

CompTIA Network+ Exam N10-008

Lesson 9



Explaining Transport Layer Protocols

Objectives

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

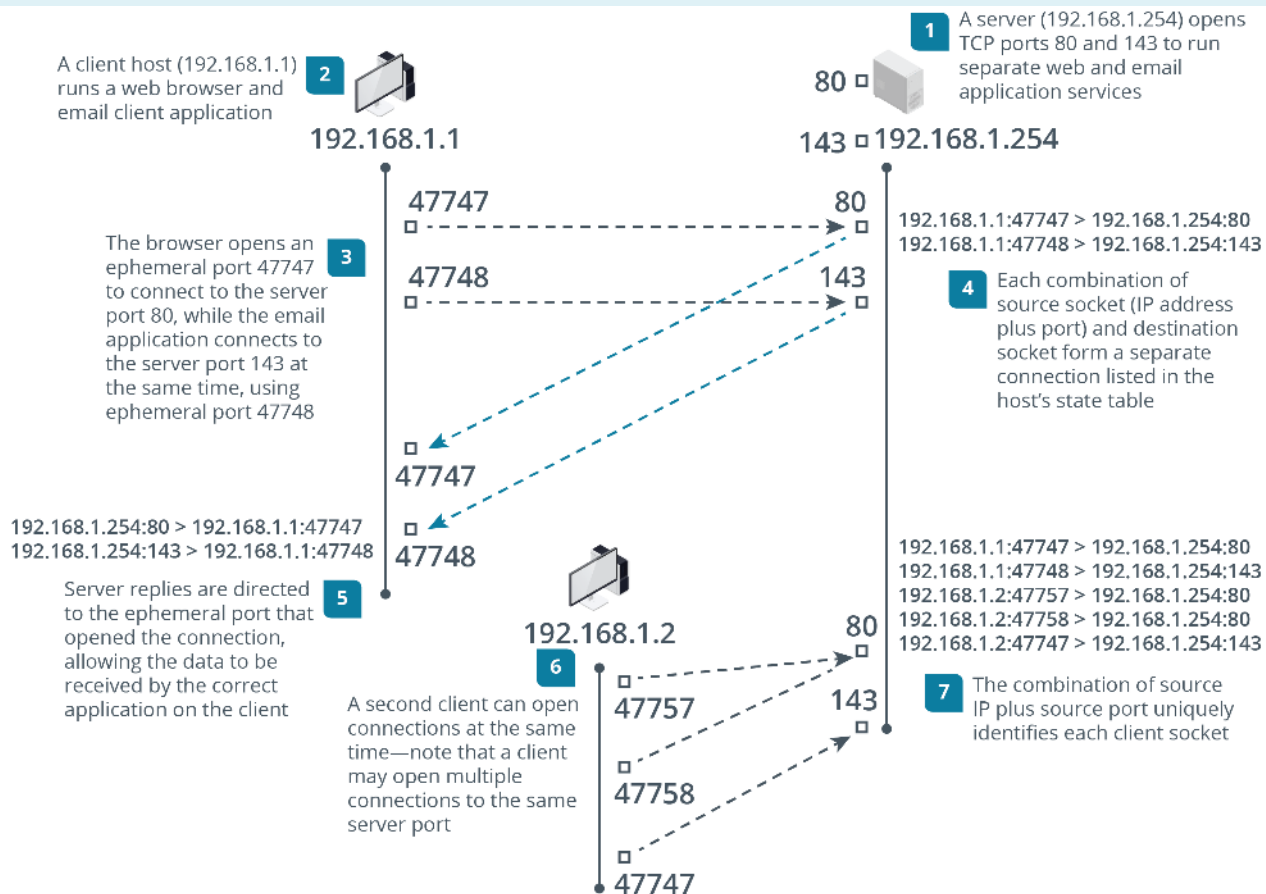
Lesson 9

Topic 9A

Compare and Contrast Transport Protocols

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 HTTPS
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

