UNIVERSITY OF TECHNOLOGY SYDNEY

UTS: ENGINEERING & INFORMATION TECHNOLOGY

NETWORK MANAGEMENT	**NAME OF STUDENT(s) (PRINT CLEARLY)** VISHAL SINGH BISHT	**STUDENT ID(s).** **12865693**

STUDENT EMAIL 12865693@student.uts.edu.au	**STUDENT CONTACT NUMBER** **0449285049**

NAME OF TUTOR **DOAN HOANG (SUBJECT COORDINATOR)** **SARAH FARAHMANDIAN**	**TUTORIAL GROUP** INDIVIDUAL	**DUE DATE** **26 May 2020**

ASSESSMENT ITEM NUMBER/ TITLE

NETMAN PROJECT

☑ I confirm that I have read, understood and followed the guidelines for assignment submission and presentation on page 2 of this cover sheet.

☑ I confirm that I have read, understood and followed the advice in my Subject Outline about assessment requirements.

☑ I understand that if this assignment is submitted after the due date it may incur a penalty for lateness unless I have previously had an extension of time approved and have attached the written confirmation of this extension.

Declaration of Originality: The work contained in this assignment, other than that specifically attributed to another source, is that of the author(s) and has not been previously submitted for assessment. I understand that, should this declaration be found to be false, disciplinary action could be taken and penalties imposed in accordance with University policy and rules. In the statement below, I have indicated the extent to which I have collaborated with others, whom I have named.

Statement of Collaboration:

Signature of Student(s) ____ VISHAL.S.B Date**_________26/05/2020______________**

∀- ---

PART-I:

EXECUTIVE SUMMARY:

Managing a network is a challenging task for a network manager. It is imperative for a network manager to monitor all aspects of network and resolve or come up with new methodologies to maintain the availability of network at all times. The following report is based on the topology as shown in figure1. The four important aspects of network management namely, configuration management, performance management, fault management and security management has been covered in the report.

The proposed plan:

A phased approach has been used for network planning. At first, the network devices are configured in a professional manner. In network management, configuration management is used for discovering the network topology, network mapping and complete set up of configuration parameters of management agents and management systems. In the proposed work, at every step of device configuration, commits are compared with the previous commits and comments are used wherever necessary. After a step by step approach for device configuration, the network topology is compared with the required topology as shown in figure1. Traceroute and Zenmap is used to verify the topology.

Network analyser tool **ntop** has been used for performance and fault management technique. The ntop tool is an opensource and highly flexible tool. When it comes to speed and space, the ntop tool is comparatively faster on the system than the other tools such as OpenNMS, Nagios and Solarwinds, as these tools are quite heavy on system since they have additional plugins. As a network manager, the tool selection for monitoring is critical. If the tool lags while monitoring the network, then the network manager might get a delay in receiving the status and information of the devices in the network. For the current topology, ntop tool fulfils the requirements and give efficient and accurate results. The ntop tool monitors network elements and file transfer protocol(ftp) using Filezilla has been executed during the active monitoring of the network. Important aspects such as polling, throughput and RTT has been covered while monitoring the network. Further, interfaces of one of the routers has been disabled during the active monitoring process. An alarm has been observed while monitoring the network and the cause and location of the fault has been displayed on the monitoring tool. After resolving the issue, it is imperative for any manager to form a report on the faults. Faults are not always due

to accidental, sometimes they can be deliberate. The attacks on the networks in the current scenario of emerging technologies are increasing day by day. A network manager is expected to secure the network and comply with CIA (Confidentiality, Integrity and Availability) triad. The access to the devices has been divided into two levels: admin level and operator level. An individual with the rights to change any configuration in the network is provided admin level access and an individual who is not concerned with the implementing any configuration settings or changing parameters is provided with operator level access. Telnet is vulnerable to man in the middle attacks. SSH service more secure as compared to Telnet, as it uses encryption and also avoids any possibility of eavesdropping.

Here, as a network manager it is highly recommended to communicate between all network elements using **ssh**. Although, the plaintext passwords are encrypted after the passwords are saved, it is better to use strong password encryption techniques such as AES and RSA. A brief procedure has been illustrated for setting up public key encryption for network devices. Router1, being the first device to connect with the client machine has been set up with firewall rules to avoid any unwanted intrusion. Finally, a network security scanner, Nessus is used to view the vulnerabilities in the network and provide detailed information of those vulnerabilities and possible attacks. The proposed network plan is efficient, secure and reliable. Detailed methodology of the network plan is provided part II of this report.

