Lanka Education and Research Network

Network Troubleshooting

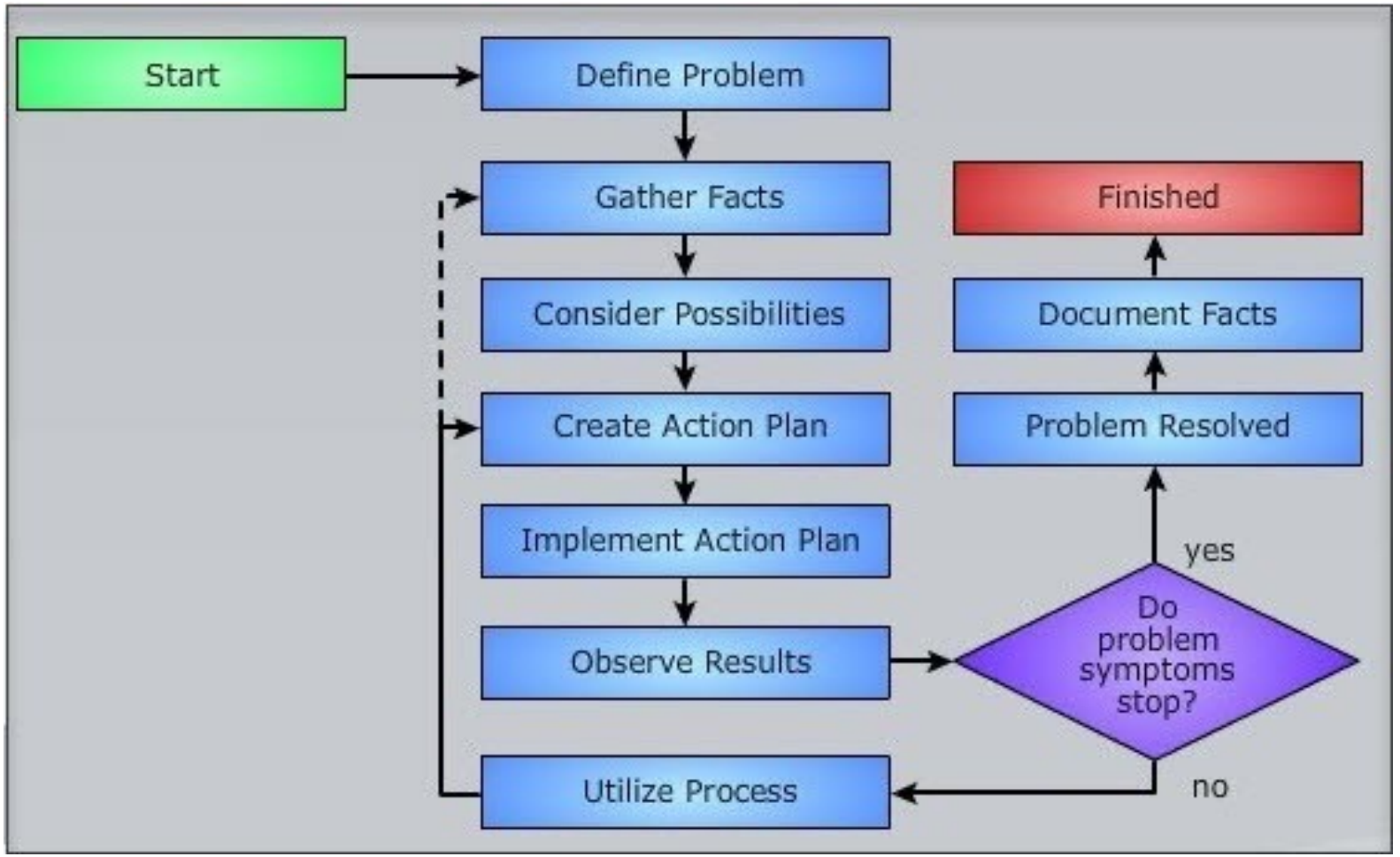
What is Network Troubleshooting?

