Scalable Network Design for Schools

Troubleshooting Basics

Ronald Matovu
rmatovu@renu.ac.ug

Troubleshooting Basics

Outline

- Troubleshooting steps
- Utilities
- Tools

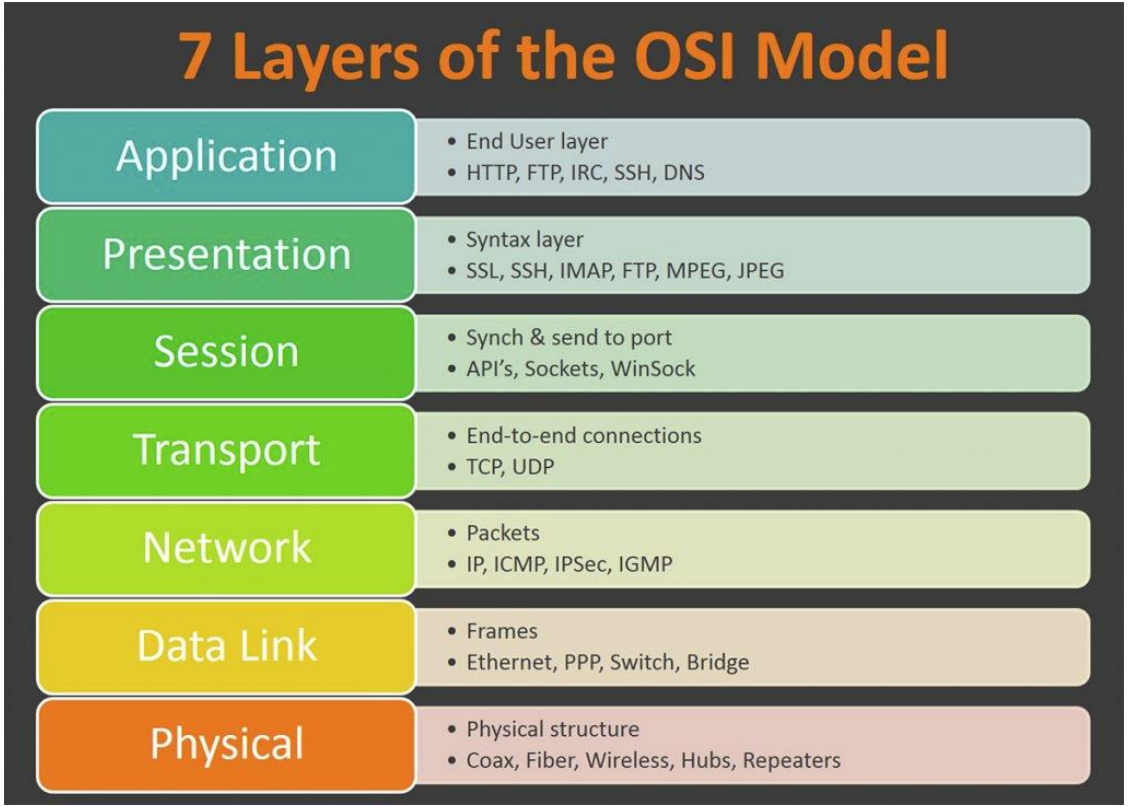
Network Troubleshooting

- Networks always break !!!
- Troubleshooting should be hierarchical, OSI model?
- Standard troubleshooting procedures

Common Network Problems

- Loss of Internet connectivity
- Slow internet connection
- Unreachable parts of the network
- Unreachable servers/resources
- High packet loss
- Unable to send/receive mail

Troubleshooting with the OSI Model



Troubleshooting steps

Step 1: Identify the problem.

Step 2: Establish a theory of probable cause.

Step 3: Test the theory to determine the cause (OSI model).

Step 4: Establish a plan of action to resolve the problem and implement the solution.

Step 5: Verify full system functionality and, if applicable, implement preventive measures.

