Study Guide

Network Troubleshooting and Tools

Created By: Ravi Raj, Teaching Assistant

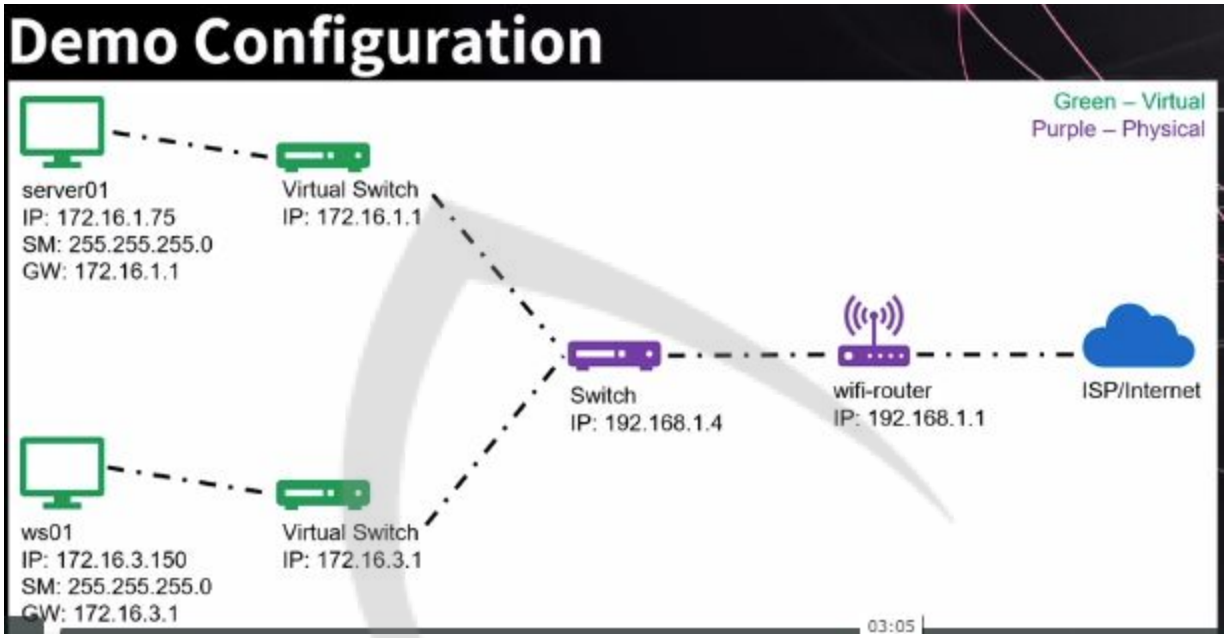
Module 1: Course Introduction

Lesson 1.1: Course and Instructor Introduction

Skills Learned From This Lesson: Troubleshooting skills, terminals and command prompt, Ports and protocols

- Target Audience:
  - Helpdesk Technicians
  - Systems Admins
  - Network Admins
  - Developers
- Having basic network troubleshooting knowledge skills will help anyone in IT.
- Prerequisites:
  - Basic working knowledge of terminal and command prompt.
  - Idea of networking basics and notations:
    192.168.1.25/24 subnet is 255.255.255.0
  - Knowing common ports and protocols like DNS on port 53, HTTP on port 80 etc.
  - DNS record types.
- Learning Objectives:
  - Verify network configuration
  - Troubleshoot network connectivity.
  - Verify domain name resolution.
  - Modify route tables.
  - Test ports and protocol.
  - Understand available advanced networking tools.
  - Understand installing and troubleshooting network devices.

- Network configuration used in the course:



Module 2: Network Troubleshooting Tools

Lesson 2.1: Testing Network Connectivity

- Learning Objectives:
  - ipconfig
  - ping
  - tracert
  - telnet
- ipconfig:
  - Internet Protocol configuration
  - View network configuration
  - Release and renew DHCP address. DHCP address is assigned by a network device configured for it.

```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::940e:6bb1:98be:c821%4
   IPv4 Address. . . . . . . . . . . : 172.16.1.75
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.1.1
```

- Ping:
  - Verifies connectivity to another computer
  - Uses TCP/IP protocol
  - Uses Internet Control Message Protocol(ICMP) echo requests

```
C:\>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:
Reply from 192.168.1.4: bytes=32 time=3ms TTL=63
Reply from 192.168.1.4: bytes=32 time=2ms TTL=63
Reply from 192.168.1.4: bytes=32 time=2ms TTL=63
Reply from 192.168.1.4: bytes=32 time=2ms TTL=63

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms
```

- Tracert:
  - Trace routee.
  - Determines route to the destinations via various hops performed.
  - Uses ICMP packets.
  - Calculate Time-To-Live(TTL)

```
1    <1 ms    <1 ms    <1 ms  172.16.1.1
2     *        *        *     Request timed out.
3     1 ms    <1 ms    <1 ms  wifi-router [192.168.1.1]
4     7 ms     8 ms     7 ms  10.9.128.1
5    10 ms    10 ms    10 ms  100.126.0.196
6    29 ms    19 ms    22 ms  100.126.0.116
```

- telnet:
  - Protocol to interact with remote computers.
  - Used to test TCP connections
  - Combine host name/IP address and port.
  - Once the session is established can be used to interact to the remote computer
    In e.g below we are doing telnet to an email server over port 25

```
C:\>telnet 172.16.1.75 25
Connecting To 172.16.1.75...
```

