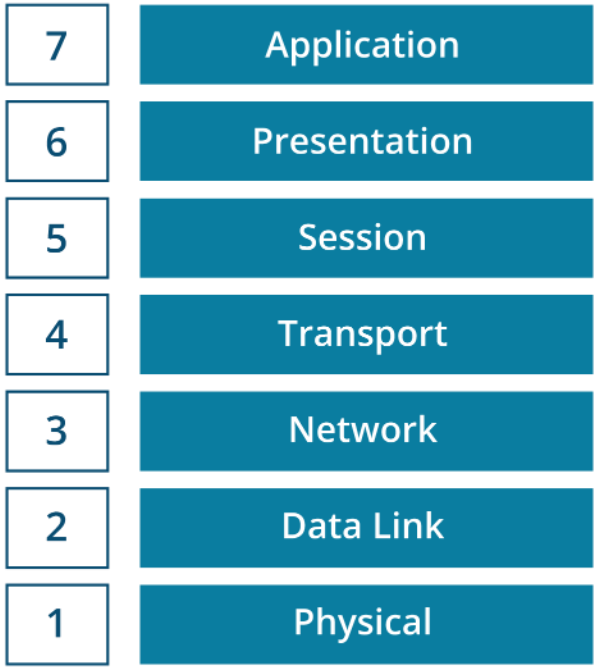
- Compare and contrast transport protocols
- Use appropriate tools to scan network ports

Lesson 9

Topic 9A

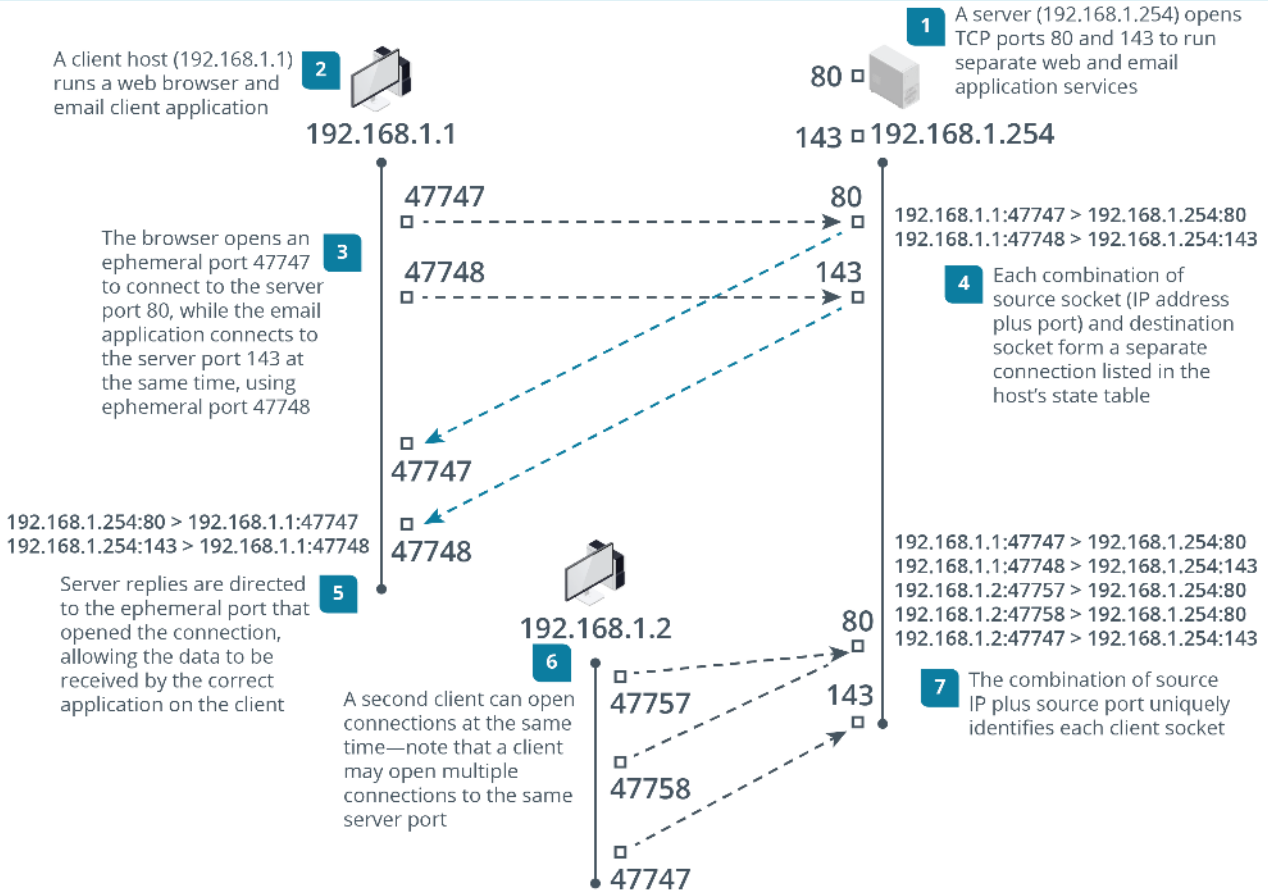
Compare and Contrast Transport Protocols

