Troubleshooting Tools

CLARUSWAY©
WAY TO REINVENT YOURSELF

Using traceroute

- TCP/IP `traceroute` (`tracert` for Windows) command-line utility answers:
  - Where do all those packets go when we send them over the Internet?
  - How do all the packets actually get to their destinations?

- `Traceroute` displays the path a packet takes to get to a remote device by using **IP packet Time to Live (TTL)** time-outs and **Internet Control Message Protocol (ICMP)** error messages

- Syntax:
  Linux/MacOS: `traceroute [DNS name] or [IP Address]`
  Windows: `tracert [DNS name] or [IP Address]`

CLARUSWAY©
WAY TO REINVENT YOURSELF

Using traceroute

- This utility is useful if you are having problems reaching a web server on the Internet and you want to know if a WAN link is down or if the server just isn't responding
- Basically, wherever the trace stops is a great place to start troubleshooting
- `Traceroute` (or `tracert`) is a handy tool to find out where your network bottlenecks are
- `pathping` command is a combination of `ping` and `tracert` commands for Windows

Using ipconfig (Windows)

- The output of the `ipconfig` command provides the basic routed protocol information on your machine
- In case the `ipconfig` command doesn't provide enough information for you, try the `ipconfig /all` command
- When you change networks, you need to get the IP address of that subnet
- If you are connected to a DHCP server use `ipconfig /renew`, and if it doesn't work try `ipconfig /release` command first

Using ifconfig (Linux/MacOS):

- `ifconfig` is similar to `ipconfig` command
- `ipconfig` is used to view TCP/IP configuration, `ifconfig` is used to both view and configure the TCP/IP protocol
- Syntax:
  ```
  ifconfig interface [address [parameters]]
  ```


Using iptables (Linux/MacOS):

- `iptables` uses following chains to allow or disallow traffics
  - Input
  - Forward
  - Output
- You can set the default action to accept, drop, or reject

Using iptables (Linux/MacOS)

Examples:

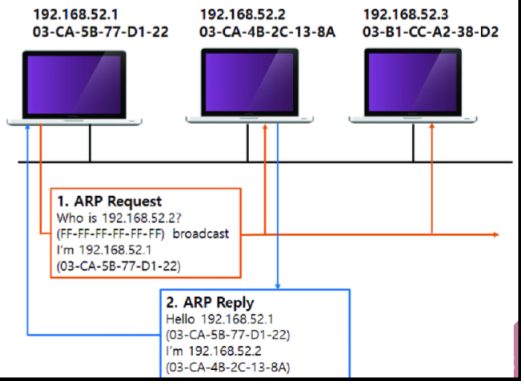
- To block a connection from the device at 192.168.10.1:
  ```
  iptables -A INPUT -s 192.168.10.1 -j DROP
  ```
- To block all connections from all devices in the 172.16.0.0/16 network:
  ```
  iptables -A INPUT -s 172.16.0.0/16 -j DROP
  ```
- Block SSH connections from 10.110.61.5:
  ```
  iptables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


Using ping

- `ping` is the most basic TCP/IP utility that is used to find out:
  - if a host is responding
  - if you can reach a host
- Syntax:
  ```
  ping hostname or IP address
  ```

Using Address Resolution Protocol (ARP)

- **ARP** is used to translate TCP/IP addresses to MAC addresses using broadcasts
- When a TCP/IP device needs to forward a packet to a device on the local subnet, it first looks in its own table, called an **ARP cache** or **MAC address lookup table**
- If no association that includes the destination IP address can be found, the device will then send out an **ARP broadcast**



CLARUSWAY©
WAY TO REINVENT YOURSELF

Using arp

- `arp` command displays and modifies the IP-to-Physical address translation tables used by ARP
- `arp` command is also useful for resolving duplicate IP addresses
- `arp -a` command displays the current ARP table

CLARUSWAY©
WAY TO REINVENT YOURSELF

Using nslookup

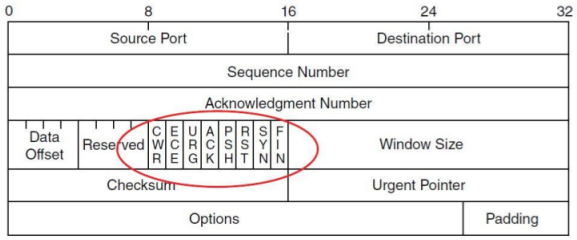
- `nslookup` utility allows you to query a name server and quickly find out which name resolves to which IP address
- `nslookup` utility tells different features of a particular domain name, the names of the servers that serve it, and how they're configured
- Syntax:
  `nslookup [option]`
- In Unix `dig` (domain information groper) commands does the exact same thing as `nslookup`

Using mtr (Linux/MacOS)

- `mtr` (My Traceroute) utility combines functions of `traceroute` and `ping`
- Also shows round-trip time and packet loss
- `pathping` in the Windows version of `mtr`

Using nmap

- `nmap` is a popular port scanning tool
- 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

Using route

- `route` command is used to manipulate network routing table
- The reason to manipulate the routing table on a server is to create a firewall
- To view the routing table on a device, use the `route print` command
- To add a route to your routing table, use the following syntax:

```
route [-f] [-p] [Command] [Destination] [mask Netmask]
[Gateway] [metric Metric] [if Interface]
```


Using route

- To add a route to the destination 10.1.1.0 with the subnet mask 255.255.255.0 and the next-hop address 10.2.2.2, type:
  `route add 10.1.1.0 mask 255.255.255.0 10.2.2.2`
- If you want to delete the route to the destination 10.100.0.0 with the subnet mask 255.255.0.0, enter:
  `route delete 10.100.0.0 mask 255.255.0.0`
- If you want to change the next-hop address of a route with the destination 10.100.0.0 and the subnet mask 255.255.0.0 from 10.2.0.1 to 10.7.0.5, type:
  `route change 10.100.0.0 mask 255.255.0.0 10.7.0.5`

Using netstat

- `netstat` checks out the inbound and outbound TCP/IP connections on your machine
- Can also be used to view packet statistics like how many packets have been sent and received, the number of errors, and so on
- `netstat -a`: Displays all TCP/IP and UDP connections
- `netstat -e`: Displays a summary of all the packets that have been sent over the NIC as of that instant

```
C:\Users\myuser>netstat -e
Interface Statistics

                           Received            Sent

Bytes                     652308520       724669536
Unicast packets             7476729         5597781
Non-unicast packets            6906          240780
Discards                          0               0
Errors                            0               1
Unknown protocols                 0
```


Using netstat

- `netstat -r`: Display the current route table for a workstation so that you can see exactly how TCP/IP information is being routed
- `netstat -s`: Displays a variety of TCP, UDP, IP, and ICMP protocol statistics
- `netstat -p`: Usually used with the -s switch to specify which protocol statistics to list in the output (IP, TCP, UDP, or ICMP):

```
netstat -s -p ICMP
```

- `netstat -n`: Reverses the natural tendency of netstat to use names instead of network addresses --displays network addresses instead of their associated network names

Using tcpdump (Linux/MacOS)

- `tcpdump` used to read either packets captured live from a network or packets that have been saved to a file
- `tcpdump -i any`: Captures traffic on all interfaces
- `tcpdump -i [eth0]`: Captures traffic on a particular interface
- `tcpdump host 192.168.5.5`: Filters traffic by IP, whether it's the source or the destination
- `windump` is the Windows version of `tcpdump`

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)
```

CLARUSWAY©
WAY TO REINVENT YOURSELF

34

Using telnet

- Telnet is a virtual terminal protocol utility that allows you to make connections to remote devices, gather information, and run programs
- You can telnet to any TCP port to see if it's responding—something that's especially useful when checking SMTP and HTTP ports
- Telnet is totally insecure because it sends all data in clear text including usernames and passwords!

CLARUSWAY©
WAY TO REINVENT YOURSELF

36

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 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>
```

Using curl

- `curl` is a command-line tool to transfer data to or from a server, using any of the supported protocols
- Syntax:
  `curl [options] [URL...]`

```
user@clarusway:~$ curl https://www.clarusway.com
```

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.

CLARUSWAY©
WAY TO REINVENT YOURSELF