Scalable Network Design and NOC Webinar:
Proactive Network Monitoring

By

Sherinah Nakazibwe
snakazibwe@renu.ac.ug

4th October 2023

Outline

- Introduction to Monitoring
- Why Proactive Monitoring
- Key Components
- Tools and Technologies
- Challenges and Considerations
- Implementation Steps

Introduction

Network monitoring is the practice of continuously observing and analyzing the performance, health, and security of a computer network to ensure its optimal operation.

Importance of network monitoring;

- Networks is a vital infrastructure
- Reliability and availability
- Complexity of modern networks
- Security concerns

Proactive Monitoring Defined

- Proactive

Involves actively tracking network health and performance in real-time or near real-time to identify and address issues before they impact users or operations.

- Reactive

Network administrators only become aware of problems when users report them or when they have already impacted operations.

Proactive monitoring relies on;

- Continuous Assessment
- Preventive Action

Why Proactive Monitoring

- Cost of network downtime
  - Significant financial consequences like revenue loss.
  - Productivity impact through disruption of employee operations
  - Reputation and customer/user trust due to failure to deliver reliable and always available services

- Benefits of proactive monitoring
  - Improved reliability through minimizing downtime and fault isolation
  - Enhanced performance by optimizing resource usage and and enabling capacity planning
  - Cost savings through preventing costly failures and allowing for lower operational costs.

Key Components

- Network health and performance

Performance metrics

- Latency which measures the delay in data transmission.
- Packet loss indicates the percentage of packets dropped during transmission
- Jitter measures variations in latency

Bandwidth Utilization

- Monitoring bandwidth usage helps ensure that network resources are efficiently allocated.

Device Uptime

- Downtime can indicate hardware or software issues that need attention.

Key Components

- Events and alerts management

Real-time monitoring

- Proactive monitoring systems continuously analyze network events and conditions in real-time

Alerting

- When predefined thresholds are exceeded or anomalies detected, alerts are generated.

Root cause analysis

- Proactive monitoring tools often provide insights into the root causes of issues, helping administrators pinpoint the source of problems.

Key Components

- Configuration monitoring

Configuration Changes

- Monitoring network device configurations helps detect unauthorized or unintended changes.

Compliance Monitoring

- Ensuring that configurations adhere to security and compliance policies is crucial for network security.

Change Control

- Proactive monitoring can provide documentation of configuration changes

Key Components

- End user experience monitoring

Application Performance

- Slow or malfunctioning applications can be identified and addressed.

End-User Monitoring

- Monitoring end-user devices, such as laptops and smartphones, helps ensure they have the necessary network connectivity and performance.

Tools and Technologies

- Simple Network Management Protocol
  - SNMP is a widely used protocol for collecting and organizing information about network devices
  - It is essential for monitoring device uptime, bandwidth utilization, and identifying issues such as high CPU or memory usage.

- Flow and Packet Analysis
  - Flow analysis tools examine network traffic patterns provide insights into the types of traffic on the network.
  - Packet analysis involves capturing and inspecting individual data packets to diagnose network issues

Tools and Technologies

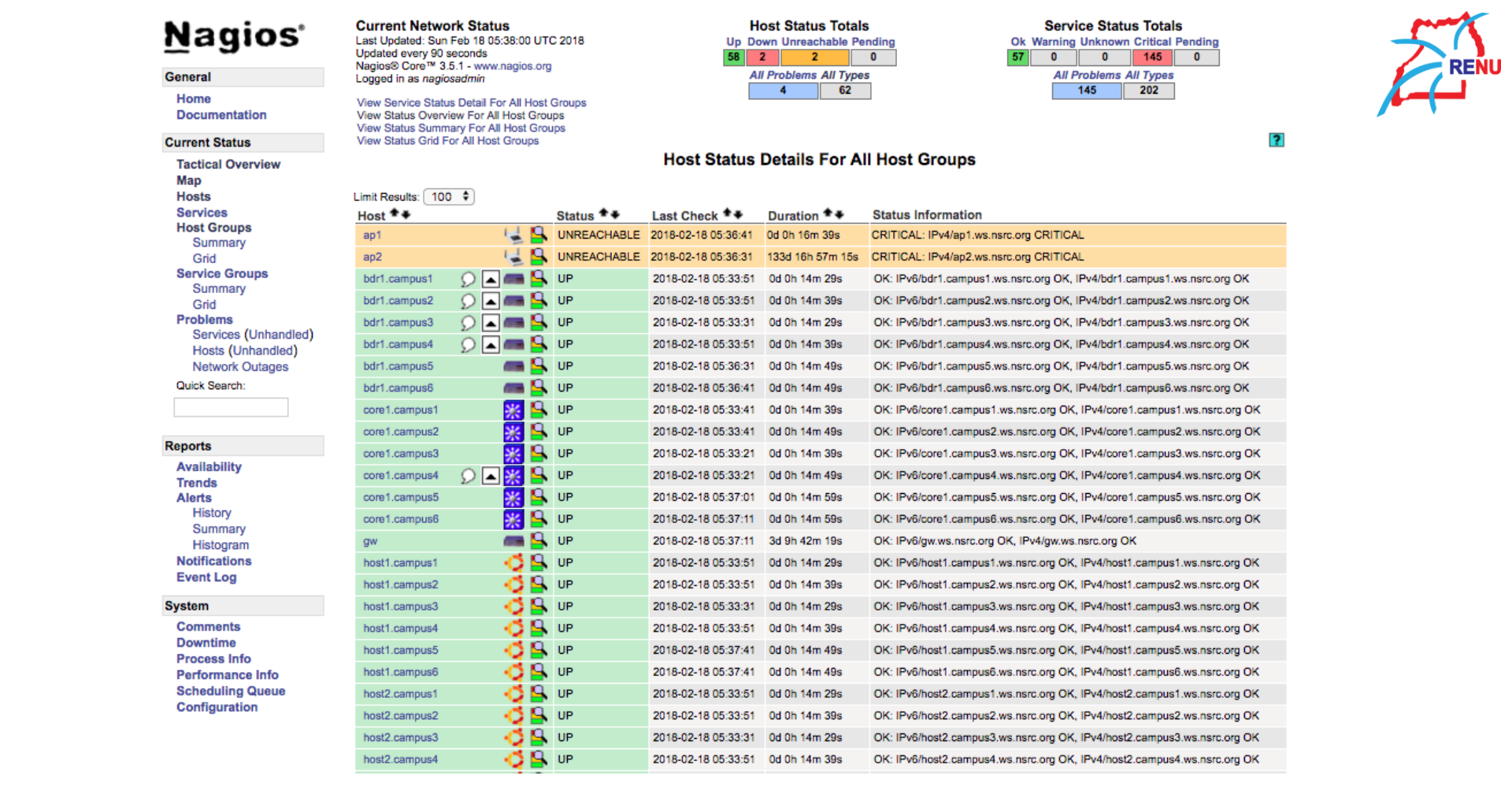
- Anomaly detection
  - Tools use historical data to establish a baseline of normal network behavior and deviations from this baseline are flagged as anomalies.
  - Anomaly detection is essential for early threat detection, as well as for spotting performance issues that may not trigger traditional threshold-based alerts.