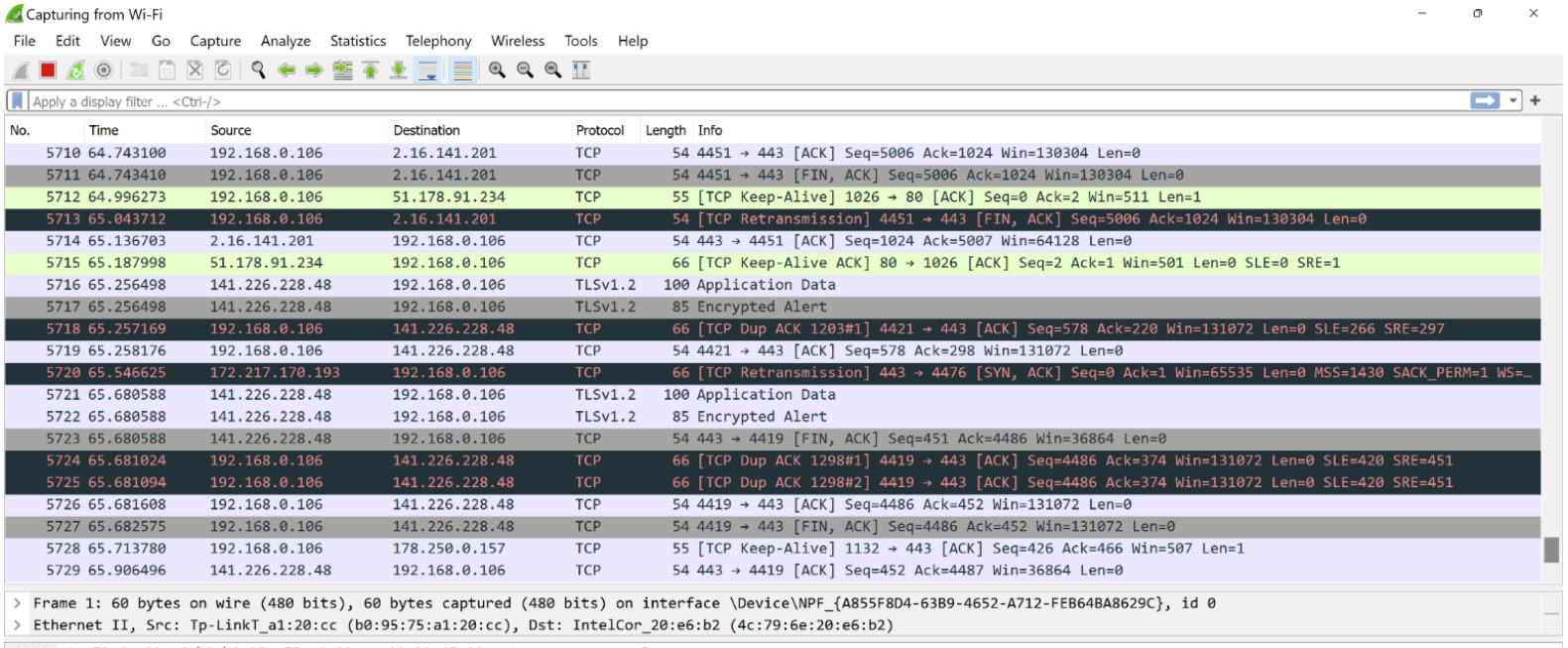
Step 6: Document findings, actions, and outcomes.

Layer 1

- Power issues
- Access links
  - Copper cable, wireless network
  - Understand cabling specifications
- Last mile connection
  - Fiber, wireless
  - Transmission issues
- Tools
    - Network analyzer
    - Cable tester

Layer 2

- Problems at Layer 2
  - Corrupted packet flooding
  - Flooding from MAC Misconfigurations
- Tools - wireshark



Layer 3

- IP Address related problems
  - wrong default gateways, subnet masks
  - Interface statistics
  - Services (DHCP, DNS)
- Routing problems
  - Routes to nowhere.
- Slow network
- Inability to reach certain network resources
- Tools & utilities
  - ping, traceroute, ipconfig, ifconfig, mtr, PingPlotter, pathping

Ping command

Utility used to test the reachability of a host on an Internet Protocol (IP) network.