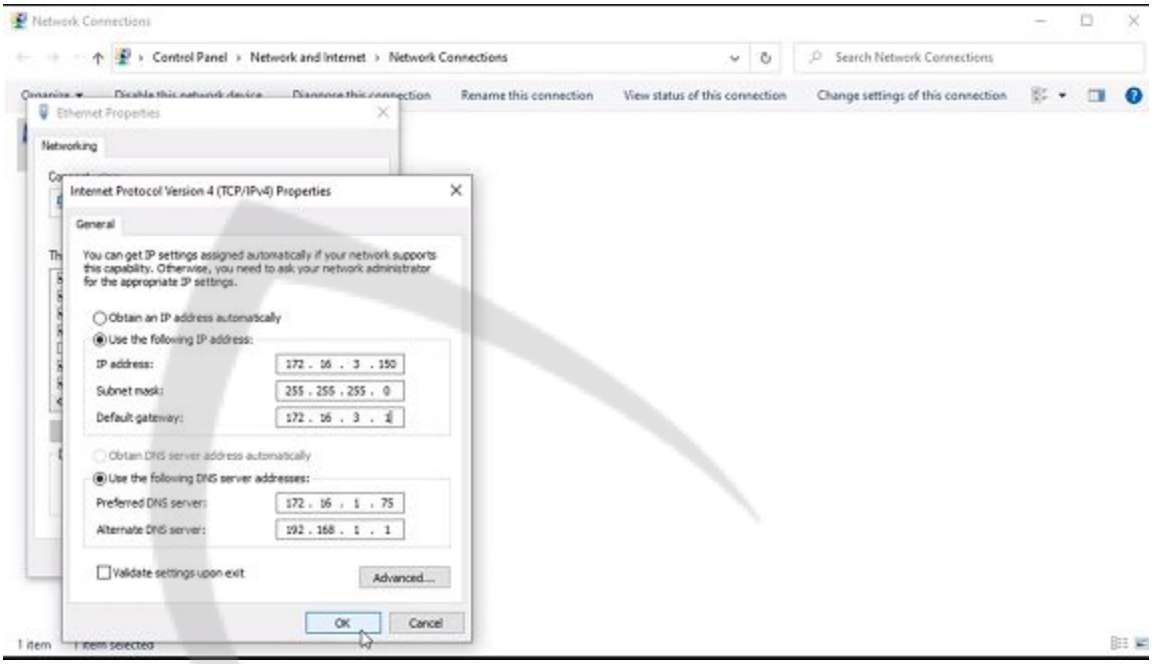
```
Welcome to Microsoft Telnet Client

Escape Character is 'CTRL+]'


Microsoft Telnet>
```

- Checking ipconfiguration in windows. Launch a command prompt and type ipconfig:

```
Command Prompt

C:\>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : upstarttech.com
   Link-local IPv6 Address . . . . . : fe80::1043:a304:d948:28c9%6
   Autoconfiguration IPv4 Address. . : 169.254.40.201
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :
```

- The IP address 169.254.*.* is assigned by default when an IP address can't be assigned by a DHCP server (Automatic private IP address).
- If the network issues are troubleshooted and DHCP server can assign an IP address we can try for using command ipconfig/renew

- Assign a static IP address:
  - Type ncpa.cpl
  - Opens the Network connection
  - Go to the Internet Protocol Version 4(TCP/IPv4) Properties and set the entries as below for static IP allocation



- Type ipconfig to get the newly static assigned IP address:

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : upstarttech.com
   Link-local IPv6 Address . . . . . : fe80::1043:a304:d948:28c9%6
   Autoconfiguration IPv4 Address. . : 169.254.40.201
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :

C:\>ncpa.cpl

C:\>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : upstarttech.com
   Link-local IPv6 Address . . . . . : fe80::1043:a304:d948:28c9%6
   IPv4 Address. . . . . . . . . . . : 172.16.3.150
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.3.1

C:\>
```

- Ipconfig /all gives more information like IPV6, MAC address information associated with the NIC.

- Use ping utility to ping the local host to check if the network stack is working properly:

```
C:\>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

- Pinging the static address just configured:

```
C:\>ping 172.16.3.1

Pinging 172.16.3.1 with 32 bytes of data:
Reply from 172.16.3.1: bytes=32 time<1ms TTL=128
Reply from 172.16.3.1: bytes=32 time<1ms TTL=128
Reply from 172.16.3.1: bytes=32 time<1ms TTL=128
Reply from 172.16.3.1: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

- We can also ping the websites and the hostnames:

```
C:\>ping google.com

Pinging google.com [216.58.194.110] with 32 bytes of data:
Reply from 216.58.194.110: bytes=32 time=14ms TTL=55
Reply from 216.58.194.110: bytes=32 time=15ms TTL=55
Reply from 216.58.194.110: bytes=32 time=13ms TTL=55
Reply from 216.58.194.110: bytes=32 time=21ms TTL=55

Ping statistics for 216.58.194.110:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 13ms, Maximum = 21ms, Average = 15ms
```

  - Not all websites will allow the ICMP packets and it may be blocked at firewall, it doesn't mean that site isn't up.

