Network Troubleshooting Tools

"Our new application is slow for me and Jasmine can't access it.

It HAS to be the network.

I've checked everything on our end"

Table of Contents

Table of Contents

1 ping

`ping` - Overview

- most **basic TCP/IP utility** for network troubleshooting
- uses the **ICMP protocol** to send a "ping" to a device
- target device must have **ICMP enabled**
- can **confirm if a host is running**
- **cannot** conclusively determine if a **host is down**

`ping` - Basic Syntax

Linux / MacOS / Windows	`ping hostname or IP address`

`ping` - Understanding the Output

```
usr > ping ec2-100-26-99-73.compute-1.amazonaws.com
PING ec2-100-26-99-73.compute-1.amazonaws.com (172.31.81.253) 56(84) bytes of data.
64 bytes from ip-172-31-81-253.ec2.internal (172.31.81.253): icmp_seq=1 ttl=255 time=0.579 ms
64 bytes from ip-172-31-81-253.ec2.internal (172.31.81.253): icmp_seq=2 ttl=255 time=0.358 ms
64 bytes from ip-172-31-81-253.ec2.internal (172.31.81.253): icmp_seq=3 ttl=255 time=0.372 ms
64 bytes from ip-172-31-81-253.ec2.internal (172.31.81.253): icmp_seq=4 ttl=255 time=0.486 ms
64 bytes from ip-172-31-81-253.ec2.internal (172.31.81.253): icmp_seq=5 ttl=255 time=0.415 ms
64 bytes from ip-172-31-81-253.ec2.internal (172.31.81.253): icmp_seq=6 ttl=255 time=2.35 ms
64 bytes from ip-172-31-81-253.ec2.internal (172.31.81.253): icmp_seq=7 ttl=255 time=2.77 ms
^C
--- ec2-100-26-99-73.compute-1.amazonaws.com ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6105ms
rtt min/avg/max/mdev = 0.358/1.048/2.773/0.967 ms
```

DNS lookup if target is a hostname

Size of packet

Hops from destination to source. Not too helpful since starting TTL is not always known.

Round trip return time (RTT) for single packet

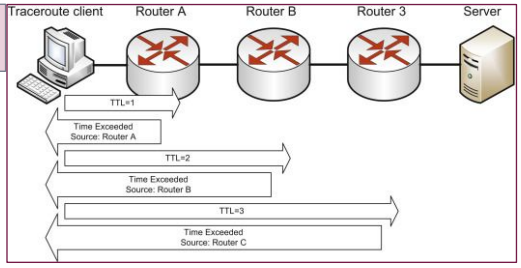
Summary statistics.
- Packet loss
- Min/max/avg RTT

2 traceroute (tracert)

`traceroute (tracert)` - Overview

- uses ICMP **ping** command by manipulating the Time To Live (**TTL**) value
- **identifies each router** between a source and destination device
- provides an ***indication* of latency**
- provides **clues to identify bottlenecks** in the path

how traceroute uses "ping" and TTL



`traceroute (tracert)` - Basic Syntax

Linux / MacOS(*)	`traceroute -I [DNS name] or [IP Address]`
Windows	`tracert [DNS name] or [IP Address]`

(*) without the -I option in Linux, traceroute may not always use the same route.

`traceroute` - Understanding the Output

```
C:>tracert www.example.com

Tracing route to example.com [93.184.216.34]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.0.1
  2     *        *        *     Request timed out.
  3     6 ms     5 ms     6 ms  100.123.249.2
  4    13 ms     8 ms     9 ms  ashbbprj02-ae2.0.rd.as.cox.net [68.1.4.139]
  5    95 ms   100 ms    90 ms  ae-104.border1.dcn.edgecastcdn.net [152.195.65.214]
  6    10 ms     8 ms     9 ms  ae-66.core1.dcb.edgecastcdn.net [152.195.65.129]
  7    10 ms     9 ms    10 ms  93.184.216.34
  8    84 ms    86 ms    84 ms  ae-40.a04.asbnva02.us.bb.gin.ntt.net [129.250.8.18]
  9    86 ms    86 ms    86 ms  ae-3.r24.asbnva02.us.bb.gin.ntt.net [129.250.2.144]
 10    85 ms    84 ms    85 ms  ae-2.r24.sanjose04.us.bb.gin.ntt.net [129.250.6.237]
 11    84 ms    85 ms    84 ms  cr1.attga.ip.sanjose04.net [153.149.219.34]
 12    85 ms    86 ms    84 ms  cr2.dlstx.ip.sanjose04.net [180.37.200.22]
 13    84 ms    84 ms    84 ms  cr2.la2ca.ip.sanjose04.net [61.126.91.154]
 14   107 ms    84 ms    85 ms  gar5.la2ca.ip.sanjose04.net [61.112.45.5]
 15    85 ms    85 ms    85 ms  61.126.30.78
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
```