- Uses ICMP
- IPv4 or IPv6 hosts

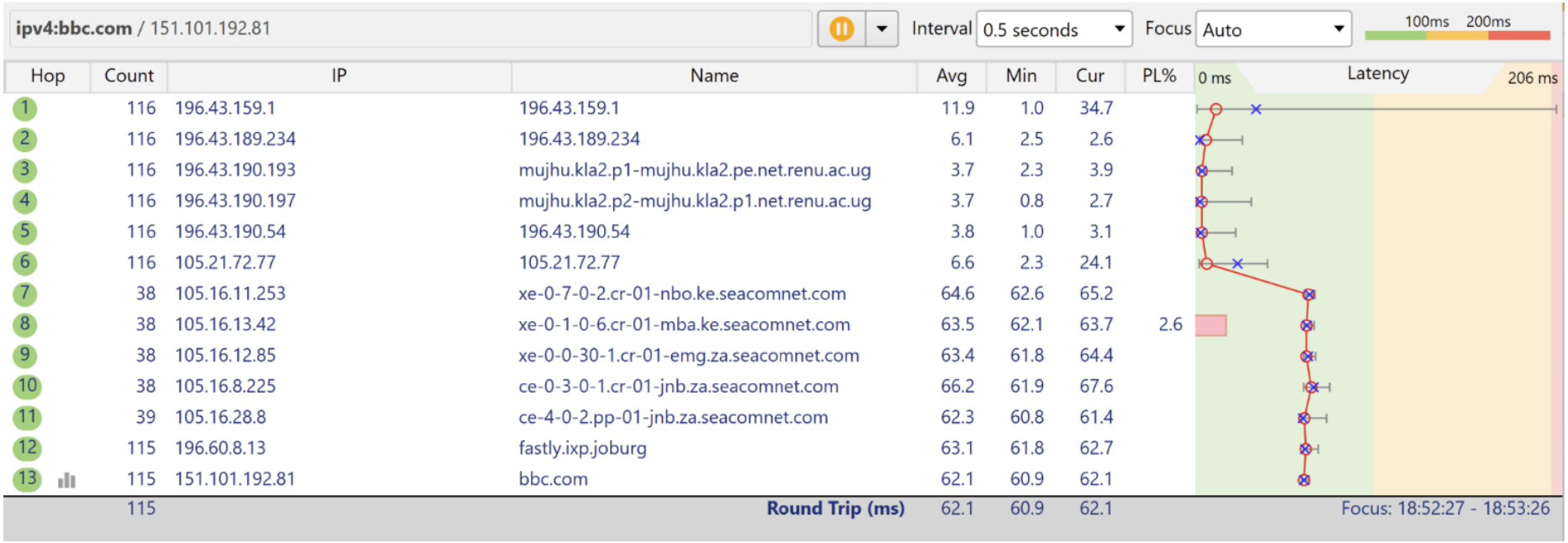
```
C:\Users\Ronald Matovu>ping google.com -4 -n 10

Pinging google.com [172.217.170.174] with 32 bytes of data:
Reply from 172.217.170.174: bytes=32 time=30ms TTL=54
Reply from 172.217.170.174: bytes=32 time=18ms TTL=54
Reply from 172.217.170.174: bytes=32 time=19ms TTL=54
Reply from 172.217.170.174: bytes=32 time=20ms TTL=54
Reply from 172.217.170.174: bytes=32 time=18ms TTL=54
Reply from 172.217.170.174: bytes=32 time=24ms TTL=54
Reply from 172.217.170.174: bytes=32 time=19ms TTL=54
Reply from 172.217.170.174: bytes=32 time=120ms TTL=54
Reply from 172.217.170.174: bytes=32 time=53ms TTL=54
Reply from 172.217.170.174: bytes=32 time=19ms TTL=54

Ping statistics for 172.217.170.174:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 18ms, Maximum = 120ms, Average = 34ms
```

traceroute command

Traceroute is a command line utility that shows the path taken by a packet to a destination server.

- Uses ICMP, but can use TCP
- Used on several platforms
  - Traceroute Linux, MacOS
  - tracert - Windows
- Other forms and tools
  - mtr
  - pathping