The combined measures and processes used to identify, diagnose and solve problems within a computer network

Basic Network Problems

- Cable Problem
- Connectivity Problem
- Configuration Issue
- Software Issue
- Network IP issue

Network Troubleshooting Flowchart



Ifconfig/ ipconfig command

Used to initialize an interface, assign **IP Address** to interface and **enable** or **disable** interface on demand.

```
$ifconfig

lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
        options=1203<RXCSUM,TXCSUM,TXSTATUS,SW_TIMESTAMP>
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=201<PERFORMNUD,DAD>

en5: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether ac:de:48:00:11:22
        inet6 fe80::aede:48ff:fe00:1122%en5 prefixlen 64 scopeid 0x4
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect (100baseTX <full-duplex>)
        status: active
```

What is Wireshark?

ifconfig with interface (eth0) command only shows specific interface details

```
$ifconfig en5

en5: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether ac:de:48:00:11:22
        inet6 fe80::aede:48ff:fe00:1122%en5 prefixlen 64 scopeid 0x4
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect (100baseTX <full-duplex>)
        status: active
```

Set IP Address and Gateway

```
# ifconfig en5 192.168.50.5 netmask 255.255.255.0
```

Enable or Disable Specific Interface

Enable interface - en5

```
# ifup en5
```

Disable interface - en5

```
# ifdown en5
```

Ping command

Best way to test connectivity between **two nodes**. Whether it is **Local Area Network** (**LAN**) or **Wide Area Network** (**WAN**).

```
$ping 8.8.8.8

PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=114 time=75.282 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=114 time=61.654 ms
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 60.929/64.246/75.282/5.024 ms

$ping google.com

PING google.com (172.217.194.113): 56 data bytes
64 bytes from 172.217.194.113: icmp_seq=0 ttl=107 time=63.789 ms
64 bytes from 172.217.194.113: icmp_seq=1 ttl=107 time=59.188 ms
--- google.com ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 55.408/67.418/79.370/7.670 ms
```

Traceroute command

Shows the number of hops taken to reach a destination also determines packets traveling path. Below we are tracing the route to the global **DNS server IP Address** and able to reach destination also shows the path of that packet is traveling

```
$traceroute 8.8.8.8

traceroute to 8.8.8.8 (8.8.8.8), 64 hops max, 52 byte packets
 1 192.168.1.1 (192.168.1.1)  21.451 ms  2.849 ms  2.837 ms
 2  * * *
 3 172.22.92.193 (172.22.92.193)  55.131 ms  51.592 ms  48.824 ms
 4  * * *
 5 172.22.65.90 (172.22.65.90)  312.464 ms  151.647 ms  186.787 ms
 6 15169.sgw.equinix.com (27.111.228.30)  87.426 ms  78.694 ms  77.910 ms
 7 74.125.242.33 (74.125.242.33)  96.145 ms
   108.170.240.225 (108.170.240.225)  87.970 ms
   108.170.240.161 (108.170.240.161)  77.927 ms
 8 142.251.49.191 (142.251.49.191)  75.174 ms  72.413 ms
   72.14.232.101 (72.14.232.101) 89.639 ms
 9 dns.google (8.8.8.8)  90.537 ms  80.010 ms  110.956 ms
```

Dig command

Query **DNS** related information like A Record, **CNAME**, **MX Record,**etc.
This command is mainly used to troubleshoot **DNS-related** queries.

```
$ dig ac.lk
; <<>> DiG 9.10.6 <<>> ac.lk
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44230
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;ac.lk. IN A

;; ANSWER SECTION:
ac.lk. 7200 IN A 192.248.1.189

;; Query time: 58 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Fri Mar 25 13:14:14 +0530 2022
;; MSG SIZE  rcvd: 50
```

Nslookup command

Used to find out **DNS-related** queries. This shows the A record(IP address) of ac.lk

```
 $ nslookup ac.lk
Server: 192.168.1.1
Address: 192.168.1.1#53


Non-authoritative answer:
Name: ac.lk
```

Netstat command

Displays connection info, routing table information

```
$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         192.248.3.254   0.0.0.0         UG        0 0          0 ens5
172.17.0.0      *               255.255.0.0     U         0 0          0 docker0
192.248.3.192   *               255.255.255.192 U         0 0          0 ens5
```