Open Systems Interconnection Model



Transport Layer Ports and Connections

- Identify individual applications as port numbers
- Socket
  - Source IP plus port bound to software process
- Connection
  - Client IP and port connected to server IP and port



Transmission Control Protocol

- Connection-oriented, guaranteed delivery
- Segments with header fields to track sequence and acknowledgements

TCP Handshake and Teardown

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\administrator>netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       652
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5985           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:47001          0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       428
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       912
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       864
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       1996
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING       524
  TCP    0.0.0.0:49703          0.0.0.0:0              LISTENING       516
  TCP    0.0.0.0:49706          0.0.0.0:0              LISTENING       524
  TCP    10.1.0.100:139         0.0.0.0:0              LISTENING       4
  TCP    10.1.0.100:49764       10.1.0.192:3000        ESTABLISHED     4280
  TCP    [::]:135               [::]:0                 LISTENING       652
  TCP    [::]:445               [::]:0                 LISTENING       4
  TCP    [::]:5985              [::]:0                 LISTENING       4
  TCP    [::]:47001             [::]:0                 LISTENING       4
```

- Three-way handshake
  - Client SYN
  - Server SYN/ACK
  - Client ACK
- Graceful teardown
  - FIN
  - ACK
  - FIN
  - ACK
- Session termination
  - RST

User Datagram Protocol

- Connectionless, non-guaranteed communication
- Fewer header fields required
- Used by protocols that can tolerate lost or out-of-order packets

Common TCP and UDP Ports

TCP/UDP/53 DNS	UDP/123 NTP	UDP/67 DHCP-Server	UDP/68 DHCP-Client	UDP/546 DHCPv6-Client	UDP/547 DHCPv6-Server	TCP/80 HTTP
TCP/25 SMTP	TCP/587 SMTPS	TCP/110 POP	TCP/995 POP3S	TCP/143 IMAP	TCP/993 IMAPS	TCP/443 HTTPS
UDP/5004 RTP	UDP/5005 RTCP	TCP/UDP/5060 SIP	TCP/UDP/5061 SIPS	TCP/1433 MS-SQL	TCP/1521 SQL*net	TCP/3306 MySQL
TCP/20 FTP-Data	TCP/21 FTP-Control	TCP/22 SSH/SFTP	TCP/23 Telnet	UDP/69 TFTP	TCP/3389 RDP	
UDP/514 Syslog	UDP/161 SNMP	UDP/162 SNMP-Trap	TCP/UDP/389 LDAP	TCP/636 LDAPS		TCP/445 SMB over TCP/IP

Review Activity: Transport Protocols

- Transport Layer Ports and Connections
- Transmission Control Protocol
- TCP Handshake and Teardown
- User Datagram Protocol
- Common TCP and UDP Ports

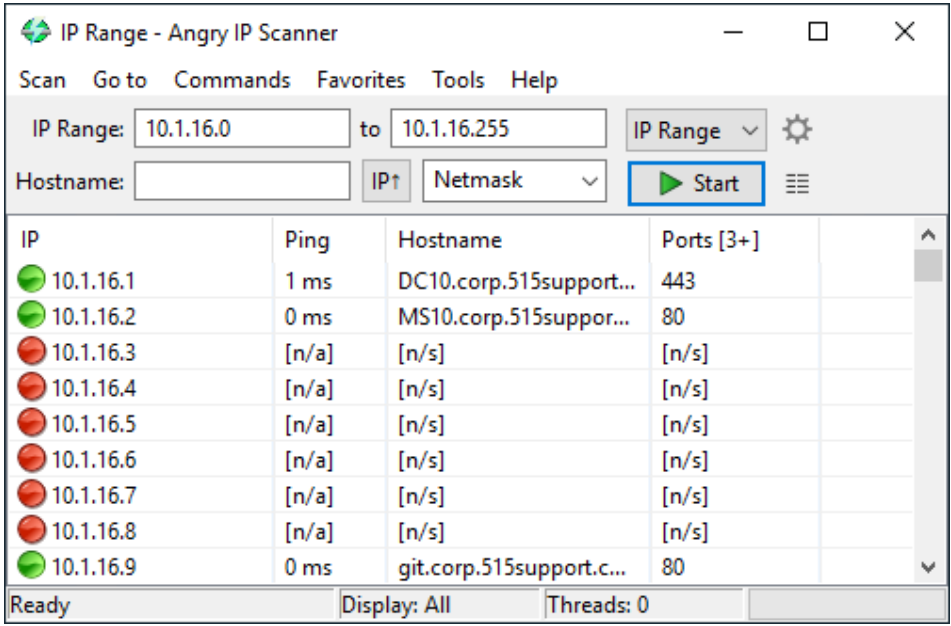
Lesson 9

Topic 9B

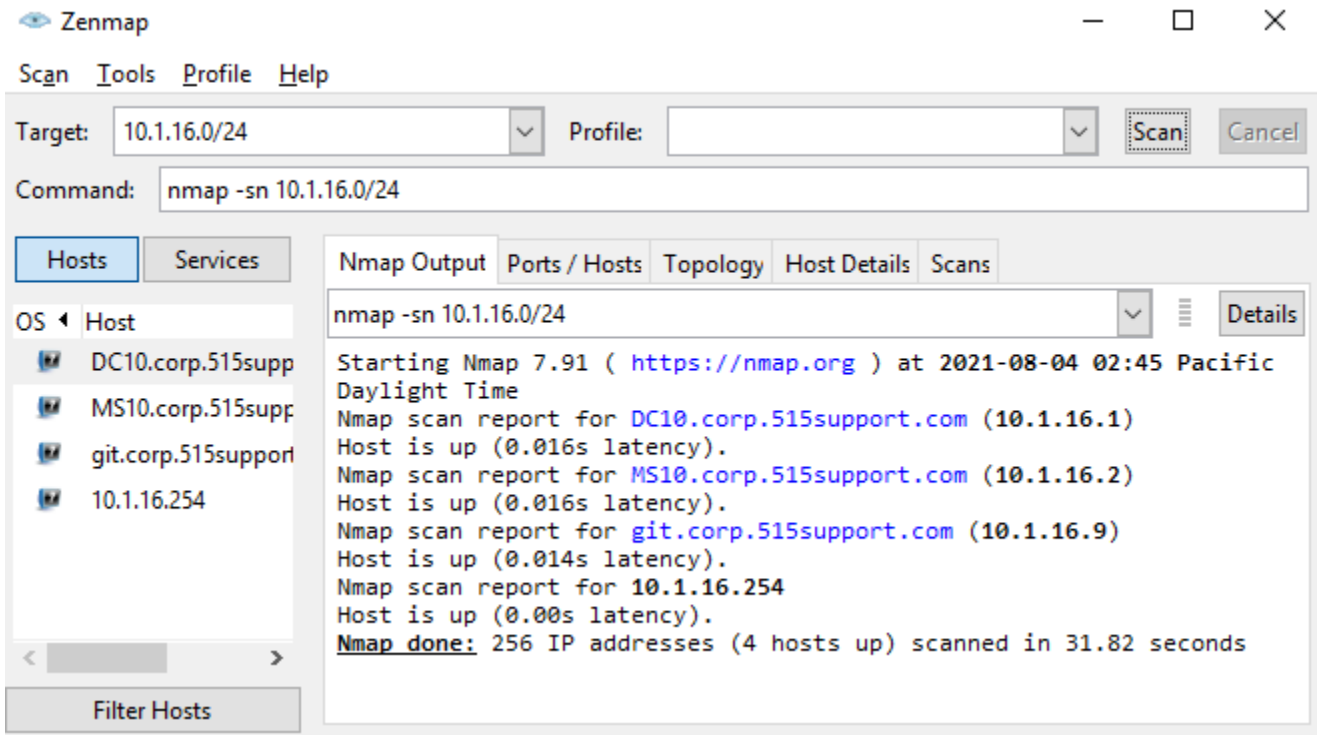