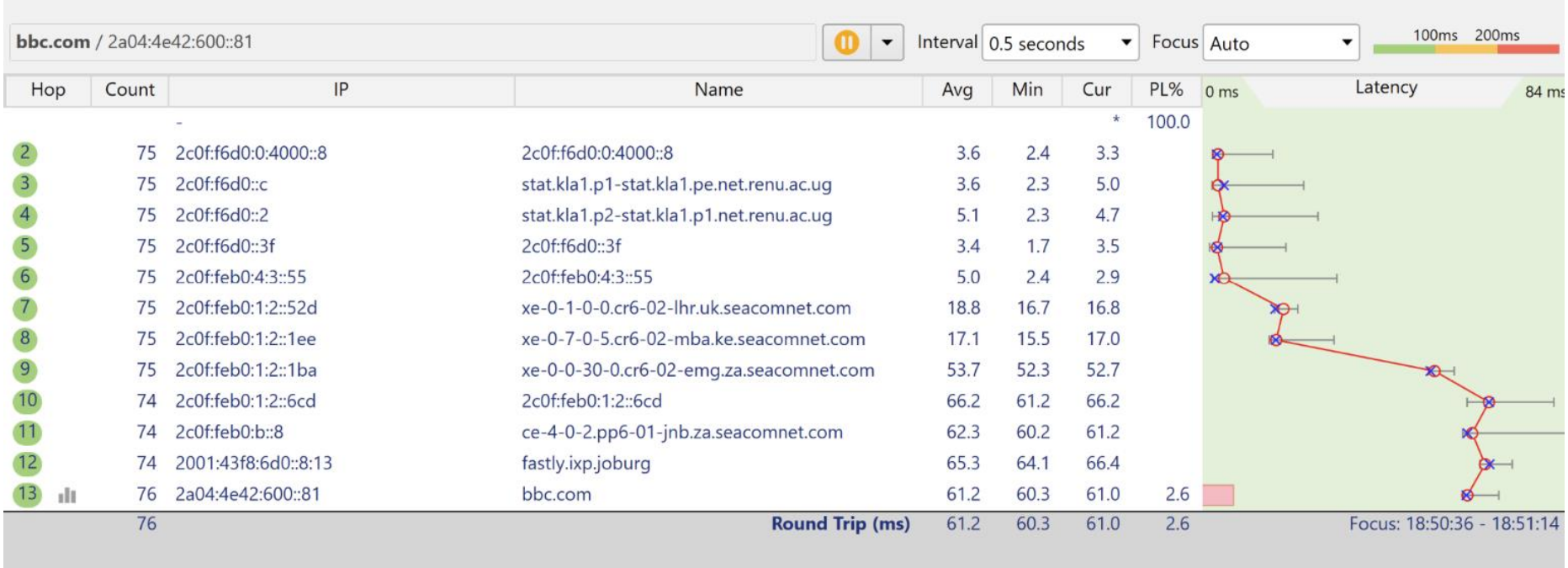
PingPlotter examples



Hop	Count	IP	Name	Avg	Min	Cur	PL%
1	116	196.43.159.1	196.43.159.1	11.9	1.0	34.7	
2	116	196.43.189.234	196.43.189.234	6.1	2.5	2.6	
3	116	196.43.190.193	mujhu.kla2.p1-mujhu.kla2.pe.net.renu.ac.ug	3.7	2.3	3.9	
4	116	196.43.190.197	mujhu.kla2.p2-mujhu.kla2.p1.net.renu.ac.ug	3.7	0.8	2.7	
5	116	196.43.190.54	196.43.190.54	3.8	1.0	3.1	
6	116	105.21.72.77	105.21.72.77	6.6	2.3	24.1	
7	38	105.16.11.253	xe-0-7-0-2.cr-01-nbo.ke.seacomnet.com	64.6	62.6	65.2	
8	38	105.16.13.42	xe-0-1-0-6.cr-01-mba.ke.seacomnet.com	63.5	62.1	63.7	2.6
9	38	105.16.12.85	xe-0-0-30-1.cr-01-emg.za.seacomnet.com	63.4	61.8	64.4	
10	38	105.16.8.225	ce-0-3-0-1.cr-01-jnb.za.seacomnet.com	66.2	61.9	67.6	
11	39	105.16.28.8	ce-4-0-2.pp-01-jnb.za.seacomnet.com	62.3	60.8	61.4	
12	115	196.60.8.13	fastly.ixp.joburg	63.1	61.8	62.7	
13	115	151.101.192.81	bbc.com	62.1	60.9	62.1	
	115		**Round Trip (ms)**	62.1	60.9	62.1	