- Machine Learning and AI
  - ML algorithms can analyze vast amounts of data to identify patterns and trends.
  - Possibility of automating responses to certain network events, reducing the need for manual intervention.

Nagios

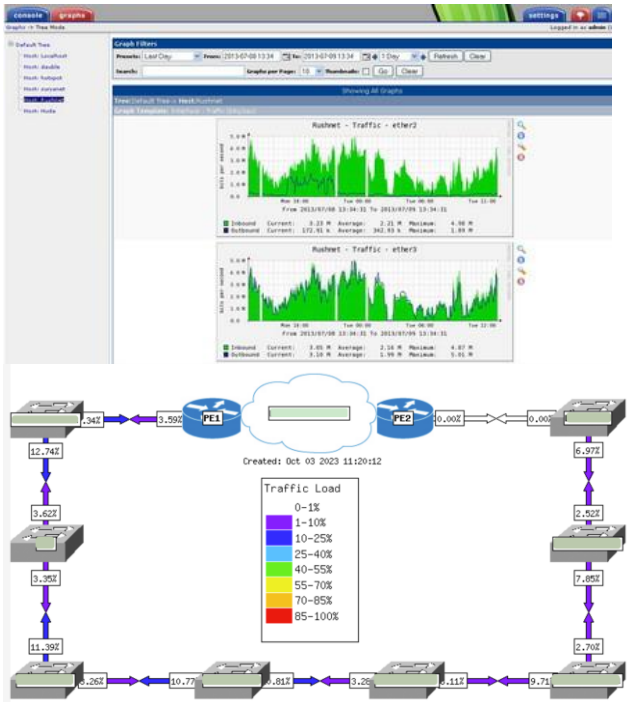
- Designed to run on Linux – open source
- Measure availability and performance of hosts and services
- Runs periodic checks on critical parameters of application, network and server resources.
- Can send out alerts if critical levels are reached based on thresholds
- Possible responses are: ok, warning, critical and unknown