```
C:\>ping bing.com

Pinging bing.com [204.79.197.200] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 204.79.197.200:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

  - We can also use ping with –t as ping google.com –t to have continuous pings. We can stop using CTRL+c. It is useful when we want to check when the device is rebooted.
- We can check the complete trace to a destination using tracert command as below. Here we are checking the trace path to the wifi router:

```
C:\>tracert 192.168.1.1

Tracing route to wifi-router [192.168.1.1]
over a maximum of 30 hops:

  1    <1 ms     *       <1 ms  172.16.3.1
  2     *        *        *     Request timed out.
  3     4 ms     7 ms    <1 ms  wifi-router [192.168.1.1]

Trace complete.

C:\>_
```

- Tracing the path to google.com

```
Trace complete.

C:\>tracert google.com

Tracing route to google.com [216.58.194.142]
over a maximum of 30 hops:

  1    <1 ms     *       <1 ms  172.16.3.1
  2     *        *        *     Request timed out.
  3     1 ms    <1 ms    <1 ms  wifi-router [192.168.1.1]
  4     8 ms     8 ms     7 ms  10.9.128.1
  5    10 ms     9 ms     8 ms  100.126.0.190
  6     9 ms    10 ms    10 ms  100.126.0.114
  7    26 ms    19 ms    22 ms  dalsbprj01-ae1.0.rd.dl.cox.net [68.1.2.109]
  8    14 ms    14 ms    12 ms  dalsbprj01-ae1-216.rd.dl.cox.net [68.105.30.62]
  9     *        *        *     Request timed out.
 10    18 ms    13 ms    13 ms  108.170.231.70
 11    13 ms    13 ms    13 ms  108.170.230.117
 12    14 ms    13 ms    14 ms  dfw06s49-in-f142.1e100.net [216.58.194.142]

Trace complete.
```

We occasionally may receive a time out.

- We can use –d in with tracert to avoid name resolution to make the execution of tracert faster:

```
C:\>tracert -d google.com

Tracing route to google.com [216.58.194.110]
over a maximum of 30 hops:

  1    <1 ms     *       <1 ms  172.16.3.1
  2     *        *        *     Request timed out.
  3     1 ms     1 ms     1 ms  192.168.1.1
  4    12 ms     8 ms    24 ms  10.9.128.1
  5     9 ms     9 ms     8 ms  100.126.0.190
  6     9 ms     8 ms     9 ms  100.126.0.114
  7    16 ms    14 ms    17 ms  68.1.2.109
  8    12 ms    18 ms    13 ms  209.85.172.68
  9    14 ms    12 ms    15 ms  108.170.252.129
 10    17 ms    15 ms    15 ms  108.170.230.113
 11    19 ms    29 ms    24 ms  216.58.194.110

Trace complete.
```

- Using telenet to connect to a server via a particular port, we are doing telnet to 172.16.1.75 over port 25

```
220 server01 Microsoft ESMTP MAIL Service, Version: 10.0.14393.2608 ready at  Wed, 4 Dec 2019 20:28:
17 -0600
```

We can send an email using SMTP server once connected to.
We can breakout of the session using CTRL+] and doing quit.
Also we can try for telent to port 80 over the same server as it hosting a web server, It would simply show a cursor on the next screen.

- If there is no port open on the server we it won't open a telnet connection and fail.

```
C:\>telnet 172.16.1.75 81
Connecting To 172.16.1.75...Could not open connection to the host, on port 81: Connect failed
```

Lesson 2.2: Testing Name Resolution

Skills Learned From This Lesson: nslookup, nbstat, arp

- Learning Objectives:
  - ipconfig
  - nslookup
  - nbstat
  - arp
- Most problems boils down to name resolution, so would be a good starting point to start with.
- Purge local DNS cache: Use this command to purge the DNS cache and get a new IP address using the ipconfig /flushdns command.
  Re-register DNS names: Use the command ipconfig /registerdns to re-register to the DNS server.

```
C:\>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\>ipconfig /registerdns

Windows IP Configuration

Registration of the DNS resource records for all adapters of this computer has been initiated.
```

- nslookup:
  - Name Server lookup.
  - Diagnose Domain Name System (DNS) infrastructure.
  - Look up host name records.
  - We can also compare against a different name server for different records

```
Non-authoritative answer:
cybrary.it      MX preference = 1, mail exchanger = aspmx.l.google.com
cybrary.it      MX preference = 10, mail exchanger = alt3.aspmx.l.google.com
cybrary.it      MX preference = 10, mail exchanger = alt4.aspmx.l.google.com
cybrary.it      MX preference = 5, mail exchanger = alt1.aspmx.l.google.com
cybrary.it      MX preference = 5, mail exchanger = alt2.aspmx.l.google.com

aspmx.l.google.com      internet address = 108.177.103.26
alt3.aspmx.l.google.com AAAA IPv6 address = 2607:f8b0:400d:c0c::1a
alt4.aspmx.l.google.com internet address = 173.194.215.26
alt1.aspmx.l.google.com AAAA IPv6 address = 2607:f8b0:4023::1a
alt2.aspmx.l.google.com internet address = 64.233.177.27
```

- nbtstat:
  - Netbios over TCP/IP statistics
  - Verifies NetBIOS name resolution or it can be used to resolved the cache of resolved system names on the host.
  - Previously this service was provided by Windows Internet Naming Service (WINS)

```
C:\>nbtstat -c

Ethernet:
Node IpAddress: [172.16.3.150] Scope Id: []

        NetBIOS Remote Cache Name Table

    Name            Type       Host Address    Life [sec]
    ------------------------------------------------------------
    SERVER01       <20>  UNIQUE         172.16.1.75         577
    SERVER01       <00>  UNIQUE         172.16.1.75         205
```

- arp:
  - Address Resolution Protocol: Maps IP address to the MAC.
  - IP address and physical addresses.

- Display and modifies entries in cache.

```
C:\>arp -a

Interface: 172.16.1.75 --- 0x4
  Internet Address      Physical Address      Type
  172.16.1.1            00-15-5d-01-66-1d     dynamic
  172.16.1.255          ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  224.0.1.24            01-00-5e-00-01-18     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

- Running the ipconfig /flushdns and ipconfig /registerdns commands requires admin privileges.