Key take-aways:

The four important aspects of network management were successfully covered with in detail explanation. The proposed work provided an in-depth knowledge of important aspects to observe and consider while working in a role as network manager. The monitoring tool selection was one of the challenges, as running heavy tools on virtual machines can be troublesome. The ntop tool successfully worked for performance and fault management. It is important to research and spend considerable time on tool selection and strategize the network plan as it is not a task which can be done short period of time.

PART-II:

SKILL-BASED COMPONENT:

Network Topology

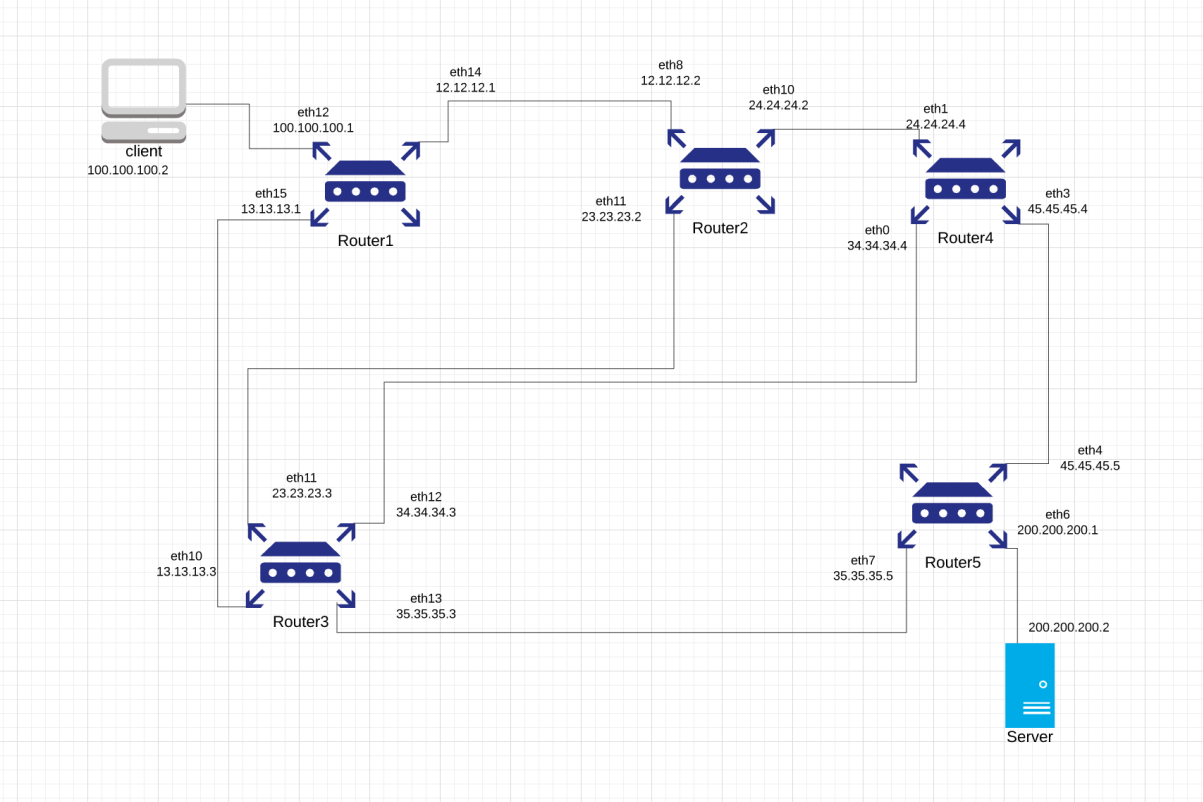


Figure 1.

1. CONFIGURATION MANAGEMENT:

As a network manager, when given a topology to configure, it is his/her responsibility to determine whether the network components are configured in accordance to the requirements specified by the company or not.

A detailed explanation of **Router1** configuration with screenshots has been provided below.