https://www.nagios.org/downloads/


Nagios
General
Home
Documentation
Current Status
Tactical Overview
Map
Hosts
Services
Host Groups
Summary
Grid
Service Groups
Summary
Grid
Problems
Services (Unhandled)
Hosts (Unhandled)
Network Outages
Quick Search:
Reports
Availability
Trends
Alerts
History
Summary
Histogram
Notifications
Event Log
System
Comments
Downtime
Process Info
Performance Info
Scheduling Queue
Configuration
Current Network Status
Last Updated: Sun Feb 18 05:38:00 UTC 2018
Updated every 90 seconds
Nagios® Core™ 3.5.1 - www.nagios.org
Logged in as nagiosadmin
View Service Status Detail For All Host Groups
View Status Overview For All Host Groups
View Status Summary For All Host Groups
View Status Grid For All Host Groups
Host Status Totals
Up Down Unreachable Pending
58 2 2 0
All Problems All Types
4 62
Service Status Totals
Ok Warning Unknown Critical Pending
57 0 0 145 0
All Problems All Types
145 202
Host Status Details For All Host Groups
Limit Results: 100
Host
Status
Last Check
Duration
Status Information
ap1 UNREACHABLE 2018-02-18 05:36:41 0d 0h 16m 39s CRITICAL: IPv4/ap1.ws.nsrc.org CRITICAL
ap2 UNREACHABLE 2018-02-18 05:36:31 133d 16h 57m 15s CRITICAL: IPv4/ap2.ws.nsrc.org CRITICAL
bdr1.campus1 UP 2018-02-18 05:33:51 0d 0h 14m 29s OK: IPv6/bdr1.campus1.ws.nsrc.org OK, IPv4/bdr1.campus1.ws.nsrc.org OK
bdr1.campus2 UP 2018-02-18 05:33:51 0d 0h 14m 39s OK: IPv6/bdr1.campus2.ws.nsrc.org OK, IPv4/bdr1.campus2.ws.nsrc.org OK
bdr1.campus3 UP 2018-02-18 05:33:31 0d 0h 14m 29s OK: IPv6/bdr1.campus3.ws.nsrc.org OK, IPv4/bdr1.campus3.ws.nsrc.org OK
bdr1.campus4 UP 2018-02-18 05:33:51 0d 0h 14m 39s OK: IPv6/bdr1.campus4.ws.nsrc.org OK, IPv4/bdr1.campus4.ws.nsrc.org OK
bdr1.campus5 UP 2018-02-18 05:36:31 0d 0h 14m 49s OK: IPv6/bdr1.campus5.ws.nsrc.org OK, IPv4/bdr1.campus5.ws.nsrc.org OK
bdr1.campus6 UP 2018-02-18 05:36:41 0d 0h 14m 49s OK: IPv6/bdr1.campus6.ws.nsrc.org OK, IPv4/bdr1.campus6.ws.nsrc.org OK
core1.campus1 UP 2018-02-18 05:33:41 0d 0h 14m 39s OK: IPv6/core1.campus1.ws.nsrc.org OK, IPv4/core1.campus1.ws.nsrc.org OK
core1.campus2 UP 2018-02-18 05:33:41 0d 0h 14m 49s OK: IPv6/core1.campus2.ws.nsrc.org OK, IPv4/core1.campus2.ws.nsrc.org OK
core1.campus3 UP 2018-02-18 05:33:21 0d 0h 14m 39s OK: IPv6/core1.campus3.ws.nsrc.org OK, IPv4/core1.campus3.ws.nsrc.org OK
core1.campus4 UP 2018-02-18 05:33:21 0d 0h 14m 49s OK: IPv6/core1.campus4.ws.nsrc.org OK, IPv4/core1.campus4.ws.nsrc.org OK
core1.campus5 UP 2018-02-18 05:37:01 0d 0h 14m 59s OK: IPv6/core1.campus5.ws.nsrc.org OK, IPv4/core1.campus5.ws.nsrc.org OK
core1.campus6 UP 2018-02-18 05:37:11 0d 0h 14m 59s OK: IPv6/core1.campus6.ws.nsrc.org OK, IPv4/core1.campus6.ws.nsrc.org OK
gw UP 2018-02-18 05:37:11 3d 9h 42m 19s OK: IPv6/gw.ws.nsrc.org OK, IPv4/gw.ws.nsrc.org OK
host1.campus1 UP 2018-02-18 05:33:51 0d 0h 14m 29s OK: IPv6/host1.campus1.ws.nsrc.org OK, IPv4/host1.campus1.ws.nsrc.org OK
host1.campus2 UP 2018-02-18 05:33:51 0d 0h 14m 39s OK: IPv6/host1.campus2.ws.nsrc.org OK, IPv4/host1.campus2.ws.nsrc.org OK
host1.campus3 UP 2018-02-18 05:33:31 0d 0h 14m 29s OK: IPv6/host1.campus3.ws.nsrc.org OK, IPv4/host1.campus3.ws.nsrc.org OK
host1.campus4 UP 2018-02-18 05:33:51 0d 0h 14m 39s OK: IPv6/host1.campus4.ws.nsrc.org OK, IPv4/host1.campus4.ws.nsrc.org OK
host1.campus5 UP 2018-02-18 05:37:41 0d 0h 14m 49s OK: IPv6/host1.campus5.ws.nsrc.org OK, IPv4/host1.campus5.ws.nsrc.org OK
host1.campus6 UP 2018-02-18 05:37:41 0d 0h 14m 49s OK: IPv6/host1.campus6.ws.nsrc.org OK, IPv4/host1.campus6.ws.nsrc.org OK
host2.campus1 UP 2018-02-18 05:33:51 0d 0h 14m 29s OK: IPv6/host2.campus1.ws.nsrc.org OK, IPv4/host2.campus1.ws.nsrc.org OK
host2.campus2 UP 2018-02-18 05:33:51 0d 0h 14m 39s OK: IPv6/host2.campus2.ws.nsrc.org OK, IPv4/host2.campus2.ws.nsrc.org OK
host2.campus3 UP 2018-02-18 05:33:31 0d 0h 14m 29s OK: IPv6/host2.campus3.ws.nsrc.org OK, IPv4/host2.campus3.ws.nsrc.org OK
host2.campus4 UP 2018-02-18 05:33:51 0d 0h 14m 39s OK: IPv6/host2.campus4.ws.nsrc.org OK, IPv4/host2.campus4.ws.nsrc.org OK

Cacti

- Measures performance and usage of devices.
- Monitor, store and present network and system/server statistics.
- Uses SNMP to collect information on devices
- Add devices and create graphs
- Weather map functionality