- Destination domain, IP
- Hop number
- Some routers intentionally drop ICMP packets, '*' indicates a timeout
- Round trip time for *3 different* packets.
- Fully qualified domain name (FQDN); i.e. router name. Not always available.
- Router IP
- Sometimes, location can be inferred
- Last set of times is indicative of end-to-end latency

Sidebar: FQDN

- **FQDN** = **f**ully **q**ualified **d**omain **n**ame
- Example
  - Hostname: myserver
  - FQDN: myserver.mydomain.com
- Devices need to distinguish between **hosts on different networks**; e.g.:
  - FQDN: myserver.*mydomain*.com - Hostname: myserver
  - FQDN: myserver.*anotherplace*.com - ***also*** Hostname: myserver
- Especially important with hybrid network in AWS

`traceroute` - Inferences

"Request timed out" message near the beginning

```
 2     *        *        *     Request timed out.
```

- Common & typically a device that doesn't respond to traceroute requests.

"Request timed out" at the end

```
16     *        *        *     Request timed out.
17     *        *        *     Request timed out.
18     *        *        *     Request timed out.
```

- May or may not be a concern
- Firewall may be blocking ICMP (application may still work)
- Could be issue with return path
- Legitimate issue connecting to the system
- **This where you want to start troubleshooting**

Latency for a later hop is less than for an earlier hop

```
 4    13 ms     8 ms     9 ms  ashbbprj02-ae2.0.rd.as.cox.net [68.1.4.139]
 5    95 ms   100 ms    90 ms  ae-104.border1.dcn.edgecastcdn.net [152.195.65.214]
 6    10 ms     8 ms     9 ms  ae-66.core1.dcb.edgecastcdn.net [152.195.65.129]
```

- Some routers de-prioritize traceroute packets
- Results in higher latency
- Best to consider the final hop as an indicator of end-to-end latency

3 mtr (pathping)

`mtr (pathping)` - Overview

- mtr - "**My Traceroute**"
- combines functionality from both **ping and traceroute**
- automatic **refresh** with **configurable** output
- Windows (pathping) not as dynamic

`mtr (pathping)` - Basic Syntax

Linux / MacOS	`mtr [DNS name] or [IP Address]`
Windows	`pathping [DNS name] or [IP Address]`

`mtr (pathping)` - Understanding the Output

```
                                My traceroute  [v0.92]
ip-172-31-88-198.ec2.internal (172.31.88.198)          2021-10-02T02:11:22+0000
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                Packets                  Pings
 Host                         Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. ???
 2. ???
 3. ???
 4. 241.0.4.136               0.0%    66    0.4   0.4   0.4   0.5   0.0
 5. 243.253.19.66             0.0%    65    0.4   0.5   0.3   1.4   0.2
 6. 240.0.28.26               0.0%    65    0.7   0.5   0.3   9.0   1.1
 7. 240.0.28.6                0.0%    65   16.1  10.5   0.7  22.4   6.6
 8. 242.0.147.49              0.0%    65    0.5   1.8   0.3  13.8   3.3
 9. 52.93.28.227              0.0%    65    0.6   1.0   0.5  13.5   1.8
10. 100.100.2.46              0.0%    65    0.8   1.6   0.5  11.5   2.3
11. 99.82.181.25              0.0%    65    0.7   0.7   0.7   1.5   0.1
12. 209.85.241.240            0.0%    65    1.0   1.0   0.9   1.3   0.1
13. 209.85.246.81             0.0%    65    1.8   2.0   1.5   6.3   0.8
14. iad23s60-in-f14.1e100.net 0.0%    65    0.8   0.9   0.8   1.2   0.1
```