Route command

Shows and manipulates the **ip** routing table

```
$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.248.3.254   0.0.0.0         UG    0      0        0 ens5
172.17.0.0      *               255.255.0.0     U     0      0        0 docker0
192.248.3.192   *               255.255.255.192 U     0      0        0 ens5
```

Host command

To find a name to **IP** or **IP** to name in **IPv4** or **IPv6** and also query **DNS** records

```
$ host google.com
google.com has address 142.251.10.139
google.com has address 142.251.10.138
google.com has address 142.251.10.101
google.com has address 142.251.10.113
google.com has address 142.251.10.100
google.com has address 142.251.10.102
google.com has IPv6 address 2404:6800:4003:c0f::71
google.com has IPv6 address 2404:6800:4003:c0f::64
google.com has IPv6 address 2404:6800:4003:c0f::66
google.com has IPv6 address 2404:6800:4003:c0f::8a
google.com mail is handled by 40 alt3.aspmx.l.google.com.
google.com mail is handled by 10 aspmx.l.google.com.
google.com mail is handled by 20 alt1.aspmx.l.google.com.
google.com mail is handled by 30 alt2.aspmx.l.google.com.
google.com mail is handled by 50 alt4.aspmx.l.google.com.
```

Arp command

ARP (Address Resolution Protocol) is useful to **view/add** the contents of the kernel's **ARP tables**.

```
$ arp -a
(192.168.1.1) at fc:dd:55:8d:7f:b7 on en0 ifscope [ethernet]
(224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
```

Iperf command

Used **in diagnosing network speed issues by measuring the maximum network throughput a server can handle**

Start **iperf** on the server:

```
$./iperf3 -s
```

This waits for incoming connections from clients. Designate another machine as a client and run this command

```
$./iperf3 -c localhost -n 10240M
```

Note : you may change localhost to ip you need to use and also desired amount of data(defaut buffer size of 8KB)

Output in server:

$./iperf3 -s

```
-----------------------------------------------------------
Server listening on 5201
-----------------------------------------------------------
Accepted connection from ::1, port 56861
[  5] local ::1 port 5201 connected to ::1 port 56862
[ ID] Interval           Transfer     Bandwidth
[  5]   0.00-1.00   sec  5.59 GBytes  48.0 Gbits/sec
[  5]   1.00-1.83   sec  4.41 GBytes  45.9 Gbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth
[  5]   0.00-1.83   sec  0.00 Bytes  0.00 bits/sec                  sender
[  5]   0.00-1.83   sec  10.0 GBytes  47.0 Gbits/sec                  receiver
```

Output in client:

$./iperf3 –c localhost -n 10240M

```
Connecting to host localhost, port 5201
[  6] local ::1 port 56862 connected to ::1 port 5201
[ ID] Interval           Transfer     Bandwidth
[  6]   0.00-1.00   sec  5.59 GBytes  48.0 Gbits/sec
[  6]   1.00-1.83   sec  4.41 GBytes  45.9 Gbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth
[  6]   0.00-1.83   sec  10.0 GBytes  47.0 Gbits/sec                  sender
[  6]   0.00-1.83   sec  10.0 GBytes  47.0 Gbits/sec                  receiver
```

telnet command

Troubleshooting connection problems on hosted servers

```
$ telnet ac.lk 80

Trying 2401:dd00:1::189...
Connected to ac.lk.
Escape character is '^]'.
```

Nmap command

This utility used for network discovery and security auditing. It is a globally recognized tool mostly used by networking experts and penetration testers to find services, hosts, and open ports on a computer network

Use following command on terminal to for more info:

```
$ man nmap
```

Scan a range of IPs

```
$ nmap 192.168.2.125-135
```

Port scanning

```
$ nmap -p 80 192.168.2.128
```

Ping Scan

```
$ Nmap -sP 192.168.2.1/24
```

Nmap command

Display open ports

```
$ nmap — open 198.152.45.33
```

Exclude Host/ IP Addresses for the Scan

```
$ nmap 172.16.121.1/24 — exclude 172.16.121.10
```

Thank you