Focus: 18:52:27 - 18:53:26

PingPlotter examples

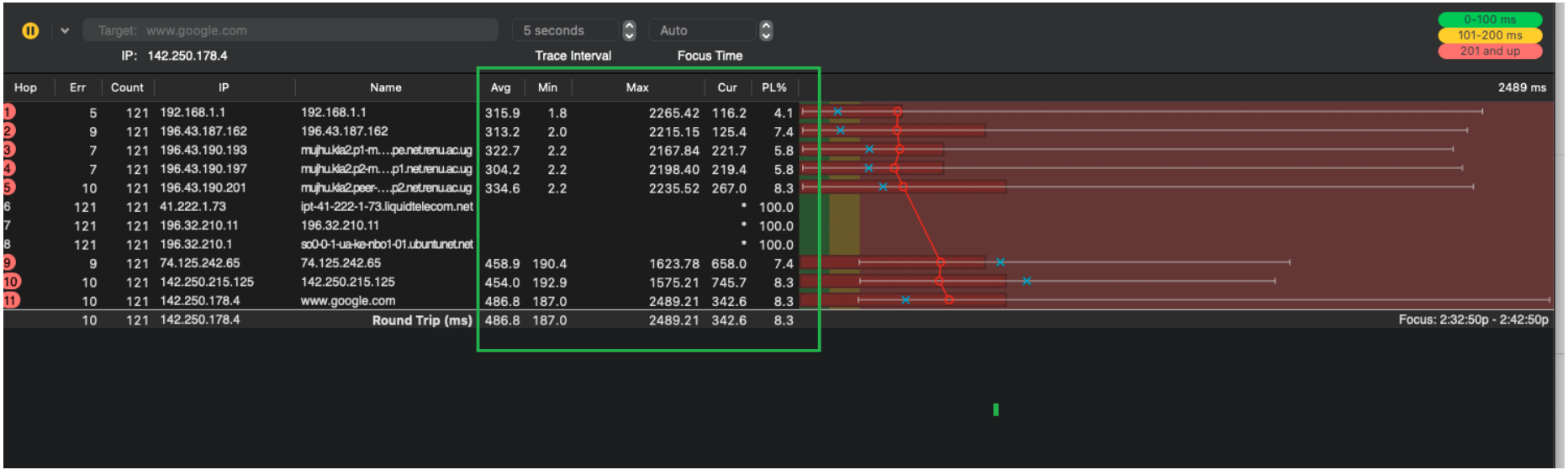


bbc.com / 2a04:4e42:600::81 — Interval: 0.5 seconds — Focus: Auto — 100ms 200ms

Hop	Count	IP	Name	Avg	Min	Cur	PL%
		-				*	100.0
2	75	2c0f:f6d0:0:4000::8	2c0f:f6d0:0:4000::8	3.6	2.4	3.3	
3	75	2c0f:f6d0::c	stat.kla1.p1-stat.kla1.pe.net.renu.ac.ug	3.6	2.3	5.0	
4	75	2c0f:f6d0::2	stat.kla1.p2-stat.kla1.p1.net.renu.ac.ug	5.1	2.3	4.7	
5	75	2c0f:f6d0::3f	2c0f:f6d0::3f	3.4	1.7	3.5	
6	75	2c0f:feb0:4:3::55	2c0f:feb0:4:3::55	5.0	2.4	2.9	
7	75	2c0f:feb0:1:2::52d	xe-0-1-0-0.cr6-02-lhr.uk.seacomnet.com	18.8	16.7	16.8	
8	75	2c0f:feb0:1:2::1ee	xe-0-7-0-5.cr6-02-mba.ke.seacomnet.com	17.1	15.5	17.0	
9	75	2c0f:feb0:1:2::1ba	xe-0-0-30-0.cr6-02-emg.za.seacomnet.com	53.7	52.3	52.7	
10	74	2c0f:feb0:1:2::6cd	2c0f:feb0:1:2::6cd	66.2	61.2	66.2	
11	74	2c0f:feb0:b::8	ce-4-0-2.pp6-01-jnb.za.seacomnet.com	62.3	60.2	61.2	
12	74	2001:43f8:6d0::8:13	fastly.ixp.joburg	65.3	64.1	66.4	
13	76	2a04:4e42:600::81	bbc.com	61.2	60.3	61.0	2.6
	76		**Round Trip (ms)**	61.2	60.3	61.0	2.6