Can modify fields in display

Additional packet info

Ping statistics

Hops

Continuously refreshed statistics

4 ifconfig (ipconfig)

`ifconfig (ipconfig)` - Overview

- "**I**nter**f**ace **Config**uration" or "**IP Config**uration"
- Provides **fundamental information about network interfaces**, including:
  - IP, Subnet Mask, Default Gateway
  - MAC Address
  - IP Lease Information
  - Other network configuration parameters
- Also able to **set configuration parameters** for network interface
  - e.g. ipconfig /renew, ipconfig /release
  - e.g. ifconfig eth1 up, ifconfig eth1 down

`ifconfig (ipconfig)` - Basic Syntax

Linux / MacOS	`ifconfig`, *also* `ifconfig -a`
Windows	`ipconfig`, *also* `ipconfig /a`

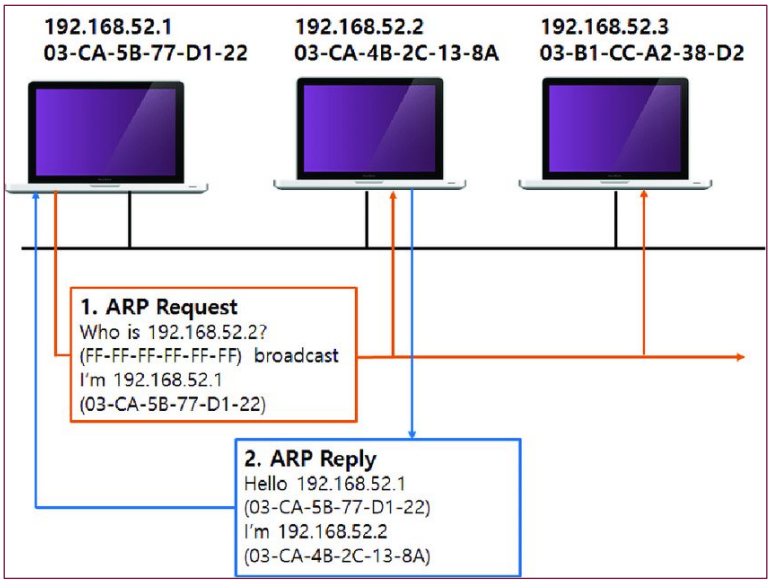
the "-a" and "/a" options shows information about all network interfaces

5 arp

`arp` - Overview

- arp - "**A**ddress **R**esolution **P**rotocol"
- used to translate **IP addresses to MAC addresses** using broadcasts
- Used when a device needs to send a packet:
  - First check is in its own **ARP cache** (or **MAC address lookup table**)
  - If not found, device will send out an **ARP broadcast**
- ARP cache clears entries until a timeout has expired
- The `arp` command is used to query and modify the ARP cache
  - Can be useful to identify errors in IP-to-MAC mapping or identifying duplicate IP addresses

ARP Broadcast



`arp` - Basic Syntax

Linux / MacOS / Windows	`arp -a` view the ARP cache `arp -s` add an entry to the cache `arp -d` delete an entry from the cache

`arp -a` - Understanding the Output

```
> arp -a

Interface: 192.168.1.178 --- 0x6
  Internet Address      Physical Address      Type
  192.168.1.1           b8-f8-53-45-37-0b     dynamic
  192.168.1.153         1c-fe-2b-34-3f-87     dynamic
  192.168.1.155         ec-5c-68-e4-7c-8e     dynamic
  192.168.1.254         94-9a-a9-67-d5-b7     static
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
```

IP address of network interface

IP to MAC address mapping

Typically entries are dynamic and managed by the device

In some cases static entries are created which must be changed manually

Entries in the cache should be for local IPs only, including the default gateway which is used to send information to other networks.