```
C:\>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\>ipconfig /registerdns

Windows IP Configuration

Registration of the DNS resource records for all adapters of this computer has been initiated. Any
 errors will be reported in the Event Viewer in 15 minutes.
```

- Using netstat command:
  - nslookup cybrary.it against the locally configured DNS server:

```
C:\>nslookup cybrary.it
Server:  server01.upstarttech.com
Address:  172.16.1.75

Non-authoritative answer:
Name:    cybrary.it
Addresses:  3.14.42.170
          3.19.210.135
          3.14.197.240
```

- nslookup against the wifi router:

```
C:\>nslookup cybrary.it 192.168.1.1
Server:  wifi-router
Address:  192.168.1.1

Non-authoritative answer:
Name:    cybrary.it
Addresses:  3.14.197.240
```

- We can check against the google DNS too:

```
C:\>nslookup cybrary.it 8.8.8.8
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    cybrary.it
Addresses:  3.19.210.135
          3.14.42.170
          3.14.197.240
```

- Checking against the cloudflare DNS:

```
C:\>nslookup cybrary.it 1.1.1.1
Server:  one.one.one.one
Address:  1.1.1.1

Non-authoritative answer:
Name:    cybrary.it
Addresses:  3.14.197.240
          3.19.210.135
          3.14.42.170
```

- Till now we have been only fetching PTR records. We can fetch MX records too using nslookup:

```
C:\>nslookup -type=mx cybrary.it
Server:  server01.upstarttech.com
Address:  172.16.1.75

DNS request timed out.
    timeout was 2 seconds.
Non-authoritative answer:
cybrary.it      MX preference = 5, mail exchanger = alt1.aspmx.l.google.com
cybrary.it      MX preference = 5, mail exchanger = alt2.aspmx.l.google.com
cybrary.it      MX preference = 1, mail exchanger = aspmx.l.google.com
cybrary.it      MX preference = 10, mail exchanger = alt3.aspmx.l.google.com
cybrary.it      MX preference = 10, mail exchanger = alt4.aspmx.l.google.com

alt1.aspmx.l.google.com internet address = 172.253.112.26
alt1.aspmx.l.google.com AAAA IPv6 address = 2607:f8b0:4023::1b
alt4.aspmx.l.google.com internet address = 173.194.215.26
alt4.aspmx.l.google.com AAAA IPv6 address = 2607:f8b0:400c:c0c::1b
```

- We can also fetch service records:

```
C:\>nslookup -type=srv _sipfederationtls._tcp.upstarttech.com 192.168.1.1
Server:  wifi-router
Address:  192.168.1.1

Non-authoritative answer:
_sipfederationtls._tcp.upstarttech.com  SRV service location:
          priority       = 100
          weight         = 1
          port           = 5061
          svr hostname   = sipfed.online.lync.com

sipfed.online.lync.com  internet address = 52.112.66.139
```

It may not be possible for a DNS record to fetch all type of records.

- We can also use nslookup to lookup against multiple DNS servers at once by interactively via nslookup. For this we can simply type command nslookup and check the required DNS, service or type of records that we checked earlier.

- nbtstat:
  - We can use following command to identify the IP address of the host:

```
C:\>nbtstat -a server01

Ethernet:
Node IpAddress: [172.16.3.150] Scope Id: []

    Host not found.
```

  - Use the following command to fetch the hostname against an IP:

```
C:\>nbtstat -A 172.16.1.75

Ethernet:
Node IpAddress: [172.16.3.150] Scope Id: []

    Host not found.
```

- Checking the cache that our system is able to matchup:

```
C:\>nbtstat -c

Ethernet:
Node IpAddress: [172.16.3.150] Scope Id: []

                NetBIOS Remote Cache Name Table

        Name             Type       Host Address    Life [sec]
    ---------------------------------------------------------
    SERVER01       <00>  UNIQUE         172.16.1.75        564
```

- Arp command:
  - Checking the arp entries:

```
C:\>arp -a

Interface: 172.16.3.150 --- 0x6
  Internet Address      Physical Address      Type
  172.16.3.1            00-15-5d-01-66-23     dynamic
  172.16.3.255          ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

- Adding an ARP entry manually requires administrator command prompt access:

```
C:\>arp -s 172.16.3.200 00-aa-00-62-c6-09

C:\>arp -a

Interface: 172.16.3.150 --- 0x6
  Internet Address      Physical Address      Type
  172.16.3.1            00-15-5d-01-66-23     dynamic
  172.16.3.200          00-aa-00-62-c6-09     static
  172.16.3.255          ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

- We can remove an ARP entry too from an ARP table:

```
C:\>arp -d 172.16.3.200

C:\>arp -a

Interface: 172.16.3.150 --- 0x6
  Internet Address      Physical Address      Type
  172.16.3.1            00-15-5d-01-66-23     dynamic
  172.16.3.255          ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

Lesson 2.3: Advanced Networking Tools

Skills Learned From This Lesson: netstat, route, netsh

- netstat:
  - Network Statistics
  - Display active connections.
  - Verify ports computer is listening on.

```
Proto  Local Address          Foreign Address        State
TCP    172.16.1.75:49671      52.230.222.68:https    ESTABLISHED
TCP    172.16.1.75:49690      52.230.222.68:https    ESTABLISHED
TCP    172.16.1.75:49930      64.4.54.254:https      TIME_WAIT
TCP    172.16.1.75:49931      13.83.149.5:https      TIME_WAIT
TCP    172.16.1.75:49932      a23-63-253-32:http     TIME_WAIT
```