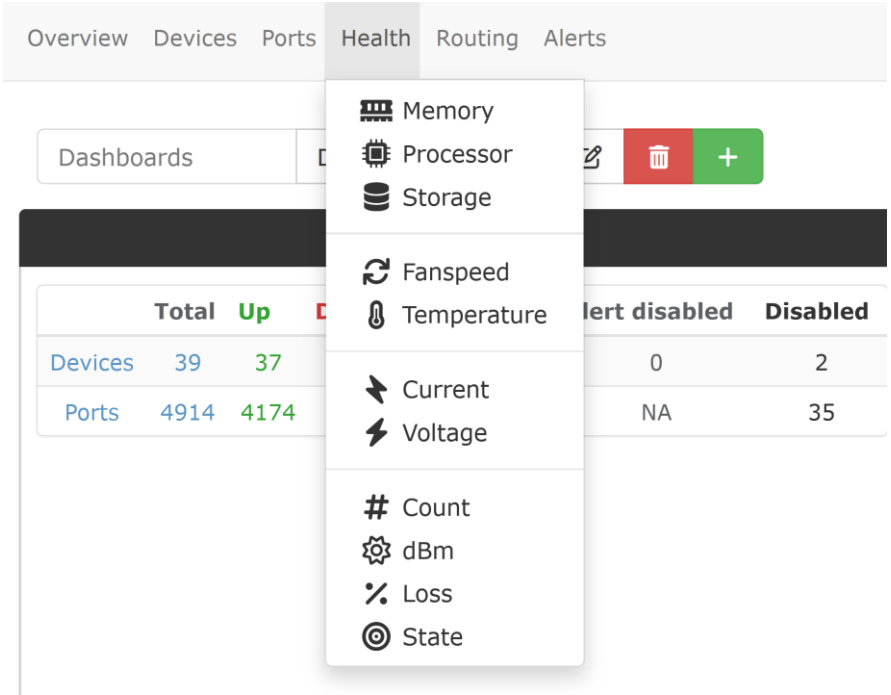


https://www.cacti.net/info/downloads

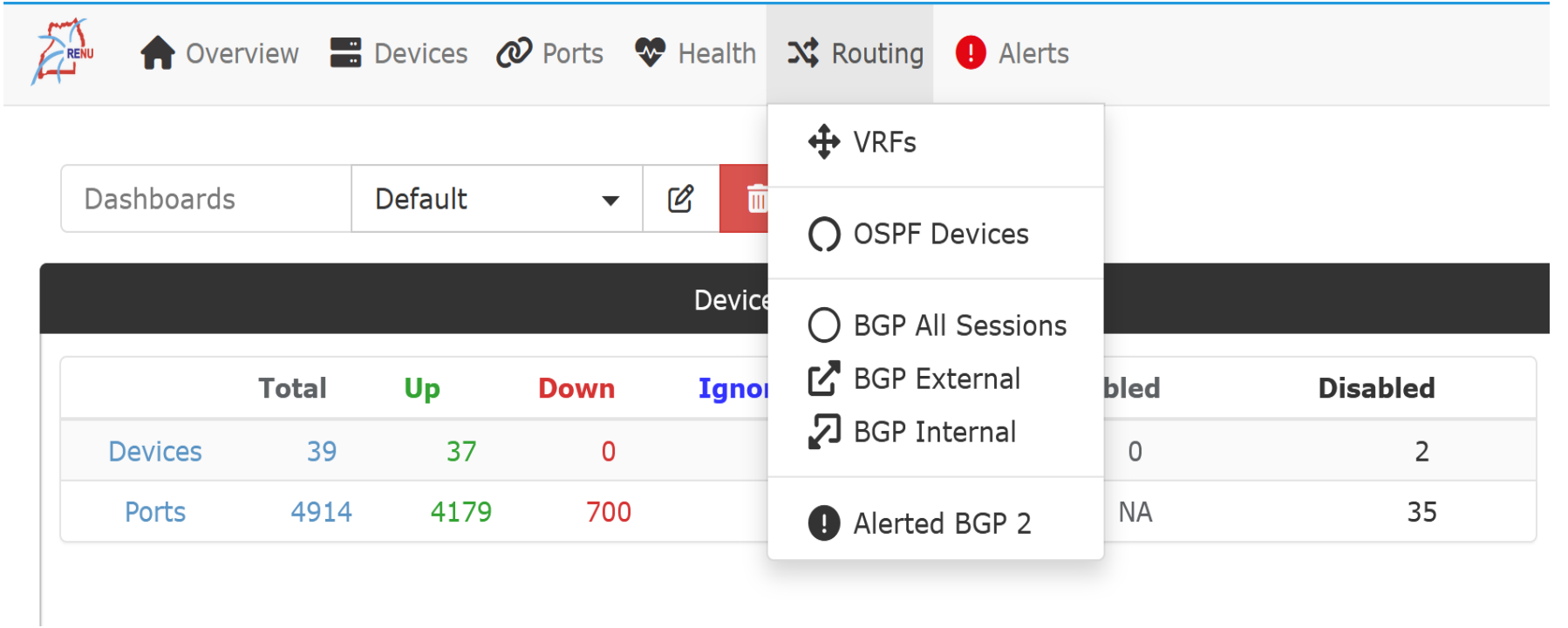
LibreNMS

- Auto-discovery tool
- Customizable alerting
- Device health, performance and availability
- Information on the available routing protocols in use and their state.
- By default, it polls devices every 5 minutes

https://www.librenms.org/#downloads



LibreNMS


Overview
Devices
Ports
Health
Routing
Alerts
VRFs
OSPF Devices
BGP All Sessions
BGP External
BGP Internal
Alerted BGP 2
Dashboards
Default
Total
Up
Down
Disabled
Devices
39
37
0
0
2
Ports
4914
4179
700
NA
35