Latency: 0 ms — 84 ms — Focus: 18:50:36 - 18:51:14

PingPlotter examples



Hop	Err	Count	IP	Name	Avg	Min	Max	Cur	PL%
1	5	121	192.168.1.1	192.168.1.1	315.9	1.8	2265.42	116.2	4.1
2	9	121	196.43.187.162	196.43.187.162	313.2	2.0	2215.15	125.4	7.4
3	7	121	196.43.190.193	mujhu.kla2.p1-m…pe.net.renu.ac.ug	322.7	2.2	2167.84	221.7	5.8
4	7	121	196.43.190.197	mujhu.kla2.p2-m…p1.net.renu.ac.ug	304.2	2.2	2198.40	219.4	5.8
5	10	121	196.43.190.201	mujhu.kla2.peer-….p2.net.renu.ac.ug	334.6	2.2	2235.52	267.0	8.3
6	121	121	41.222.1.73	ipt-41-222-1-73.liquidtelecom.net				*	100.0
7	121	121	196.32.210.11	196.32.210.11				*	100.0
8	121	121	196.32.210.1	sc0-0-1-ua-ke-nbo1-01.ubuntunet.net				*	100.0
9	9	121	74.125.242.65	74.125.242.65	458.9	190.4	1623.78	658.0	7.4
10	10	121	142.250.215.125	142.250.215.125	454.0	192.9	1575.21	745.7	8.3
11	10	121	142.250.178.4	www.google.com	486.8	187.0	2489.21	342.6	8.3
	10	121	142.250.178.4	Round Trip (ms)	486.8	187.0	2489.21	342.6	8.3

High RTT at the first hop,
Packet loss at the LAN

ARP - Address Resolution Protocol

Procedure that connects a dynamic Internet Protocol (IP) address to a fixed physical machine address, also known as a media access control (MAC) address, in a local-area network (LAN).

Who is this?

- https://macvendors.com/
- https://dnschecker.org/mac-lookup.php


```
C:\Users\Ronald Matovu>arp -a

Interface: 192.168.56.1 --- 0xb
  Internet Address      Physical Address      Type
  192.168.56.255        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
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.106.196 --- 0x14
  Internet Address      Physical Address      Type
  192.168.98.7          38-be-ab-bc-32-68     dynamic
  192.168.98.35         30-7b-c9-c6-af-1d     dynamic
  192.168.98.101        f8-b5-4d-6d-6c-f8     dynamic
  192.168.99.196        38-be-ab-bc-4b-a4     dynamic
  192.168.100.43        28-39-5e-d3-87-0a     dynamic
  192.168.100.166       d8-e0-e1-12-79-a2     dynamic
  192.168.100.207       3c-91-80-e6-58-5f     dynamic
  192.168.102.207       48-51-b7-3f-21-c2     dynamic
  192.168.102.228       24-0a-64-cf-e1-31     dynamic
  192.168.104.148       e6-59-20-b2-a5-c9     dynamic
  192.168.105.29        a4-fc-77-22-bc-47     dynamic
  192.168.107.1         10-b2-32-29-ca-cc     dynamic
  192.168.107.141       3c-91-80-de-b9-71     dynamic
  192.168.107.204       3c-91-80-de-b9-b0     dynamic
  192.168.107.237       20-10-7a-77-9d-2f     dynamic
  192.168.108.86        28-39-5e-d3-ac-07     dynamic
```

ipconfig or ifconfig

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : localdomain
   Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   Physical Address. . . . . . . . . : 9C-B6-54-20-28-98
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::a1ed:ce11:be62:7a4%24(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.2.88(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Saturday, March 13, 2021 11:04:10 AM
   Lease Expires . . . . . . . . . . : Saturday, March 13, 2021 1:04:10 PM
   Default Gateway . . . . . . . . . : 192.168.2.2
   DHCP Server . . . . . . . . . . . : 192.168.2.2
   DHCPv6 IAID . . . . . . . . . . . : 396146260
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-27-97-A2-C1-02-00-4C-4F-4F-50
   DNS Servers . . . . . . . . . . . : 196.43.185.3
                                       196.43.185.35
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