- route:
  - displays local IP routing table.
  - Add static routes to control network traffic.

```
C:\>route print
===========================================================================
Interface List
  6...00 15 5d 01 66 2f ......Microsoft Hyper-V Network Adapter
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      172.16.3.1     172.16.3.150    271
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
```

- netsh:
  - Network shell.
  - Display and configure network communication settings.
  - Reset network adapter.

```
C:\>netsh winsock reset

Sucessfully reset the Winsock Catalog.
You must restart the computer in order to complete the reset.
```

- Netstat:
  - It checks the various active connections to the system. State established means the connection is established. State TIME_WAIT means there is no connection yet.

```
C:\>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    172.16.1.75:80         ws01:49938             ESTABLISHED
  TCP    172.16.1.75:49674      52.230.222.68:https    ESTABLISHED
  TCP    172.16.1.75:50051      52.230.222.68:https    ESTABLISHED
  TCP    172.16.1.75:50092      72.21.81.240:http      TIME_WAIT
  TCP    172.16.1.75:50097      64.4.54.254:https      TIME_WAIT
  TCP    172.16.1.75:50100      72.21.81.240:http      TIME_WAIT
```

- netstat –f resolves the addresses into a FQDN.

```
C:\>netstat -f

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    172.16.1.75:80         ws01:49938             ESTABLISHED
  TCP    172.16.1.75:49674      52.230.222.68:https    ESTABLISHED
  TCP    172.16.1.75:50051      52.230.222.68:https    ESTABLISHED

C:\>nslookup 52.230.222.38 8.8.8.8
Server:  dns.google
Address:  8.8.8.8

*** dns.google can't find 52.230.222.38: Non-existent domain
```

- netstat –a lists all the IP address that the system is listening to and their status.
- netstat –an adds the port number to the IP address.
- netstat –ano includes the PID(process ID) of the process.
- To filter through the noise we can just search for the port that we are interested in:

```
C:\>netstat -ano | findstr ":25"
  TCP    0.0.0.0:25             0.0.0.0:0              LISTENING       1740
  UDP    172.16.1.75:2535       *:*                                    1752
```

- route:
  - route print

Network Destination: It is the n/k address of the destination n/k . 0.0.0.0 means all the traffic or the internet traffic.
Metric: it determines the precedence. Lower value means higher precedence.

```
C:\>route print
===========================================================================
Interface List
  6...00 15 5d 01 66 2f ......Microsoft Hyper-V Network Adapter
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      172.16.3.1    172.16.3.150    271
        127.0.0.0        255.0.0.0         On-link        127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link        127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link        127.0.0.1    331
       172.16.3.0    255.255.255.0         On-link      172.16.3.150    271
     172.16.3.150  255.255.255.255         On-link      172.16.3.150    271
     172.16.3.255  255.255.255.255         On-link      172.16.3.150    271
        224.0.0.0        240.0.0.0         On-link        127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link      172.16.3.150    271
  255.255.255.255  255.255.255.255         On-link        127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link      172.16.3.150    271
===========================================================================
```

- We can add static routes to direct traffic through a particular route(needs administrator command prompt):

```
C:\>route ADD 172.16.5.0 MASK 255.255.255.0 172.16.1.1 METRIC 115 IF 6
 OK!
```

```
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      172.16.3.1     172.16.3.150    271
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      172.16.3.0   255.255.255.0         On-link      172.16.3.150    271
    172.16.3.150  255.255.255.255         On-link      172.16.3.150    271
    172.16.3.255  255.255.255.255         On-link      172.16.3.150    271
      172.16.5.0   255.255.255.0      172.16.1.1      172.16.3.150    130
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link      172.16.3.150    271
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link      172.16.3.150    271
===========================================================================
Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric
          0.0.0.0          0.0.0.0      172.16.3.1  Default
===========================================================================

IPv6 Route Table
===========================================================================
Active Routes:
```

- We can use route Delete <IP> to delete a route print.
- We can add a route to keep it persistent through reboots using the –p switch.

```
C:\>route -p ADD 172.16.5.0 MASK 255.255.255.0 172.16.1.1 METRIC 115 IF 6
```

```
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      172.16.3.1     172.16.3.150    271
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      172.16.3.0   255.255.255.0         On-link      172.16.3.150    271
    172.16.3.150  255.255.255.255         On-link      172.16.3.150    271
    172.16.3.255  255.255.255.255         On-link      172.16.3.150    271
      172.16.5.0   255.255.255.0      172.16.1.1      172.16.3.150    130
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link      172.16.3.150    271
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link      172.16.3.150    271
===========================================================================
Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric
          0.0.0.0          0.0.0.0      172.16.3.1  Default
      172.16.5.0   255.255.255.0      172.16.1.1     115
===========================================================================

IPv6 Route Table
===========================================================================
Active Routes:
```

We may need a persistent route in case we have a server with multiple network interfaces and need to direct traffic through a particular interface only.