Common Network utilities

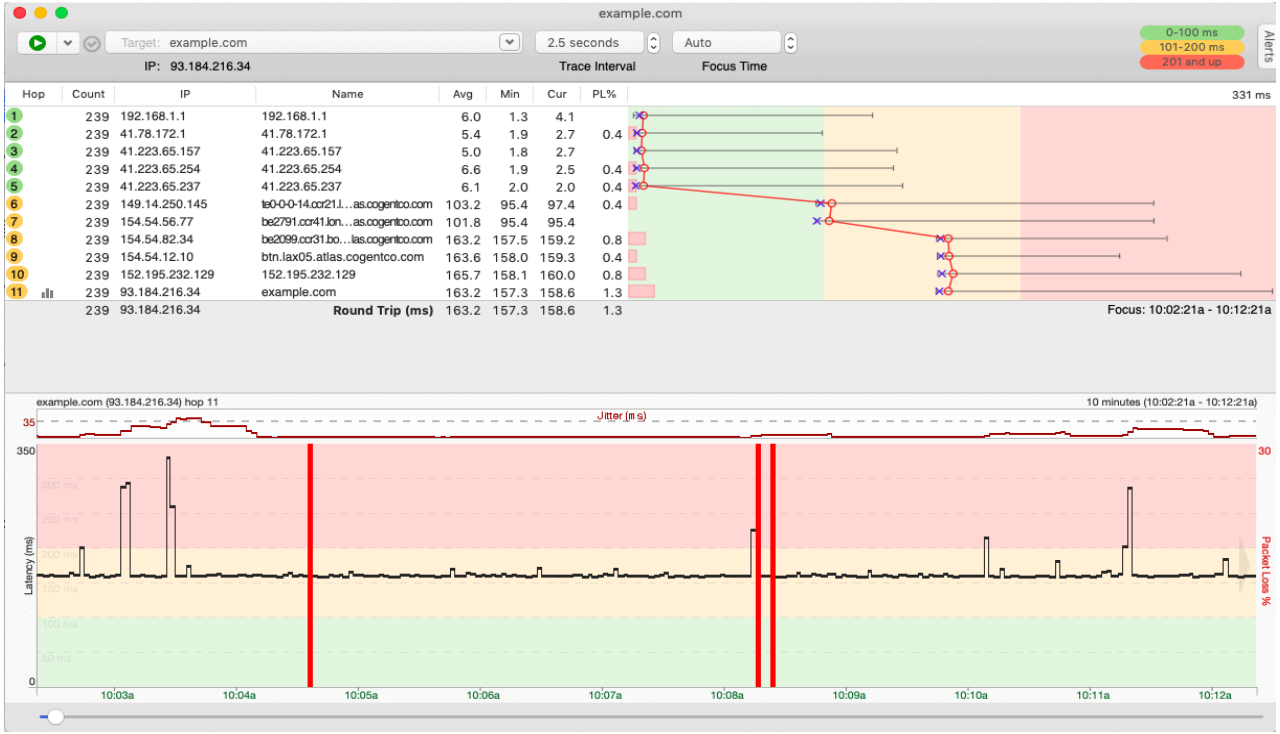
- Ping
- Traceroute
- PathPing
- Nmap
- Netstat
- ARP and Ipconfig
- Nslookup
- PingPlotter

PingPlotter

- Graphic network monitoring and troubleshooting.
- Plot latency, packet loss, and jitter on an infinite timeline.
- Discovers bottlenecks on your LAN as well as issues beyond.
- Analyzes and presents detailed graphs and prove whether issues are caused by local networks, ISPs, or something else.