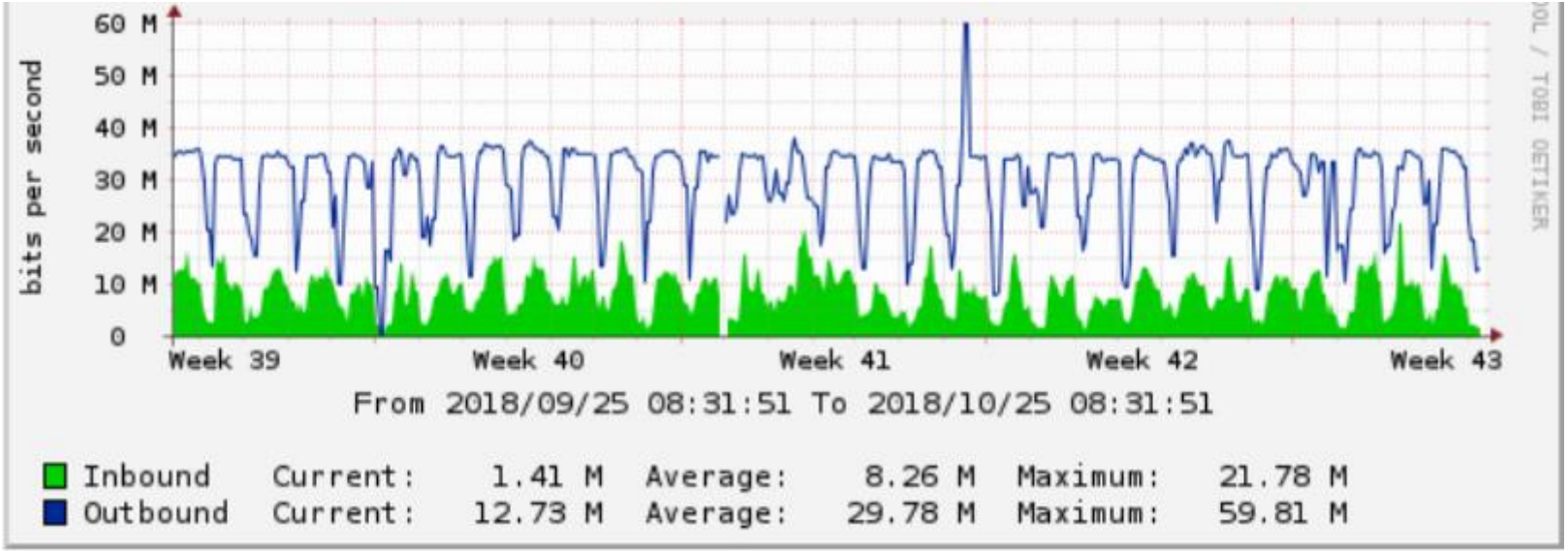
ipconfig or ifconfig

- 169.254.0.0/16

  Automatic Private IP Addressing (APIPA)