- netsh
  - use reset command to reset the network stack:

```
C:\>netsh winsock reset

Sucessfully reset the Winsock Catalog.
You must restart the computer in order to complete the reset.
```

Lesson 2.4: Capturing Network Traffic

Skills Learned From This Lesson: wireshark, fiddler, netsh

- netsh:
  - Network shell
  - Capture network traffic
  - Persistent through system restarts

```
C:\>netsh trace start persistent=yes capture=yes tracefile=C:\netshtrace\demo.etl

Trace configuration:
-------------------------------------------------------------------
Status:             Running
Trace File:         C:\netshtrace\demo.etl
Append:             Off
Circular:           On
Max Size:           250 MB
Report:             Off
```

- Wireshark:
  - Open-source
  - Network-packet analyzer

ip.addr == 172.16.1.75

No.	Time	Source	Destination	Protocol	Length	Info
5	3.368627	172.16.3.150	172.16.1.75	NBNS	92	Name query NB SERVER01<00>
6	3.370111	172.16.1.75	172.16.3.150	NBNS	104	Name query response NB 172.16.1.75
23	3.671669	172.16.3.150	172.16.1.75	TCP	66	50064 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
24	3.672991	172.16.1.75	172.16.3.150	TCP	66	80 → 50064 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
25	3.673051	172.16.3.150	172.16.1.75	TCP	54	50064 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
26	3.673216	172.16.3.150	172.16.1.75	HTTP	423	GET / HTTP/1.1
27	3.729708	172.16.1.75	172.16.3.150	TCP	54	80 → 50064 [ACK] Seq=1 Ack=370 Win=262656 Len=0
28	3.796495	172.16.1.75	172.16.3.150	HTTP	982	HTTP/1.1 200 OK (text/html)
29	3.796581	172.16.3.150	172.16.1.75	TCP	54	50064 → 80 [ACK] Seq=370 Ack=929 Win=261120 Len=0
30	3.814245	172.16.3.150	172.16.1.75	HTTP	416	GET /iisstart.png HTTP/1.1

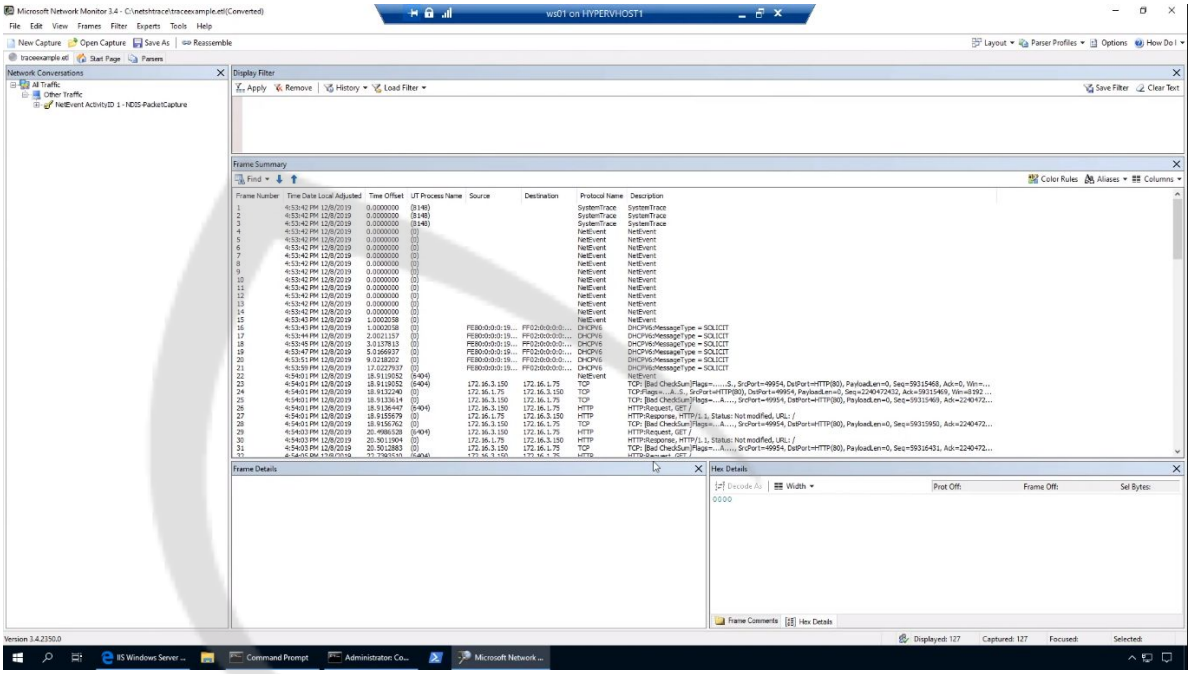
- Fiddler;
  - Capture HTTP traffic.
  - Decrypt to view secure sessions.
  - Acts as a proxy.

#	Result	Protocol	Host	URL	Body	Caching	Content-Type	Process
1	200	HTTPS	www.fiddler2.com	/UpdateCheck.aspx?isBet...	699	private	text/plain; ...	
2	200	HTTP	fiddler2.com	/content/GetArticles?clien...	747	no-cac...	application/...	fiddler:...
3	200	HTTP	fiddler2.com	/content/GetBanner?client...	130,750	no-cac...	application/...	fiddler:...
4	200	HTTP	Tunnel to	bing.com:443	0			microso...
5	304	HTTP	server01	/	0			microso...
6	304	HTTP	server01	/iisstart.png	0			microso...
7	301	HTTPS	bing.com	/edgepinning/allowlist	162	private	text/html; c...	microso...
8	304	HTTP	server01	/	0			microso...
9	304	HTTP	server01	/iisstart.png	0			microso...

- netsh:
  - mkdir netshtrace: creates a folder for saving the trace.
  - netsh trace start persistent=yes capture=yes tracefile=C:\netshtrace\traceexample.etl starts tracing.