https://www.pingplotter.com/download/

PingPlotter

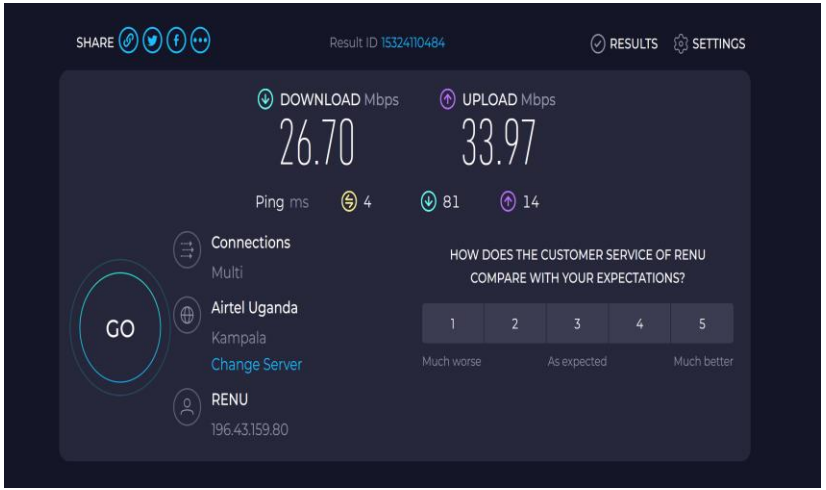


Speed Test

- Understanding how a speed test works and interpreting results

Available servers for testing

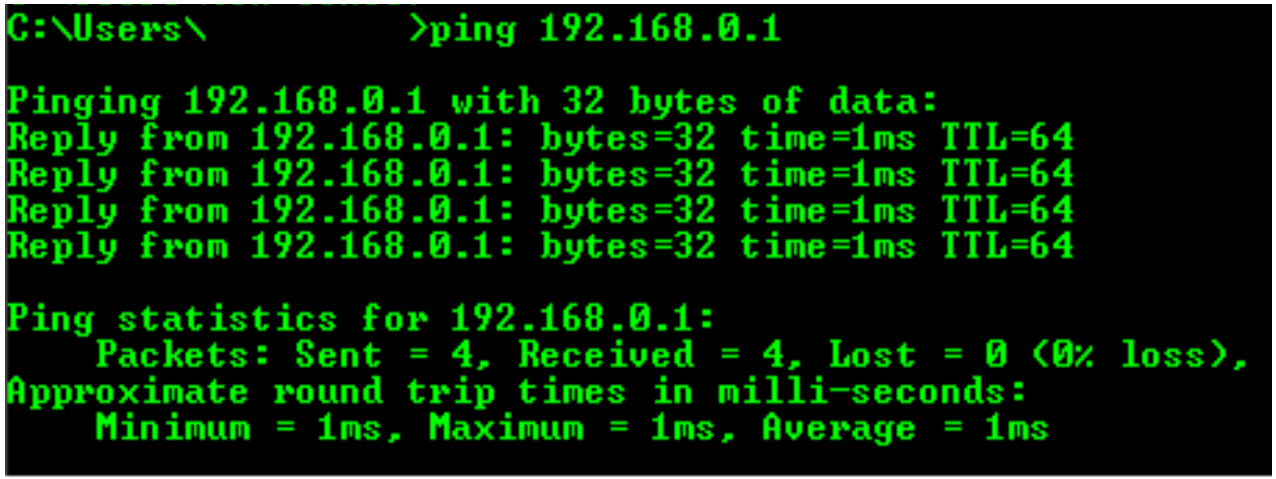
- speedtest.net
- fast.com
- speed.cloudflare.com
- pfs-raxio.renu.ac.ug/speedtest/
- pfs-mujhu.renu.ac.ug/speedtest/



- Is my Internet speed okay?

Ping

- Ping (Packet InterNet Groper) uses ICMP
  - Determines whether a device is reachable from another device
  - Identify latency and packet loss between the two devices.
  - Not getting a response does not necessarily mean that there is a fault



Traceroute

- Traceroute is diagnostic tool that displays the path and transit delays of a packet from your machine to a chosen IP address or DNS name.
- Displays information breakdown on each point
- More useful where a connection has broken down.

```
Tracing route to www.google.com [173.194.65.104]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  192.168.0.1
  2    16 ms    15 ms    16 ms  10.lnsgw05.thd.as8586.net [213.246.145.246]
  3    16 ms    18 ms    18 ms  PoCh2.lnsbr01.thd.uk.as8586.net [213.246.177.221
]
  4    15 ms    18 ms    16 ms  xe1-5.core02.thd.uk.as8586.net [212.58.37.119]
  5    17 ms    17 ms    18 ms  ge-0-0-?-scr010.thn.as13285.net [78.144.3.22]
  6    17 ms    16 ms    16 ms  host-78-144-10-101.as13285.net [78.144.10.101]
  7    16 ms    17 ms    16 ms  72.14.242.127
  8    17 ms    40 ms    18 ms  209.85.246.246
  9    17 ms    19 ms    17 ms  209.85.245.2
 10    34 ms    32 ms    24 ms  216.239.48.82
 11    26 ms    51 ms    31 ms  74.125.37.119
 12    27 ms    28 ms    25 ms  216.239.49.30
 13     *        *        *     Request timed out.
 14    26 ms    25 ms    24 ms  ee-in-f104.1e100.net [173.194.65.104]

Trace complete.
```

PathPing

- A route tracing tool that combines elements and features of the traceroute and ping tools.
- It is essentially a traceroute with an extra statistics breakdown for each hop.