4 Using `nslookup`

`nslookup` - Overview

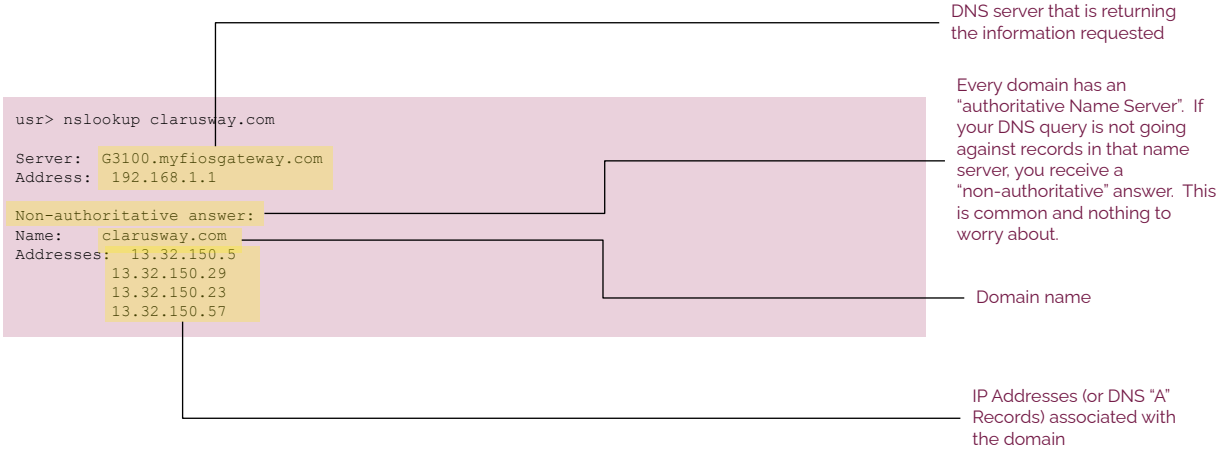
- used to perform **DNS queries** and receive:
  - **IP addresses**
  - other specific **DNS Records** (NS, MX, etc…)
- default behavior is to return IP address for a given domain
- does a lookup using the **default DNS server**
- useful to ensure your **DNS is properly configured**

`nslookup` - Basic Syntax

Linux / MacOS / Windows	`nslookup <domain name>`

in Unix-based systems, the `dig` command is favored over nslookup and achieves the same results.

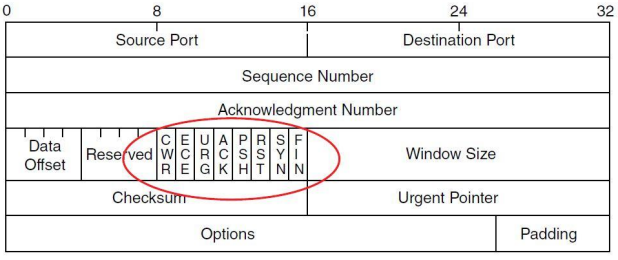
`nslookup` - Understanding the Output



6 nmap - a port scanning tool

nmap - Overview

- nmap is a popular port scanning **tool** (i.e. not a command)
- By scanning certain **flags in packets**, security analysts (and hackers) can make certain assumptions
- These flags are used to **control the TCP connection process** and so are present only in TCP packets



Using nmap

- Security analysts and hackers alike can perform **scans with these flags** set in the scan packets to get responses that allow them to determine the following information:
  - If a **port is open** on a device
  - If the port is **blocked by a firewall** before its gets to the device

- nmap can also be used:
  - To **determine the live hosts** on a network
  - To create a **logical "map" of the network**

7 Using `route`

`route` - Overview

- used to **view and manipulate the** network **route table**
- helpful to debug **outbound traffic issues**

`route` - Basic Syntax

Linux / Windows (MacOS: `netstat -rn`)	`route print`	prints the current route table
	`route -p add [opt]`	add a route
	`route -p change [opt]`	changes a route
	`route -p delete [opt]`	delete a route

be careful changing routes, it's complex and you must understand what you're doing

Sidebar - Special IPs

- **0.0.0.0/0**
  - "Everything else"
  - Traffic directed to the default gateway
  - Often means Internet traffic
- **x.x.x.x/32 (or x.x.x.x 255.255.255.255)**
  - Single IP x.x.x.x i.e. device

`route` - Understanding the Output

```
route print
===========================================================================
Interface List
 10...9c 7b ef 95 af 85 ......Intel(R) Ethernet Connection (4) I219-V
 13...a4 c3 f0 f2 35 24 ......Microsoft Wi-Fi Direct Virtual Adapter
 <snipped>
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.1.1    192.168.1.178     50
        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
      192.168.1.0    255.255.255.0         On-link    192.168.1.178    306
    192.168.1.178  255.255.255.255         On-link    192.168.1.178    306
    192.168.1.255  255.255.255.255         On-link    192.168.1.178    306
    255.255.255.255  255.255.255.255       On-link    192.168.1.178    306
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
<snipped>
```

available interfaces with MAC addresses

everything else not defined in this table goes to the default gateway

Loopback traffic

Traffic on local subnet

Traffic to itself

Route cost (lower is better).