Use Appropriate Tools to Scan Network Ports

IP Scanners

- Perform host and topology discovery to maximize network visibility
  - Standalone tools
  - IP Address Management (IPAM)
- Determining “up” status
  - ping, arp, traceroute
  - Simple Network Management Protocol (SNMP)
  - Query DHCP/DNS



Nmap


Zenmap
Scan Tools Profile Help
Target: 10.1.16.0/24
Profile:
Scan
Cancel
Command: nmap -sn 10.1.16.0/24
Hosts
Services
OS Host
DC10.corp.515supp
MS10.corp.515supp
git.corp.515support
10.1.16.254
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -sn 10.1.16.0/24
Details
Starting Nmap 7.91 (https://nmap.org) at 2021-08-04 02:45 Pacific Daylight Time
Nmap scan report for DC10.corp.515support.com (10.1.16.1)
Host is up (0.016s latency).
Nmap scan report for MS10.corp.515support.com (10.1.16.2)
Host is up (0.016s latency).
Nmap scan report for git.corp.515support.com (10.1.16.9)
Host is up (0.014s latency).
Nmap scan report for 10.1.16.254
Host is up (0.00s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 31.82 seconds

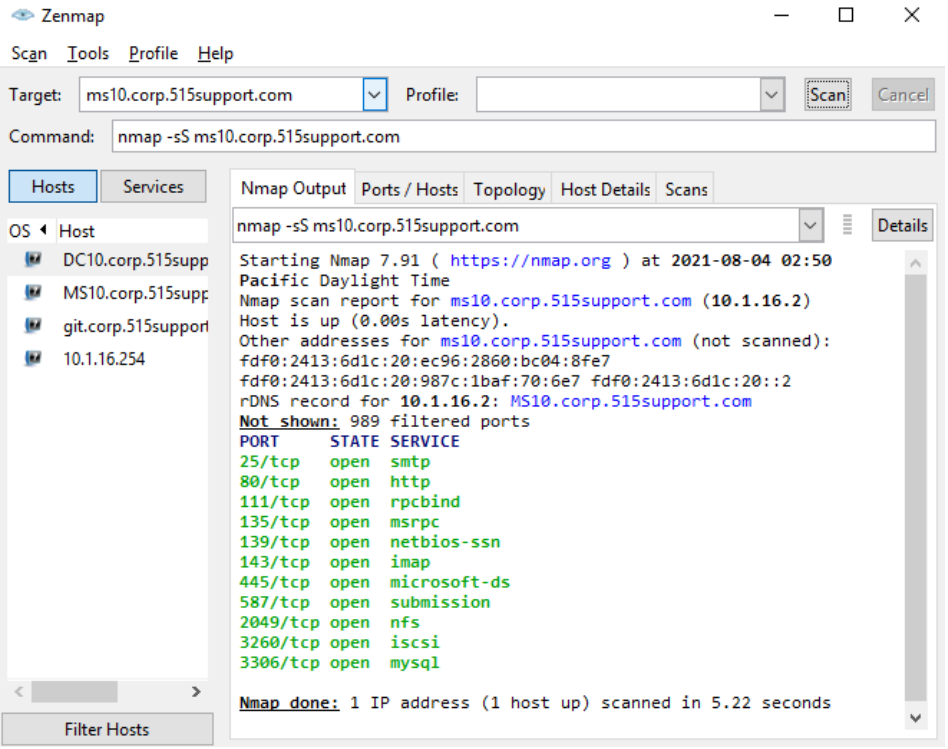
netstat

- Report local port status
  - TCP versus UDP
  - Local IP and port
  - Remote IP and port
  - State (Listening, Established, …)
- Options
  - Skip name resolution, show process, report statistics, …
  - Windows versus Linux syntax differences
  - iproute2 ss and nstat commands replace netstat