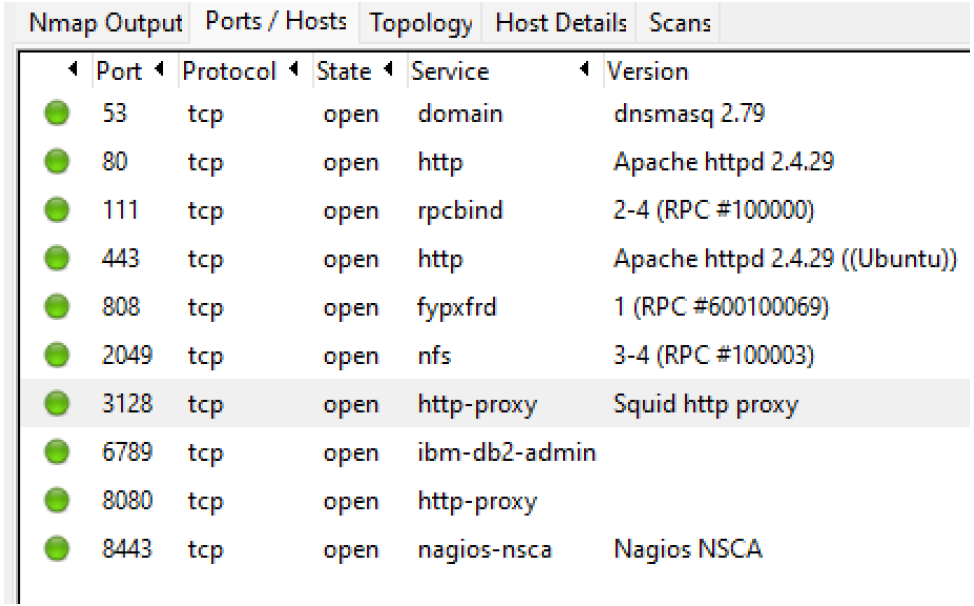
How optimal is my path?

```
Tracing route to google.com [172.217.170.206]
over a maximum of 30 hops:
  0  RENU-SHERINAH.renu.ac.ug [196.43.159.80]
  1  196.43.159.1
  2  196.43.189.232
  3  raxio.kla1.p1-raxio.kla1.pe.net.renu.ac.ug [196.43.190.225]
  4  raxio.kla1.p2-raxio.kla1.p1.net.renu.ac.ug [196.43.190.246]
  5  google.v4.rxo.uixp.co.ug [196.223.25.128]
  6  172.253.53.49
  7  216.239.63.239
  8  mba01s10-in-f14.1e100.net [172.217.170.206]

Computing statistics for 200 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           RENU-SHERINAH.renu.ac.ug [196.43.159.80]
                                   2/ 100 =  2%   |
  1    4ms     2/ 100 =  2%     0/ 100 =  0%  196.43.159.1
                                   0/ 100 =  0%   |
  2    6ms     2/ 100 =  2%     0/ 100 =  0%  196.43.189.232
                                   0/ 100 =  0%   |
  3    8ms     2/ 100 =  2%     0/ 100 =  0%  raxio.kla1.p1-raxio.kla1.pe.net.renu.ac.ug [196.43.190.225]
                                   0/ 100 =  0%   |
  4    7ms     3/ 100 =  3%     1/ 100 =  1%  raxio.kla1.p2-raxio.kla1.p1.net.renu.ac.ug [196.43.190.246]
                                   0/ 100 =  0%   |
  5   23ms     3/ 100 =  3%     1/ 100 =  1%  google.v4.rxo.uixp.co.ug [196.223.25.128]
                                   0/ 100 =  0%   |
  6   21ms     2/ 100 =  2%     0/ 100 =  0%  172.253.53.49
                                   1/ 100 =  1%   |
  7  ---     100/ 100 =100%    97/ 100 = 97%  216.239.63.239
                                   0/ 100 =  0%   |
```

Nmap

- Network Mapper, is used for network discovery, networking mapping and networking auditing.
- It is handy for network scans.
- Uses IP packets to determine what hosts, ports, services and IP addresses are available and open on a network, both LAN and WAN.



Port	Protocol	State	Service	Version
53	tcp	open	domain	dnsmasq 2.79
80	tcp	open	http	Apache httpd 2.4.29
111	tcp	open	rpcbind	2-4 (RPC #100000)
443	tcp	open	http	Apache httpd 2.4.29 ((Ubuntu))
808	tcp	open	fypxfrd	1 (RPC #600100069)
2049	tcp	open	nfs	3-4 (RPC #100003)
3128	tcp	open	http-proxy	Squid http proxy
6789	tcp	open	ibm-db2-admin	
8080	tcp	open	http-proxy	
8443	tcp	open	nagios-nsca	Nagios NSCA

https://nmap.org/download.html

Netsat

- Most handy to check whether a connection to a certain device or website is established or not.
- Displays very detailed information and statistics about the device you are using and how it is connected to the network.
- Each line of the output represents a request from your machine to a device beyond your machine
- Protocol of the entry, local address and port, destination and state of each request.