Broadcast traffic

Read up for Windows

8 Using `netstat`

`netstat` - Overview

- **lists TCP/IP** connections on a device - both inbound and outbound
- alternatively, shows **packet statistics** - both sent and received
- helpful for:
  - **identifying connections** to/from a device
  - indicating **transmission errors**

`netstat` - Basic Syntax

Linux / MacOS / Windows	`netstat -a`	Shows connections
	`netstat -e`	displays overall packet statistics
	`netstat -s [-p <protocol>]`	displays protocol-level statistics

`netstat -a` - Understanding the Output

```
> netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  <snip>
  TCP    127.0.0.1:49477        kubernetes:49478       ESTABLISHED
  TCP    127.0.0.1:49478        kubernetes:49477       ESTABLISHED
  <snip>
  TCP    192.168.1.178:139      DESKTOP-D4LE3NN:0      LISTENING
  TCP    192.168.1.178:1025     40.76.170.235:https    TIME_WAIT
  TCP    192.168.1.178:1026     52.114.128.93:https    TIME_WAIT
  TCP    192.168.1.178:1027     52.96.90.34:https      TIME_WAIT
  TCP    192.168.1.178:1028     13.69.109.131:https    ESTABLISHED
  TCP    192.168.1.178:1029     52.113.206.22:https    ESTABLISHED
  TCP    192.168.1.178:1030     BRWEC5C68E47C8E:http   TIME_WAIT
  TCP    192.168.1.178:1031     52.96.35.178:https     ESTABLISHED
  TCP    192.168.1.178:1032     162.125.19.130:https   ESTABLISHED
  <snip>
```

Shows communication on the same machine between two ports (host:port).

Connection is active

Listening on port 139, available to connect

Remote device has disconnected, waiting to terminate

Example of a public IP connection

9 Using `tcpdump`

`tcpdump` - Overview

- used to **read packets** captured **live** from a network or previously **saved to a file**
- available on **Linux/MacOS**
- **WinDump** is a utility available for Windows
- output is extensive, must **filter for specific conditions** of interest
- helpful to troubleshoot and **check traffic** from a **specific IP** or on a **particular interface**

`tcpdump` - Basic Syntax

Linux / MacOS	`tcpdump`	view all traffic
	`tcpdump -i <interface>`	display traffic on interface
	`tcpdump host <IP>`	display traffic to/from host

10 Using `telnet`

`telnet` - Overview

- utility that allows you to make **connections to remote devices**
- can telnet to **any TCP port** to see if it's responding
- useful to check if **ports on remote machines are listening** - e.g. SMTP and HTTPS - a "quick & easy" test
- warning: it is **insecure** since it sends all data in clear text
- often, **not installed by default** on most devices

`telnet` - Basic Syntax

Linux / MacOS / Windows	`telnet <host> <port>`

12 Using `curl`

`curl` - Overview

- **transfer data to or from a server**, using any of the supported protocols
- very **helpful when no UI is available** (e.g. no web browser on Linux)
  - can check if remote web server is responding
  - or if a device is able to connect to a remote web server
- besides http & https, **supports many protocols**

`curl` - Basic Syntax

Linux / MacOS / Windows	`curl [options] URL`

13

Linux Network Configuration Files

CLARUSWAY©
WAY TO REINVENT YOURSELF

Network Configuration Files

- "**/etc/sysconfig/network**" file is a global configuration file. It allows us to define whether:
  - we want networking (NETWORKING=yes|no)
  - what the hostname should be (HOSTNAME=)
  - which gateway to use (GATEWAY=)

- "**/etc/hosts**" configuration file resolves hostnames that cannot be resolved any other way. It can also be used to resolve hostnames on small networks with no DNS server.

- "**/etc/resolv.conf**" file is used for configuring the DNS resolver library. It contains information parameters used by the DNS resolver.