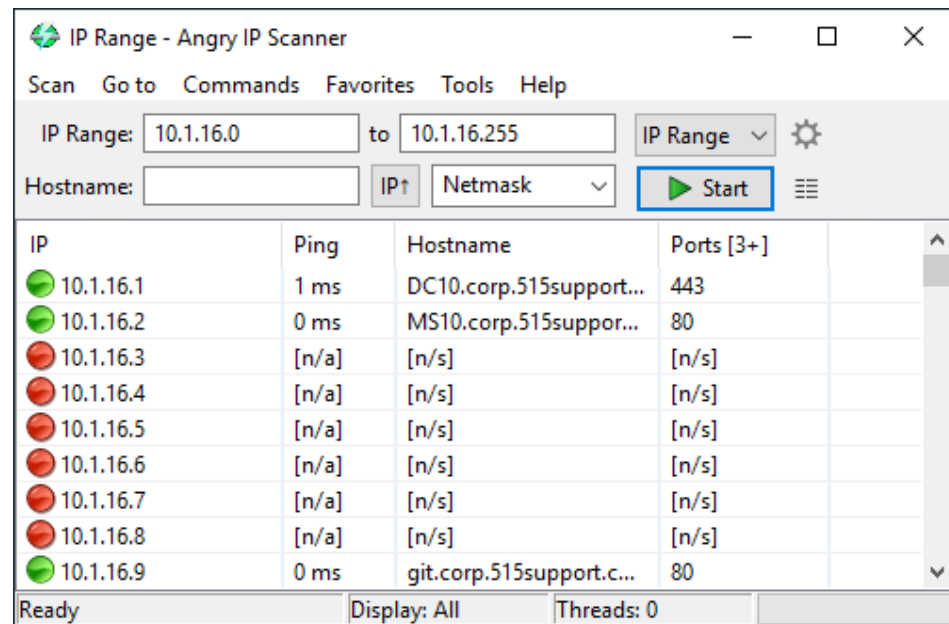
Lesson 9

Topic 9B

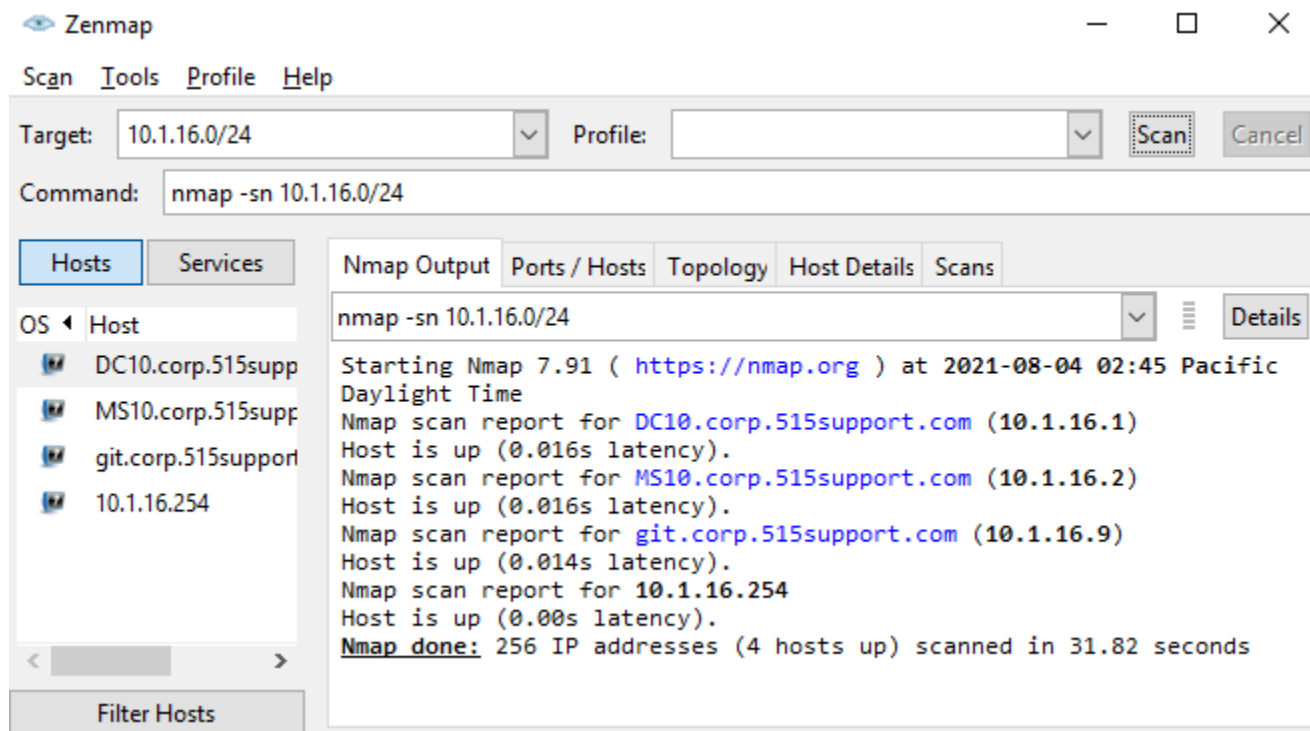
Use Appropriate Tools to Scan Network Ports