Router1 Configuration:

There are two modes present in VyOs router:

1. **Operational mode-** User can view system information such as routing table and firewalls information etc.
2. **Configuration mode-** User can change system configuration.

The **~$** depicts that the user is in operational mode. To enter the configuration mode, the user needs to input following command:

- **config**

The screenshot below shows that the user has entered the configuration mode.

```
vyos@vyos:~$ config
[edit]
vyos@vyos#
```

Further, by using **show** command it can be seen that the ethernet ports **eth12, eth13, eth14, eth15** are currently not configured.

```
interfaces {
    ethernet eth12 {
        hw-id 00:0c:29:c5:35:99
    }
    ethernet eth13 {
        hw-id 00:0c:29:c5:35:85
    }
    ethernet eth14 {
        hw-id 00:0c:29:c5:35:8f
    }
    ethernet eth15 {
        hw-id 00:0c:29:c5:35:a3
    }
    loopback lo {
    }
}
protocols {
    ospf {
        area 0 {
            network 100.100.100.0/24
            network 12.12.12.0/24
            network 13.13.13.0/24
        }
    }
}
```

The ethernet ports are configured using the following command:

- **set interface ethernet ethx (x=8,9,10,11) address <IP/Port>**

```
 interfaces {
     ethernet eth12 {
+        address 100.100.100.1/24
         hw-id 00:0c:29:c5:35:99
     }
     ethernet eth13 {
+        address dhcp
         hw-id 00:0c:29:c5:35:85
     }
     ethernet eth14 {
+        address 12.12.12.1/24
         hw-id 00:0c:29:c5:35:8f
     }
     ethernet eth15 {
+        address 13.13.13.1/24
         hw-id 00:0c:29:c5:35:a3
     }
     loopback lo {
     }
 }
 protocols {
     ospf {
         area 0 {
             network 100.100.100.0/24
```

Once all the ethernet ports are set with required IP address following commands are executed to finalize the configuration for router.

- **commit**
- **save**

```
vyos@vyos# commit
[ interfaces ethernet eth13 address dhcp ]
Starting DHCP client on eth13 ...

[edit]
vyos@vyos# save
Saving configuration to '/config/config.boot'...
Done
[edit]
```

To make it easier to understand and remember the settings, a comment is added after every final commit.

- **comment interfaces "Router1 interfaces configured"**

```
+/* Router1 interfaces configured */
 interfaces {
```

To view all the interfaces and their status:

- **run show interfaces**

```
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                     S/L  Description
---------        ----------                     ---  -----------
eth12            100.100.100.1/24               u/u
eth13            172.16.7.153/24                u/u
eth14            12.12.12.1/24                  u/u
eth15            13.13.13.1/24                  u/u
lo               127.0.0.1/8                    u/u
                 ::1/128
```

In the screenshot above it can be seen that the State/Link of interfaces are **-u** up.

To view all the system commits:

- **show system commit**

```
vyos@vyos:~$ show system commit
0   2020-05-23 03:35:59 by vyos via cli
1   2020-05-23 03:15:16 by root via boot-config-loader
2   2020-05-21 23:48:39 by root via boot-config-loader
3   2020-04-12 07:03:14 by root via boot-config-loader
4   2017-04-26 01:58:07 by vyos via cli
5   2017-04-26 01:44:25 by root via boot-config-loader
6   2017-04-26 01:07:33 by root via boot-config-loader
7   2017-04-26 01:07:33 by root via init
```

It is a good practice to compare the commits when there is any issue with the particular network component or in the topology. Also, if there are any malicious configuration changes, compare command comes in handy for enumeration. An illustration of commit comparison is shown below.