14

Host-Based Firewalls

iptables (Linux)
Windows Firewall (Windows)

Firewalls - A Brief Overview

- one of a firewall's (FW) functions is **packet filtering**
- early on, this was based on **port-protocol rules** only
  - e.g. allow: TCP:80, TCP:443
- FWs can be **appliances** (hardware) or **software**
- firewall **placement varies**
  - typically a FW is placed at the **network perimeter**
  - sometimes, additional FWs are placed **inside a private network**
  - some FWs run **directly on a device**
- two common categories
  - **network FW**
  - **host-based FW**

Host-Based Firewalls

- by definition, **software-only**
- concerned only with **traffic in-and-out of the host**
- common host-based FWs
  - **iptables** (Linux)
  - **Windows Defender** (Windows) - sometimes just called **Windows Firewall**

Secure, but an Operational Headache

- FWs provide a much needed **layer of security** to an IT environment
- given concerns about security, there are sometimes **layers of FWs** that traffic needs to cross
  - e.g. perimeter FW → internal FW 1 → internal FW 2 → host-based FW
- downsides are:
  - **performance degradation**
  - operational challenges to **debug access and performance issues**
- understanding where FWs are and **how rules are constructed** is important

A last note on FWs: AWS Security Groups

- **AWS security groups (SGs)** protect EC2 instances much like host-based FWs
- many traditional security and IT practitioners continue to insist on additional host-based FWs
  - this creates yet **another layer of FWs** for traffic to traverse

`iptables` - Overview

- uses 3 "**chains**" to decide which rules to apply:
  - **Input** (inbound)
  - **Forward** (transient)
  - **Output** (outbound)
- uses 3 actions to decide what to do with the traffic:
  - **accept**
  - **drop** (no error returned)
  - **reject**
- various "front-ends" are available, such as Shorewall

`iptables` - Example Syntax

Linux / MacOS	`iptables -A INPUT -s 192.168.10.1 -j DROP`
	blocks a connection from the device at 192.168.10.1
	
	`iptables -A INPUT -s 172.16.0.0/16 -j DROP`
	blocks all connections from all devices in the 172.16.0.0/16 network
	
	`iptables -A INPUT -p tcp --dport ssh -s 10.110.61.5 -j DROP`
	blocks SSH connections from 10.110.61.5
	
	`iptables -A INPUT -p tcp --dport ssh -j DROP`
	blocks SSH connections from any IP address

15

Summary of Network Debugging Tools and Commands

Summary of Tools & Commands - Part 1

Tool/Command	What it Does	How it Helps	Notes
`ping`	Sends an ICMP “are you there?” request	Can determine definitively if a host is running	Cannot say for certain a host is down if it fails
`traceroute/tracert`	Sends ICMP requests to all routers on the path from source to destination	Identifies the number of hops from end-to-end and indicates latency	
`mtr/pathping`	Combines ping and tracert with continuous refresh	Identifies if a host is up and any potential latency issues	
`ifconfig/ipconfig`	Enables you to view or modify properties of network interfaces	Helps ensure interfaces are properly configured	
`arp`	Allows you to view or edit the ARP cache (IP-MAC address lookup)	Troubleshoot any outbound packet drops	Be wary of making changes to the ARP cache
`nslookup`	Provides DNS information about a particular domain	Debug to make sure source-to-destination connections are going where expected	

Summary of Tools & Commands - Part 2

Tool/Command	What it Does	How it Helps	Notes
`nmap`	A tool that allows you to discover open ports and map a network topology	Provides a birds-eye view of a network to identify which devices have which ports open	This is a 3rd party tool and may or may not be approved by an organization to use
`route`	View and edit the network route table	Troubleshoot any issues for any inbound or outbound packet loss	Be wary of changing a route table
`telnet`	Connect to a remote host on any port	Ensure remote ports are listening and a path exists from source to target	Telnet is insecure and not installed by default usually
`curl`	Receive or send information to a remote host using a range of protocols	Ensures that the remote application is connected and able to respond	Particularly useful when no UI is available, especially for http & https
Linux network configuration files	View and modify host aliases and resolver addresses	Look here to determine if the host is misconfigured with the wrong DNS server or aliases	
`iptables/` Windows Firewall	View and edit host-based firewall rules	Determine if any rules are blocking traffic you are expecting	There are layers of FWs in any network that cause operational headaches