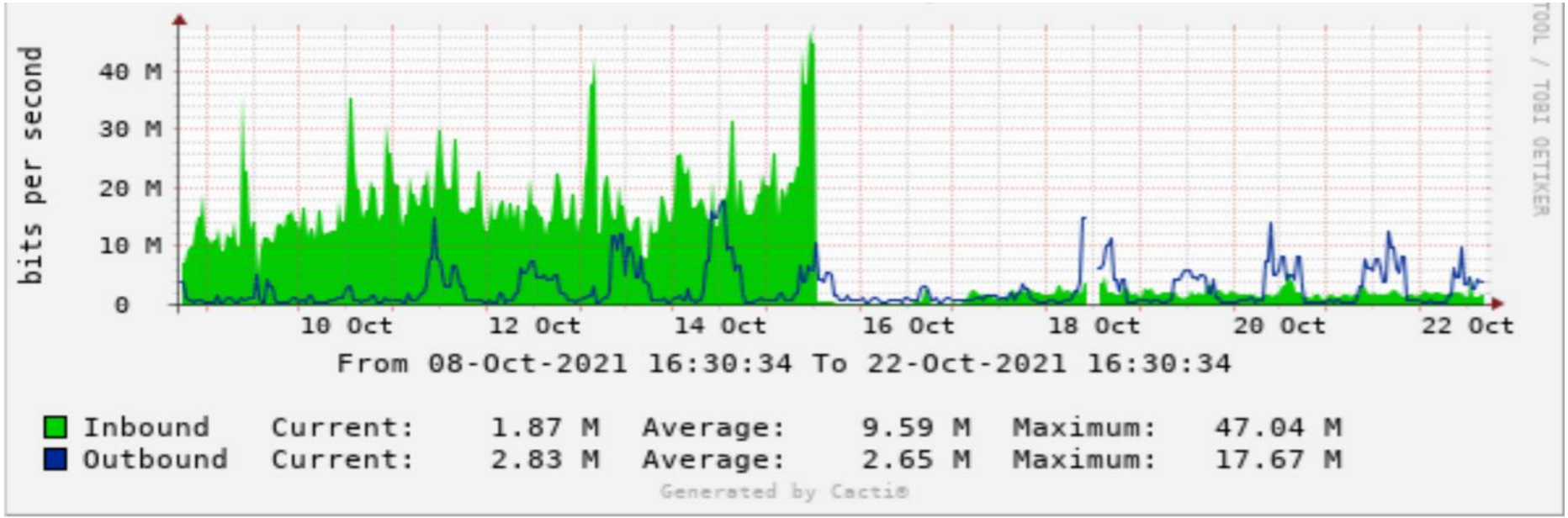
- DHCP unreachable

Bandwidth Utilisation - cacti



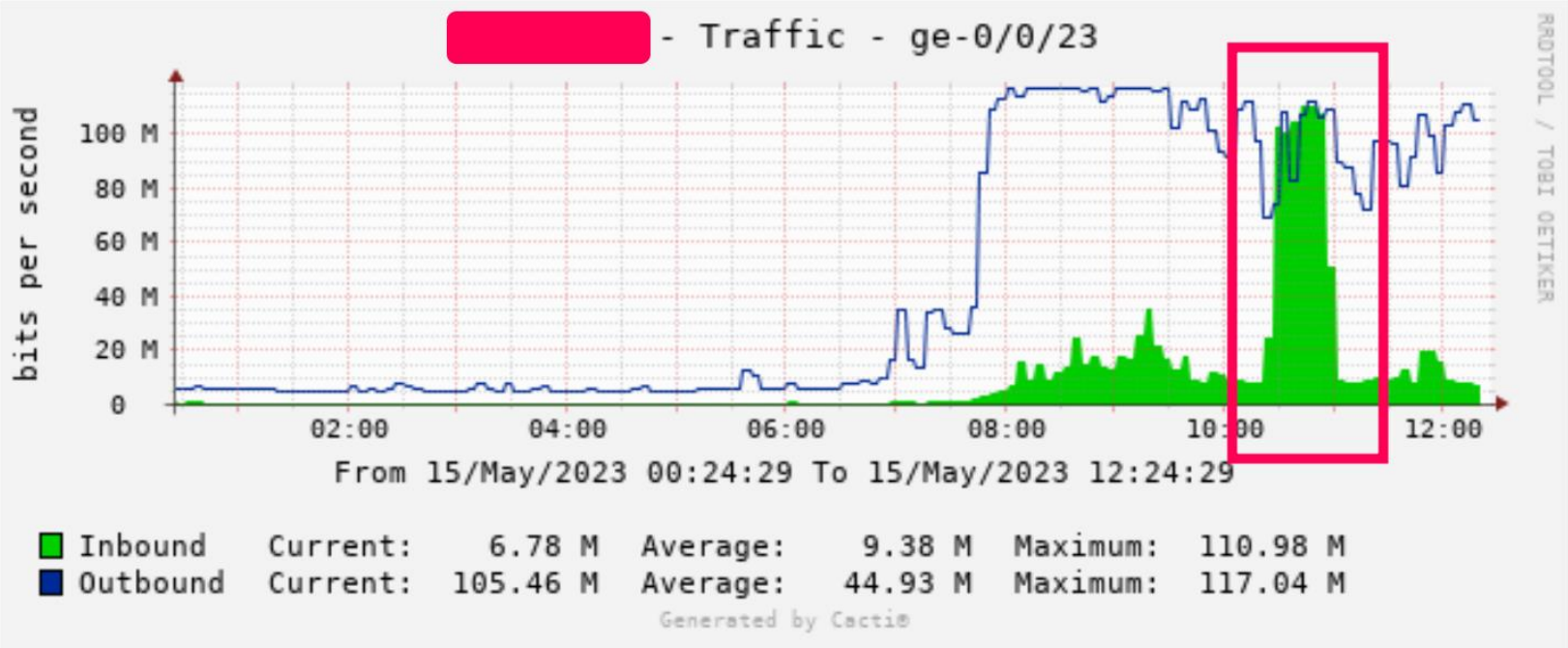
- Determine trends
- Utilisation vs performance

Bandwidth Utilisation - cacti



Compromised server

Bandwidth Utilisation - cacti



When do you do backups?

Testing Inter-RENU Traffic

- https://pfs-raxio.renu.ac.ug/speedtest/
- https://pfs-mujhu.renu.ac.ug/speedtest/

Summary

- Know your network
- Monitor network/user performance
- User sensitisation
- Network / wireless authentication
- Wireless coverage
- Password policies
- Budgetary consideration

Q & A

THE END

Thank you for your time