- **compare [tab]**

```
vyos@vyos# compare
Possible completions:
  <Enter>       Compare working & active configurations
  saved         Compare working & saved configurations
  <N>           Compare working with revision N
  <N> <M>       Compare revision N with M

  Revisions:
    0   2020-05-19 11:03:33 vyos by cli
    1   2020-05-19 06:58:32 root by boot-config-loader
    2   2020-04-12 07:03:14 root by boot-config-loader
    3   2017-04-26 01:58:07 vyos by cli
    4   2017-04-26 01:44:25 root by boot-config-loader
    5   2017-04-26 01:07:33 root by boot-config-loader
    6   2017-04-26 01:07:33 root by init
```

```
vyos@vyos# compare 0 1
[edit interfaces ethernet eth8]
+address 100.100.100.1/24
[edit interfaces ethernet eth9]
+address dhcp
[edit interfaces ethernet eth10]
+address 12.12.12.1/24
[edit interfaces ethernet eth11]
+address 13.13.13.1/24
[edit]
```

The output shows that how configuration 0 is when compared to configuration 1. The + sign depicts the additional parts configuration 0 has when compared to configuration 1. Similarly, when compared with configuration 0 and 2, there is a – sign, which indicates the lacking parts in configuration 2 when compared to 0.

```
[edit interfaces]
-ethernet eth4 {
-    duplex auto
-    hw-id 00:0c:29:fb:4c:29
-    smp_affinity auto
-    speed auto
-}
-ethernet eth5 {
-    duplex auto
-    hw-id 00:0c:29:fb:4c:33
-    smp_affinity auto
-    speed auto
-}
-ethernet eth6 {
-    duplex auto
-    hw-id 00:0c:29:fb:4c:1f
-    smp_affinity auto
-    speed auto
-}
-ethernet eth7 {
-    duplex auto
-    hw-id 00:0c:29:fb:4c:15
-    smp_affinity auto
-    speed auto
```

Client Configuration:

To gain access to routers, client gateway is required to be configured. The Client IP address from interface **ens33** is removed and configured with **100.100.100.2.**

```
netman@netman-virtual-machine:~$ sudo ip addr flush ens33
[sudo] password for netman:
netman@netman-virtual-machine:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether 00:0c:29:8b:82:44  txqueuelen 1000  (Ethernet)
        RX packets 86590  bytes 107216831 (107.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 35321  bytes 3138675 (3.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=329<UP,LOOPBACK,RUNNING,PROMISC>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 229908  bytes 49945203 (49.9 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 229908  bytes 49945203 (49.9 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
netman@netman-virtual-machine:~$ sudo ifconfig ens33 100.100.100.2 netmask 255.255.255.0
netman@netman-virtual-machine:~$ sudo route add default gw 100.100.100.1 ens33
netman@netman-virtual-machine:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         100.100.100.1   0.0.0.0         UG    0      0        0 ens33
100.100.100.0   0.0.0.0         255.255.255.0   U     0      0        0 ens33
```

Once all the routers are configured, it is important to check the reachability of routers by using **ping** command. Below is the screenshot, where client is pinging **Router5.**

```
netman@netman-virtual-machine:~$ ping 45.45.45.5
PING 45.45.45.5 (45.45.45.5) 56(84) bytes of data.
64 bytes from 45.45.45.5: icmp_seq=1 ttl=62 time=1.71 ms
64 bytes from 45.45.45.5: icmp_seq=2 ttl=62 time=1.46 ms
64 bytes from 45.45.45.5: icmp_seq=3 ttl=62 time=1.40 ms
64 bytes from 45.45.45.5: icmp_seq=4 ttl=62 time=1.53 ms
64 bytes from 45.45.45.5: icmp_seq=5 ttl=62 time=1.09 ms
64 bytes from 45.45.45.5: icmp_seq=6 ttl=62 time=2.11 ms
64 bytes from 45.45.45.5: icmp_seq=7 ttl=62 time=2.22 ms
```

Verification of network:

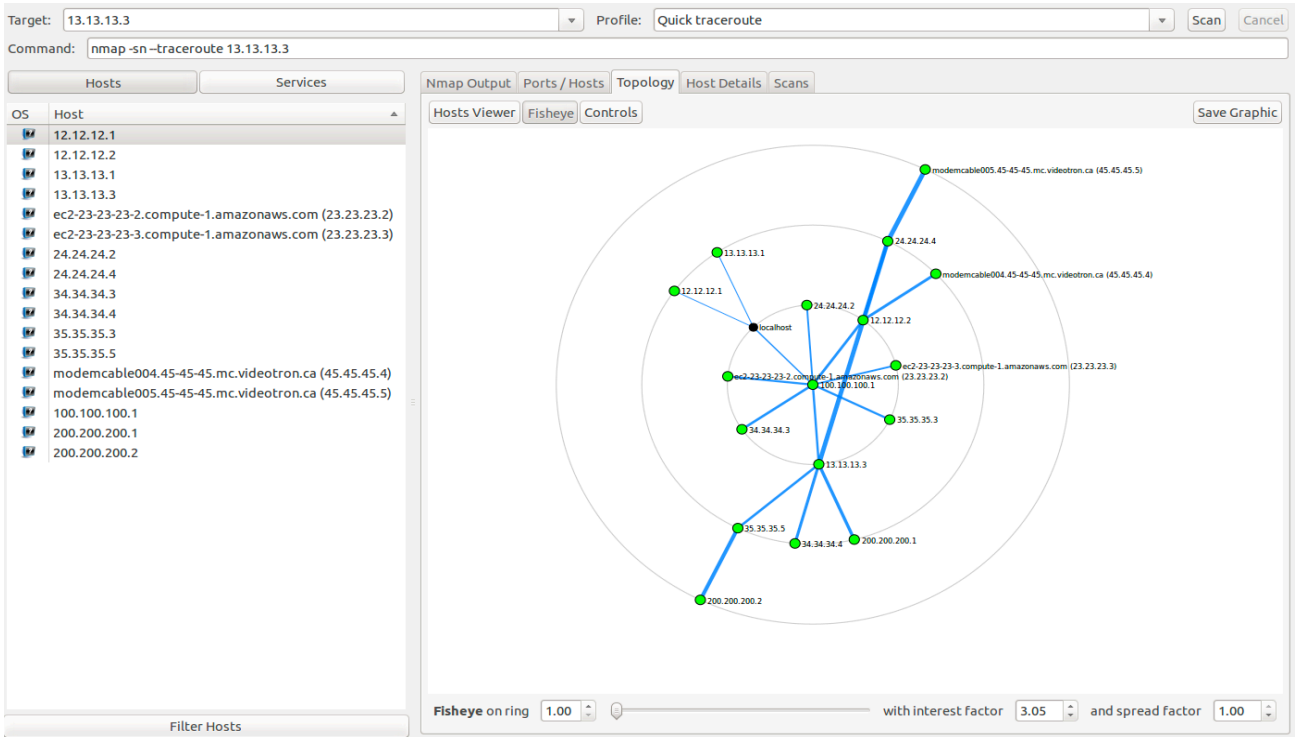
Traceroute:

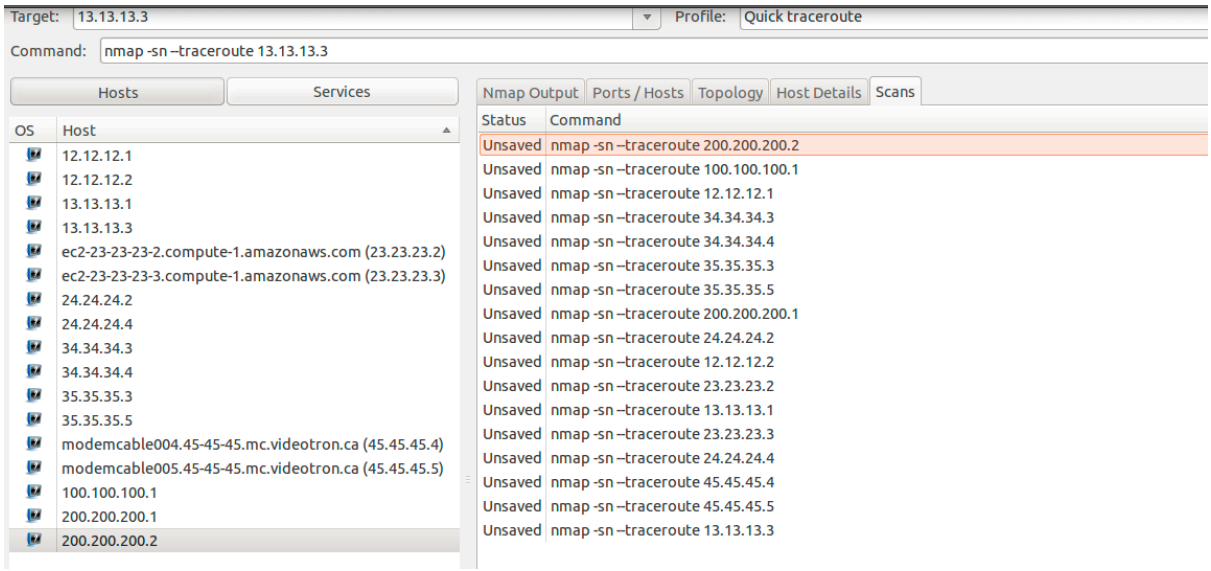
To verify that the network is configured correctly, **traceroute** is used to display the network path used between two hosts.

```
netman@netman-virtual-machine:~$ traceroute 23.23.23.3
traceroute to 23.23.23.3 (23.23.23.3), 64 hops max
  1   100.100.100.1  0.312ms  0.280ms  0.230ms
  2   23.23.23.3  0.526ms  12.12.12.2  0.466ms  23.23.23.3  0.459ms
netman@netman-virtual-machine:~$ traceroute 45.45.45.5
traceroute to 45.45.45.5 (45.45.45.5), 64 hops max
  1   100.100.100.1  1.116ms  0.172ms  0.123ms
  2   12.12.12.2  0.514ms  13.13.13.3  0.561ms  12.12.12.2  0.528ms
  3   34.34.34.4  0.726ms  24.24.24.4  0.628ms  45.45.45.5  0.743ms
netman@netman-virtual-machine:~$ traceroute 200.200.200.2
traceroute to 200.200.200.2 (200.200.200.2), 64 hops max
  1   100.100.100.1  0.202ms  0.098ms  0.177ms
  2   13.13.13.3  0.413ms  0.364ms  0.356ms
  3   35.35.35.5  0.681ms  0.672ms  0.737ms
  4   200.200.200.2  1.559ms  1.045ms  0.715ms
netman@netman-virtual-machine:~$ traceroute 34.34.34.3
traceroute to 34.34.34.3 (34.34.34.3), 64 hops max
  1   100.100.100.1  1.443ms  0.242ms  0.155ms
  2   34.34.34.3  0.488ms  0.469ms  0.487ms
netman@netman-virtual-machine:~$ traceroute 24.24.24.2
traceroute to 24.24.24.2 (24.24.24.2), 64 hops max
  1   100.100.100.1  2.089ms  0.262ms  0.160ms
  2   24.24.24.2  0.501ms  0.581ms  0.400ms
netman@netman-virtual-machine:~$
```

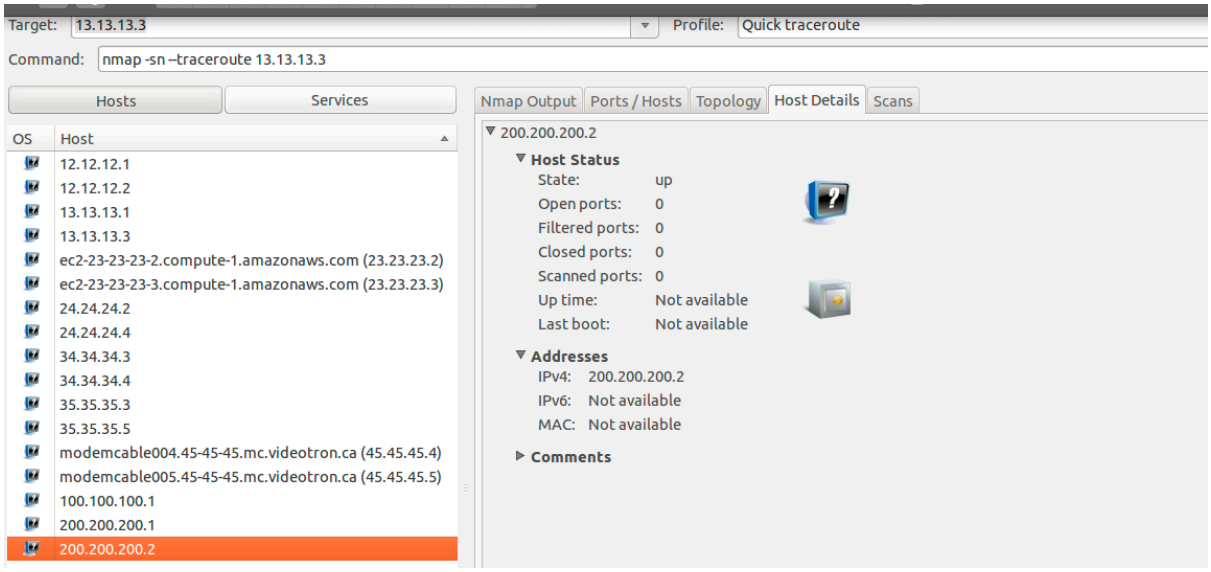
Zenmap:

Zenmap is the security scanner GUI of Nmap. It has been used to give the overview of network topology as shown below.