Summary of Tools & Commands - Part 2

Tool/Command	What it Does	How it Helps	Notes
`nmap`	A tool that allows you to discover open ports and map a network topology	Provides a birds-eye view of a network to identify which devices have which ports open	This is a 3rd party tool and may or may not be approved by an organization to use
`route`	View and edit the network route table	Troubleshoot any issues for any inbound or outbound packet loss	Be wary of changing a route table
`netstat`	View TCP connections and packet statistics by protocol	Validate existing connections and identify issues with packet errors	
`tcpdump`	View live network traffic	Trace traffic from a particular host and/or ensure it is arriving	
`telnet`	Connect to a remote host on any port	Ensure remote ports are listening and a path exists from source to target	Telnet is insecure and not installed by default usually
`curl`	Receive or send information to a remote host using a range of protocols	Ensures that the remote application is connected and able to respond	Particularly useful when no UI is available, especially for http & https

Summary of Tools & Commands - Part 3

Tool/Command	What it Does	How it Helps	Notes
Linux network configuration files	View and modify host aliases and resolver addresses	Look here to determine if the host is misconfigured with the wrong DNS server or aliases	
`iptables/` Windows Firewall	View and edit host-based firewall rules	Determine if any rules are blocking traffic you are expecting	There are layers of FWs in any network that cause operational headaches

16

Accessing remote hosts

Using ssh

- Secure Shell (SSH) provides the same options as Telnet, plus a lot more and transfers the data in encrypted form
- To use SSH, your servers, routers, and other devices need to be enabled with SSH
- Syntax:
  `ssh user-name@host(IP or Domain Name)`

Using ftp

- File Transfer Protocol (FTP) is used for the transfer of files
- To start the ftp utility, enter `ftp` at a command prompt/terminal

```
C:\Users\clarusway>ftp
ftp> ?
Commands may be abbreviated.  Commands are:

!               delete          literal         prompt          send
?               debug           ls              put             status
append          dir             mdelete         pwd             trace
ascii           disconnect      mdir            quit            type
bell            get             mget            quote           user
binary          glob            mkdir           recv            verbose
bye             hash            mls             remotehelp
cd              help            mput            rename
close           lcd             open            rmdir
```

Using ftp

- To connect a FTP server type `open [server name]`

```
C:\Users\clarusway> ftp

ftp> open ftp.claruswaytrainer.com

Connected to ftp.claruswaytrainer.com.
220---------- Welcome to Pure-FTPd [TLS] ----------
220-You are user number 1 of 100 allowed.
220-Local time is now 11:45. Server port: 21.
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
User (ftp.claruswaytrainer.com:(none)): enter
230 Anonymous user logged in
ftp>
```

- After successfully connecting to the FTP server you need to log in with your username and password

Using ftp

- Before downloading a file from a FTP server you need to set the file type as **ASCII** or **binary**:

```
ftp>ascii
Type set to A
```

```
ftp>binary
Type set to I
```

- After setting up the file type use use `get` command to download the file:

```
ftp>get test.exe
200 PORT command successful.
150 Opening BINARY mode data connection for 'test.exe'
(567018 bytes).
```

- When the file has downloaded, following message is displayed:

```
226 Transfer complete.
567018 bytes received in 116.27 seconds (4.88 Kbytes/sec)
```

Using ftp

- To upload a file to a FTP server you have to have rights
- Before uploading file from a FTP server you need to set the file type as **ASCII** or **binary**
- After setting up the file type use use `put` command to upload the file:

```
ftp> put [local file] [destination file]
```

```
ftp> put test.txt myfile.txt
```

- When the file has uploaded, following message is displayed:

```
200 PORT command successful.
150 Opening BINARY mode data connection for myfile.txt
226 Transfer complete.
743622 bytes sent in 0.55 seconds (1352.04 Kbytes/sec)
```


Using scp

- `scp` (Secure Copy) a command-line tool which is used to transfer files and directories across the systems securely over the network through ssh connection
- Syntax:

```
scp <options> <files or directories> user@target-host:/<folder>
scp <options> user@target host:/files <folder-local-system>
```

17 Test Your Knowledge

I use ping against a remote device and there is no response.

Which of the following is definitely true?