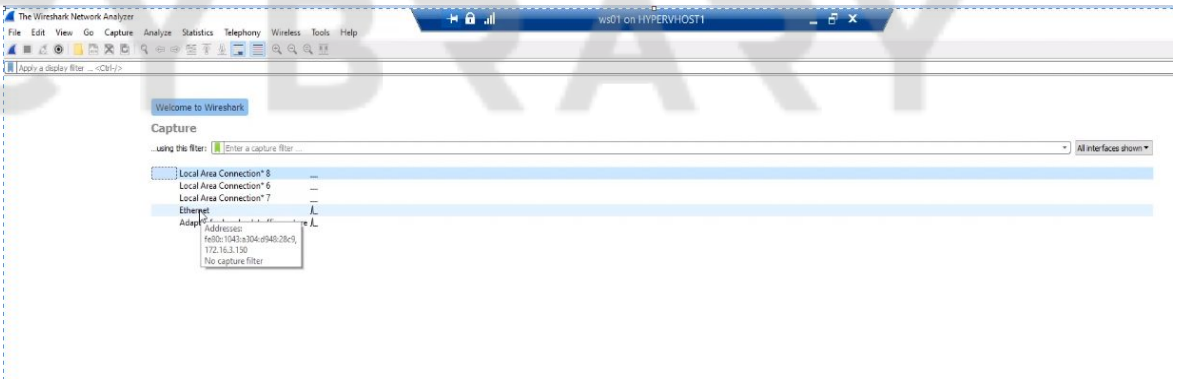
```
C:\>netsh trace start persistent=yes capture=yes tracefile=C:\netshtrace\traceexample.etl

Trace configuration:
-------------------------------------------------------------------
Status:             Running
Trace File:         C:\netshtrace\traceexample.etl
Append:             Off
Circular:           On
Max Size:           250 MB
Report:             Off
```

Use Network monitor tool to open the etl file generated:



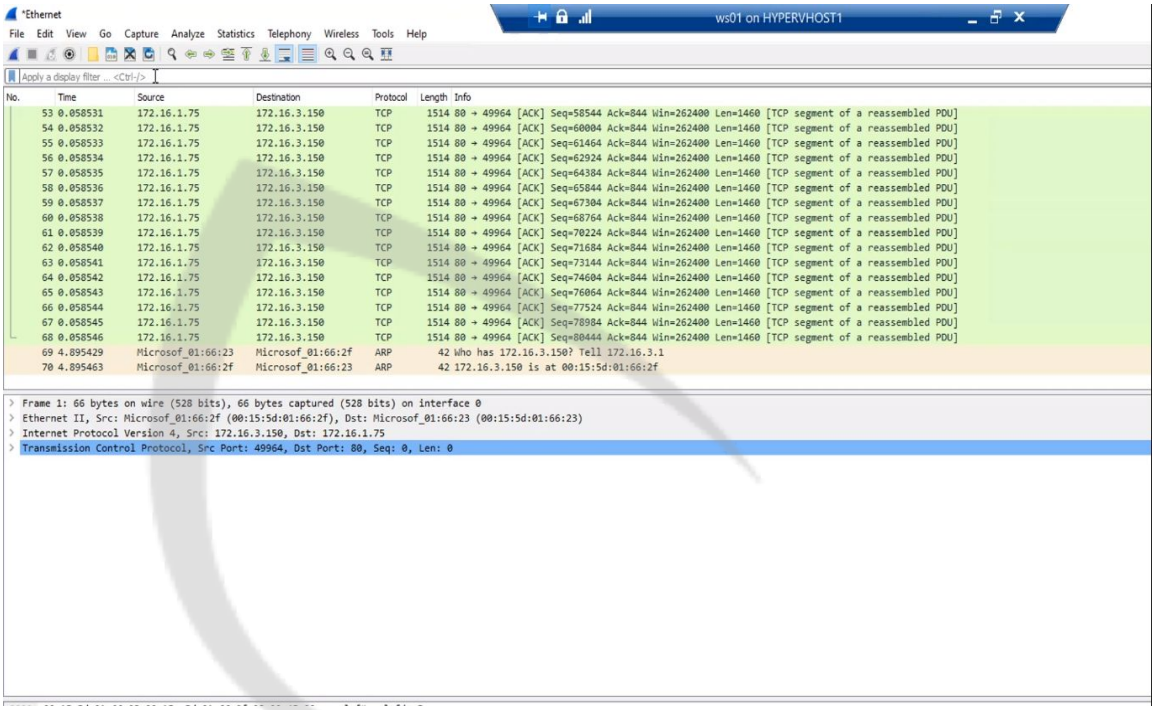
Once it finishes reading the file we can see source and Destination IPs in the logs.

- Wireshark:
  - Open wireshark and select the interface you want to capture the traffic on:

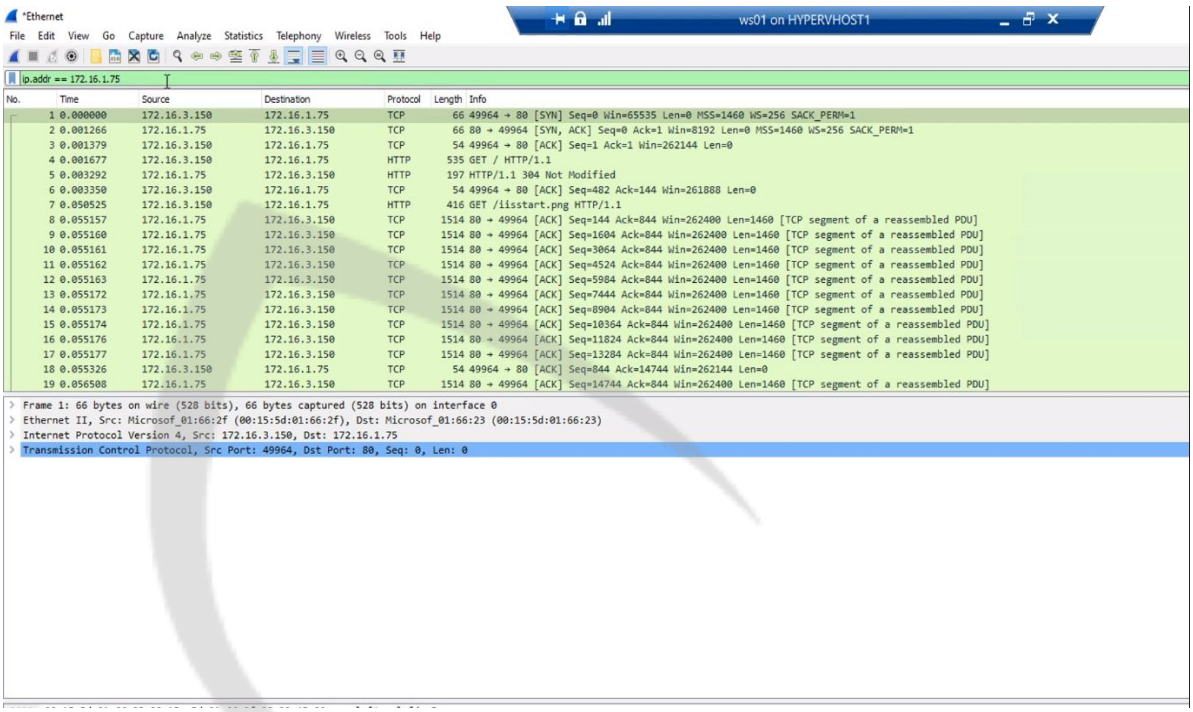


  - Start capturing the traffic and stop once done.

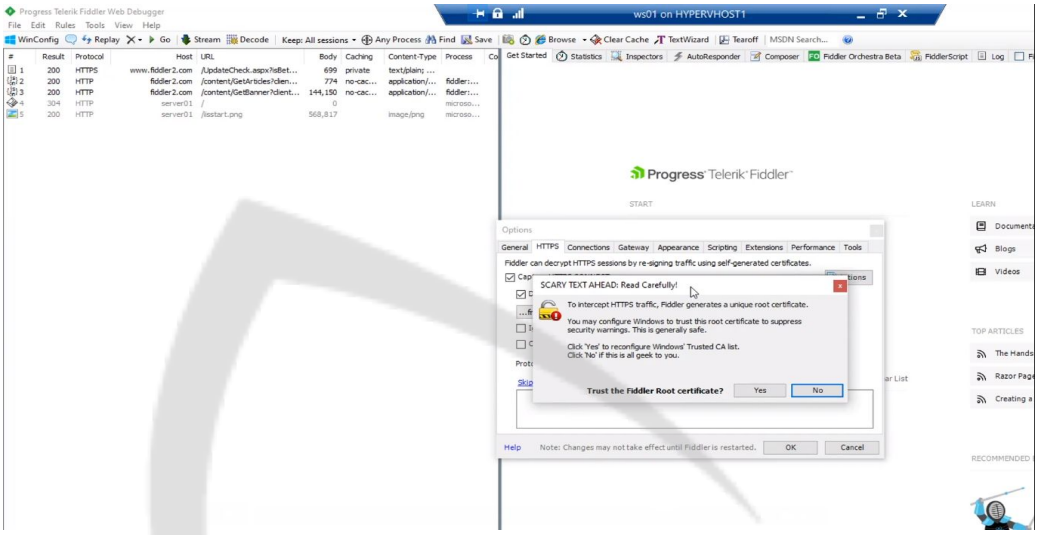
Following traffic is captured



- Search the logs for ip address 172.16.1.75 only:



- Fiddler:
  - Fiddler is useful for capturing the HTTPS traffic and decrypt it by acting as a proxy
  - We have to install a root certificate to enable the traffic decryption:



- We can also choose what type of traffic we want to capture.

Module 3: Course Introduction

Lesson 3.1: Troubleshoot Network Devices

Skills Learned From This Lesson: Physical Connections, Network Devices, Network Architecture

- Physical Connections:
  - Verify the network cable. Ensure it isn't broken.
  - Verify the network card.
  - Verify network activity lights. Blinking light ensures it is working
- Network Device Availability:
  - Verify power and network connectivity.
  - Access admin interface(GUI, SSH). Check if the device is reachable, use tracert.
  - Direct connection
- Network Device Configuration:
  - Verify the port connectivity.

Port	Status	Speed/Duplex		Flow Control	
		Config	Actual	Config	Actual
Port 1	Disabled	Auto	Link Down	Off	Off
Port 2	Enabled	Auto	100MF	Off	Off
Port 3	Enabled	10MH	Link Down	Off	Off

- Verify port enablement:

Port	Status	Speed/Duplex		Flow Control	
		Config	Actual	Config	Actual
Port 1	Disabled	Auto	Link Down	Off	Off
Port 2	Enabled	Auto	100MF	Off	Off
Port 3	Enabled	10MH	Link Down	Off	Off

- Verify port speed configuration:

Port	Status	Speed/Duplex		Flow Control	
		Config	Actual	Config	Actual
Port 1	Disabled	Auto	Link Down	Off	Off
Port 2	Enabled	Auto	100MF	Off	Off
Port 3	Enabled	10MH	Link Down	Off	Off

- Verify VLAN: Ensure device is plugged into the correct virtual LAN.

- Network Architecture:
  - Documentation and diagrams: Proper documentation showing various devices in the environment.
  - Understand traffic flows.
  - Security devices(firewall, proxies): ensure that firewall and proxy have proper configuration to allow the traffic.