Netsat

```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:4243         49156                  ESTABLISHED
  TCP    127.0.0.1:49156        4243                   ESTABLISHED
  TCP    127.0.0.1:49161        49162                  ESTABLISHED
  TCP    127.0.0.1:49162        49161                  ESTABLISHED
  TCP    127.0.0.1:49163        49164                  ESTABLISHED
  TCP    127.0.0.1:49164        49163                  ESTABLISHED
  TCP    127.0.0.1:49165        49166                  ESTABLISHED
  TCP    127.0.0.1:49166        49165                  ESTABLISHED
  TCP    127.0.0.1:49167        49168                  ESTABLISHED
  TCP    127.0.0.1:49168        49167                  ESTABLISHED
  TCP    127.0.0.1:49182        49183                  ESTABLISHED
  TCP    127.0.0.1:49183        49182                  ESTABLISHED
  TCP    127.0.0.1:49184        49185                  ESTABLISHED
  TCP    127.0.0.1:49185        49184                  ESTABLISHED
  TCP    127.0.0.1:49186        49187                  ESTABLISHED
  TCP    127.0.0.1:49187        49186                  ESTABLISHED
  TCP    127.0.0.1:49188        49189                  ESTABLISHED
  TCP    127.0.0.1:49189        49188                  ESTABLISHED
  TCP    127.0.0.1:49280        49281                  ESTABLISHED
  TCP    127.0.0.1:49281                               ESTABLISHED
  TCP    192.168.0.3:49191      r-062-043-234-077:http  ESTABLISHED
  TCP    192.168.0.3:49314      157.56.53.48:12350     ESTABLISHED
  TCP    192.168.0.3:49316      db3msgr5011211:https   ESTABLISHED
  TCP    192.168.0.3:49327      104.46.43.67:https     ESTABLISHED
  TCP    192.168.0.3:51023      r-149-058-045-005:http  CLOSE_WAIT
  TCP    192.168.0.3:53006      r-253-058-045-005:http  CLOSE_WAIT
  TCP    192.168.0.3:53678      64.4.23.140:40034      ESTABLISHED
  TCP    192.168.0.3:53680      149.5.7.10:https       ESTABLISHED
  TCP    192.168.0.3:53691      code42:4282            ESTABLISHED
  TCP    192.168.0.3:53700      wn-in-f125:5222        ESTABLISHED
  TCP    192.168.0.3:53835      lhr14s24-in-f69:https  ESTABLISHED
  TCP    192.168.0.3:53894      wl-in-f189:https       ESTABLISHED
  TCP    192.168.0.3:53936      aboukir:http           CLOSE_WAIT
  TCP    192.168.0.3:53938      float:http             CLOSE_WAIT
  TCP    192.168.0.3:53945      glbny:http             TIME_WAIT
  TCP    192.168.0.3:53946      glbny:http             TIME_WAIT
  TCP    192.168.0.3:53947      glbny:http             TIME_WAIT
  TCP    192.168.0.3:53948      glbny:http             TIME_WAIT
  TCP    192.168.0.3:53949      glbny:http             TIME_WAIT
  TCP    192.168.0.3:53950      glbny:http             TIME_WAIT
  TCP    192.168.0.3:53951      bay406-m:https         ESTABLISHED
```

ARP and ipconfig

- **ARP** – Map IP addresses to MAC addresses.
  Useful in identifying unknown devices that you think may be accessing your network maliciously.
  arp –a
- ipconfig
  Displays all of the current TCP/IP network settings on your machine.
  /all
  /release
  /renew
  /flushdns

NSlookup

- Nslookup is used for querying the DNS zone files to obtain useful information such as domain names, IP addresses, or specific DNS records.
- Supports reverse DNS lookup.
  - nslookup www.google.com 8.8.8.8
  - nslookup 142.250.4.113

```
C:\Users\nsher>nslookup renu.ac.ug 8.8.8.8
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    renu.ac.ug
Address:  196.43.185.101
```

Best Practices

- Defining Monitoring Goals

Clearly stating the priorities in line with what you want to achieve.

- Selecting the right metrics

The metrics should be relevant to avoid data overload

- Setting thresholds and alerts

Clearly define thresholds and customize alerts to avoid alert fatigue.

- Establishing baselines

Analysing data and coming up with Reference point for identifying anomalies.

- Automation of remediation

Challenges

- Scalability

Challenge to scale monitoring solutions to accommodate the additional devices, traffic, and data sources.

- False positives and alert fatigue

Generation of large volumes of data yet storing and managing this data can be resource-intensive.

- Integrating with existing tools.

Some tools are vendor specific like ‘The Dude’for MikroTik devices.

Considerations

- Scalability

Consider using scalable architecture and prioritization

- Data volume and retention

Data retention policies and data compression and storage.

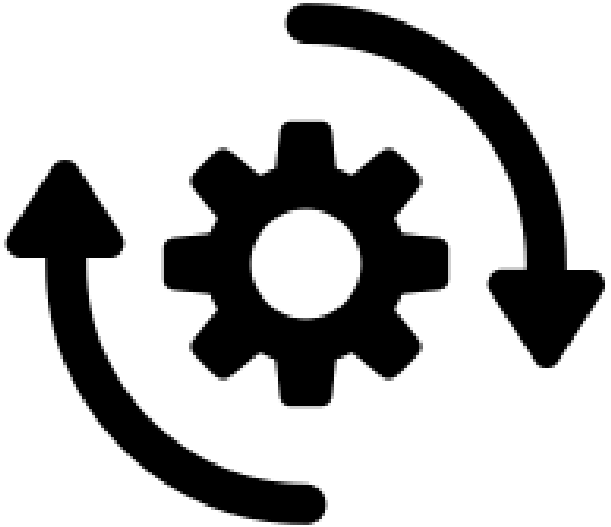
- False positives and alert fatigue

Threshold tuning.

Implementation Steps

- Assessing current monitoring capabilities
  - Current State Assessment
  - Data Collection.
  - Documentation.

- Selecting Proactive Monitoring Tools
  - Vendor Evaluation
  - Compatibility
  - Customization



Implementation Steps

- Designing Monitoring Strategies
  - Goal Alignment
  - Metric Selection
  - Thresholds and Alerts
  - Incident Response Plans