A. The remote server is down

B. ICMP is not enabled on the remote device

C. A firewall along the way is blocking ICMP traffic

D. There is nothing for certain based on this ping result

I use traceroute and get the output below. Approximately what is the latency from source to target?

```
Tracing route to example.com [93.184.216.34]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.0.1
  2     *        *        *     Request timed out.
  3     6 ms     5 ms     6 ms  100.123.249.2
  4    13 ms     8 ms     9 ms  ashbbprj02-ae2.0.rd.as.cox.net [68.1.4.139]
  5    95 ms   100 ms    90 ms  ae-104.border1.dcn.edgecastcdn.net [152.195.65.214]
  6    10 ms     8 ms     9 ms  ae-66.core1.dcb.edgecastcdn.net [152.195.65.129]
  7    10 ms     9 ms    10 ms  93.184.216.34
```

A. Approximately 125ms (the sum of the 3rd column)

B. Approximately 10ms (one value in the 7th row)

C. Approximately 22ms (the average of all the columns)

D. Approximately 391ms (the sum of all the columns)

I use traceroute and get the output below. My manager tells me that there is an issue with the network at the 5th hop. Is she correct?

```
Tracing route to example.com [93.184.216.34]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.0.1
  2     *        *        *     Request timed out.
  3     6 ms     5 ms     6 ms  100.123.249.2
  4    13 ms     8 ms     9 ms  ashbbprj02-ae2.0.rd.as.cox.net [68.1.4.139]
  5    95 ms   100 ms    90 ms  ae-104.border1.dcn.edgecastcdn.net [152.195.65.214]
  6    10 ms     8 ms     9 ms  ae-66.core1.dcb.edgecastcdn.net [152.195.65.129]
  7    10 ms     9 ms    10 ms  93.184.216.34
```

A. No, chances are that router is de-prioritizing ICMP packets

B. No, chances are that router is dropping ICMP packets

C. No, my computer probably glitched when it sent that request

D. Yes, she's right

I use traceroute and get the output below. An application engineer looks at it and tells me traffic is being blocked at hop #2. Is it correct?

```
Tracing route to example.com [93.184.216.34]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.0.1
  2     *        *        *     Request timed out.
  3     6 ms     5 ms     6 ms  100.123.249.2
  4    13 ms     8 ms     9 ms  ashbbprj02-ae2.0.rd.as.cox.net [68.1.4.139]
  5    95 ms   100 ms    90 ms  ae-104.border1.dcn.edgecastcdn.net [152.195.65.214]
  6    10 ms     8 ms     9 ms  ae-66.core1.dcb.edgecastcdn.net [152.195.65.129]
  7    10 ms     9 ms    10 ms  93.184.216.34
```

A. Yes, the request definitely timed out

B. Yes, since every attempted ping resulted in a *

C. No, that router is most likely dropping ICMP requests

D. No, the previous result is <1ms and it's too fast for hop #2 to respond

You're on a Linux server within a secure company network which is not connected to the Internet. How do you find out what your IP is?

A. Use ipconfig

B. Use ifconfig

C. Use my browser to go to whatismyip.com

D. Check the resolver file at /etc/resolv.conf

You're on a Linux server with no GUI. You want to check if a specific website responds properly from that server. What will you do?

A. curl the URL

B. nslookup the domain

C. log in to my Windows laptop, which is on the same network anyhow, and use my browser

D. check the hosts file at /etc/hosts

Some asks you to check the local firewall rules on the Linux server that is having issues. What do you do?

A. call the security engineer, as a Cloud Architect I don't have to worry about firewall rules

B. log into the network firewall and download the rules to view on the server

C. check Defender, which is the host-based firewall

D. check iptables

8

Which of the following does not represent a single server?

A. 130.10.5.1

B. 192.168.255.255

C. 192.168.2.10

D. 192.168.2.10/32

9

You want to test your network bandwidth. What will you use?

A. ping

B. mtr

C. netstat

D. none of these

10

Traffic is not egressing from a single server to the default gateway? What might you do?

A. use arp to check the ARP cache and make sure the MAC address of the default gateway is correct

B. use iptables and make sure there is no outbound rule blocking traffic

C. use the “route print” command to verify the routes are properly setup

D. all of these

E. none of these

THANKS!

Any questions?

You can find me at:

- @David - Instructor
- david@clarusway.com