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



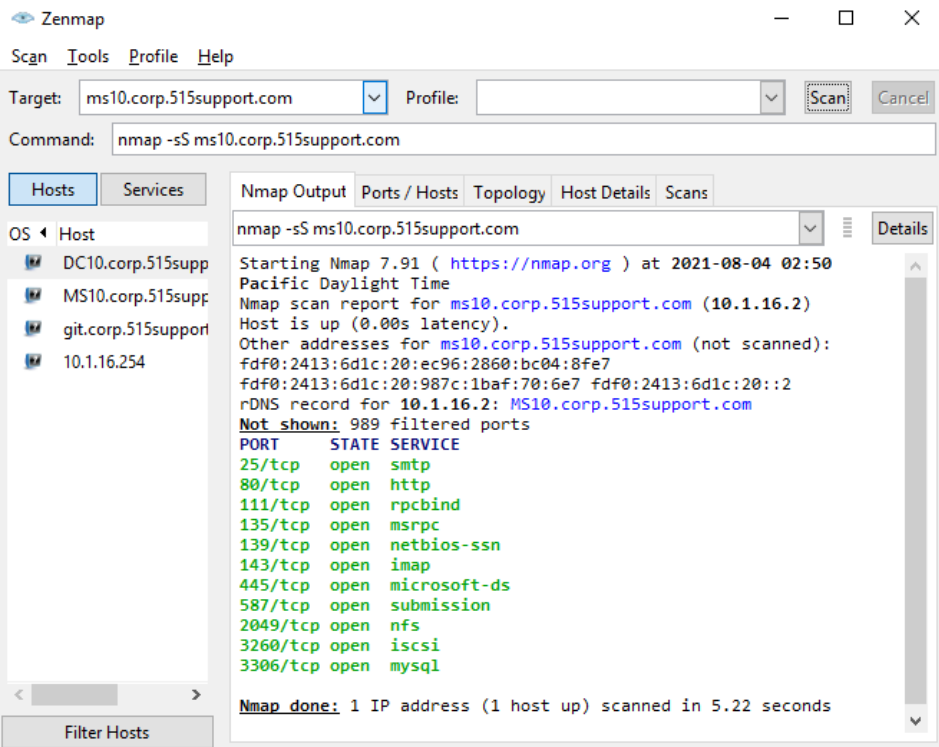
netstat

- 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:*               ESTABLISHED
udp      0      0 172.16.0.201:bootpc     0.0.0.0:*               ESTABLISHED
```

```
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
```

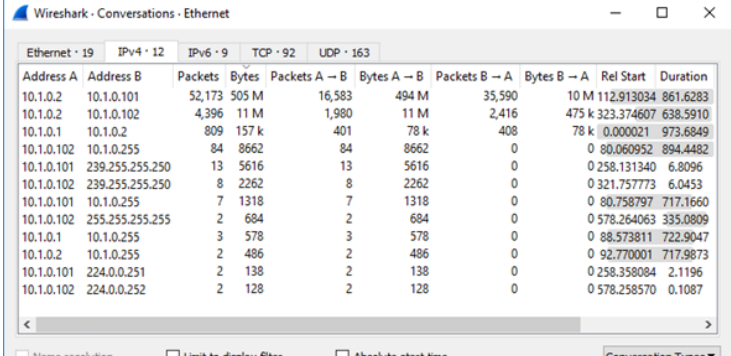
Remote Port Scanners



- 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



Wireshark - Conversations - Ethernet


Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration
10.1.0.2	10.1.0.101	52,173	505 M	16,583	494 M	35,590	10 M	112.913034	861.6283
10.1.0.2	10.1.0.102	4,396	11 M	1,980	11 M	2,416	475 k	323.374607	638.5910
10.1.0.1	10.1.0.2	809	157 k	401	78 k	408	78 k	0.000021	973.6849
10.1.0.102	10.1.0.255	84	8662	84	8662	0	0	80.060952	894.4482
10.1.0.101	239.255.255.250	13	5616	13	5616	0	0	258.131340	6.8096
10.1.0.102	239.255.255.250	8	2262	8	2262	0	0	321.757773	6.0453
10.1.0.101	10.1.0.255	7	1318	7	1318	0	0	80.758797	717.1660
10.1.0.102	255.255.255.255	2	684	2	684	0	0	578.264063	335.0809
10.1.0.1	10.1.0.255	3	578	3	578	0	0	88.573811	722.9047
10.1.0.2	10.1.0.255	2	486	2	486	0	0	92.770001	717.9873
10.1.0.101	224.0.0.251	2	138	2	138	0	0	258.358084	2.1196
10.1.0.102	224.0.0.252	2	128	2	128	0	0	578.258570	0.1087

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s
Frame	100.0	57626	100.0	517234742	5517 k
Ethernet	100.0	57626	0.2	806764	8606
Internet Protocol Version 6	0.7	390	0.0	15600	166
Internet Protocol Version 4	99.3	57204	0.2	1144080	12 k
User Datagram Protocol	0.5	283	0.0	2264	24
Simple Service Discovery Protocol	0.0	12	0.0	1380	14
NetBIOS Name Service	0.0	23	0.0	1150	12
NetBIOS Datagram Service	0.0	11	0.0	2158	23
Multicast Domain Name System	0.0	2	0.0	54	0
Link-local Multicast Name Resolution	0.0	2	0.0	44	0
Domain Name System	0.4	218	0.0	9278	98
Data	0.0	9	0.0	5616	59
Connectionless Lightweight Director...	0.0	4	0.0	811	8
Bootstrap Protocol	0.0	2	0.0	600	6
Transmission Control Protocol	98.8	56921	99.6	515215393	5496 k
Simple Mail Transfer Protocol	4.4	2515	0.7	3421454	36 k
NetBIOS Session Service	37.2	21423	77.9	402860633	4297 k
Kerberos	0.1	74	0.0	70741	754
Internet Message Access Protocol	5.0	2894	2.0	10273205	109 k
Hypertext Transfer Protocol	0.1	29	0.1	491155	5239
Data	0.0	18	0.0	18	0
Address Resolution Protocol	0.1	32	0.0	896	9

Review Activity: Port Scanning

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

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