```
lamp@lamp:~$ netstat -tua
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:5000            0.0.0.0:*               LISTEN
tcp        0      0 localhost:mysql         0.0.0.0:*               LISTEN
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*               LISTEN
tcp        0      0 localhost:33060         0.0.0.0:*               LISTEN
tcp        0      1 172.16.0.201:52492      172.16.0.254:domain     SYN_SENT
tcp6       0      0 [::]:http               [::]:*                  LISTEN
tcp6       0      0 [::]:ssh                [::]:*                  LISTEN
udp        0      0 172.16.0.201:43367      172.16.0.254:domain     ESTABLISHED
udp        0      0 172.16.0.201:42410      172.16.0.254:domain     ESTABLISHED
udp        0      0 172.16.0.201:47084      172.16.0.254:domain     ESTABLISHED
udp        0      0 localhost:domain        0.0.0.0:*
udp        0      0 172.16.0.201:bootpc     0.0.0.0:*
```

```
lamp@lamp:~$ netstat -i
Kernel Interface table
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0      1500     4069      0      0 0          8134      0      0      0 BMRU
lo       65536     5322      0      0 0          5322      0      0      0 LRU
```

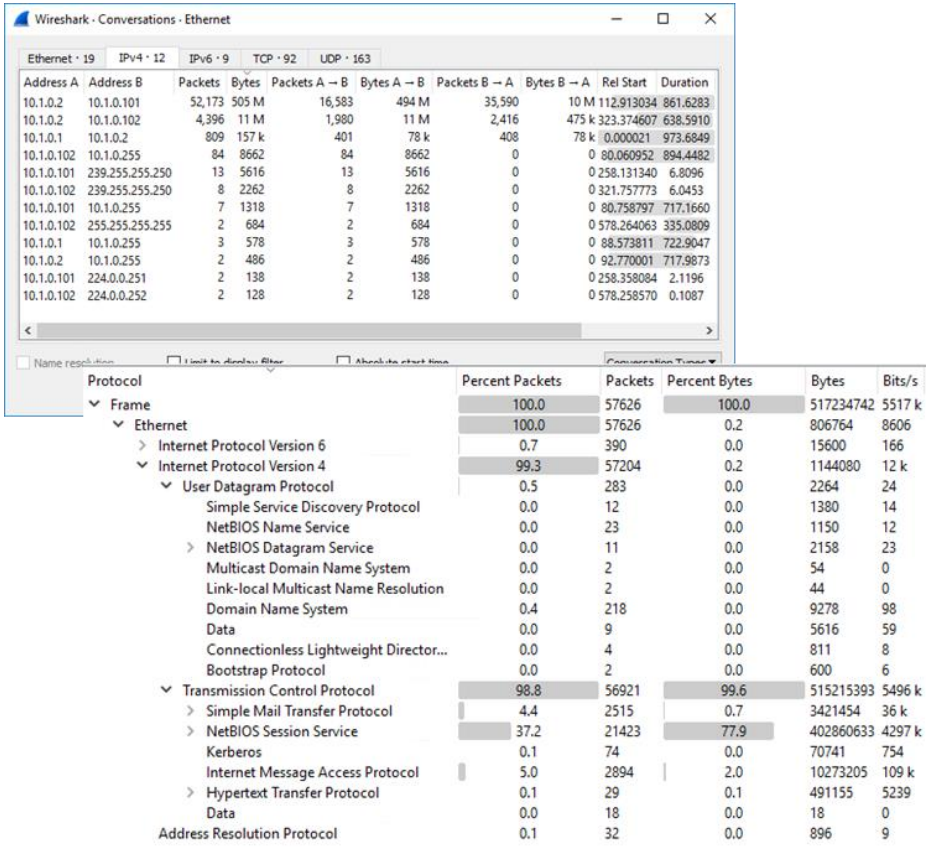
Remote Port Scanners



- Report port status from a remote host
- Scan types
  - Half-open, full connect, UDP, port range, …
- Host and service fingerprinting

Protocol Analyzers

- Decode frames captured by sniffer
  - Live capture or saved capture file (pcap)
  - Parse header fields to reveal packet metadata
  - Reconstruct TCP streams
- Analyze traffic statistics
  - Per-host utilization
  - Per-protocol utilization



Review Activity: Port Scanning

- IP Scanners
- Nmap
- netstat
- Remote Port Scanners
- Protocol Analyzers

Lab Activity

Assisted Lab: Use Network Scanners

- Lab types
  - Assisted labs guide you step-by-step through tasks
  - Applied labs set goals with limited guidance
- Complete lab
  - Submit all items for grading and check each progress box
  - Select “Grade Lab” from final page
- Save lab
  - Select the hamburger menu and select “Save”
  - Save up to two labs in progress for up to 7 days
- Cancel lab without grading
  - Select the hamburger menu and select “End”

CompTIA Network+ Exam N10-008

Lesson 9

Summary