Screenshot showing the scans performed in each network component.



Screenshot showing the Host details.

2. PERFORMANCE MANAGEMENT:

Network managers are expected to maintain and monitor the network performance. Network performance management involves several parameters. However, (Subramanian 2000) defines throughput, response time, network availability and network reliability as parameters of network performance on a global level.

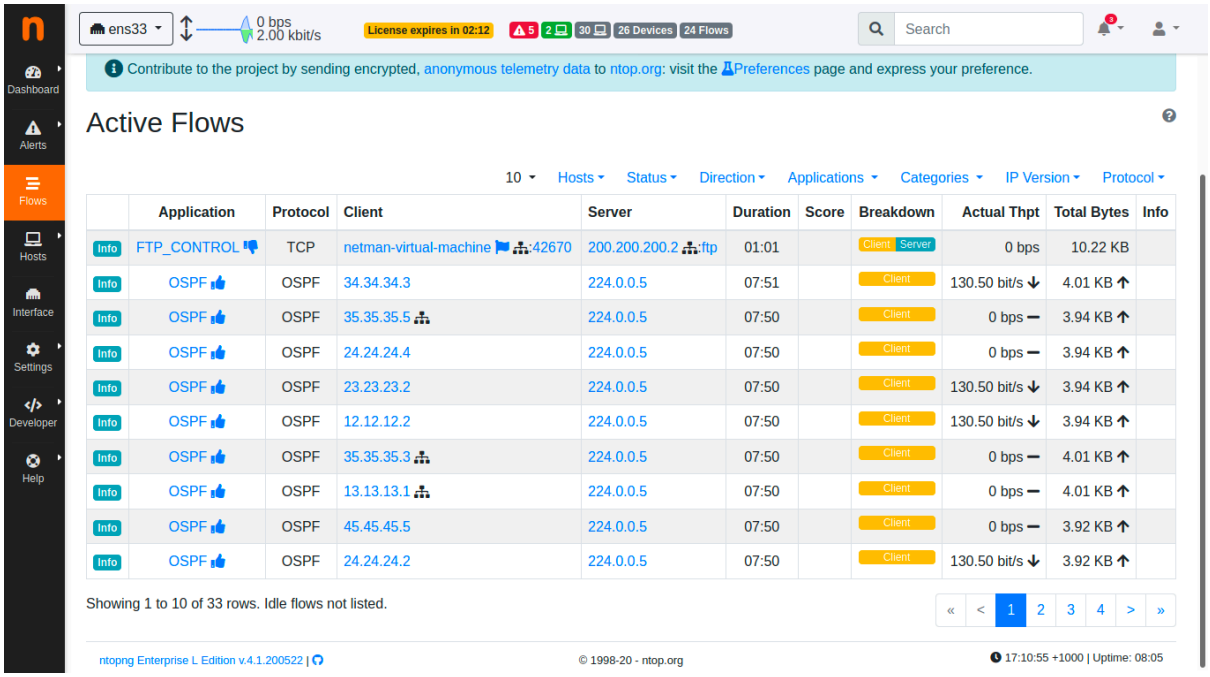
Network analysis tool **ntop** has been used to monitor the network performance and statistics. **nprobe** has been used with **ntop** to collect the netflows and deliver flows to ntopng web GUI.

```
netman@netman-virtual-machine:~$ nprobe --zmq "tcp://*:5556" -i none -n none --collector-port 2055 -T "@NTOPNG@"
23/May/2020 17:01:11 [plugin.c:177] No plugins found in ./plugins
23/May/2020 17:01:11 [plugin.c:185] Loading 23 plugins [.so] from /usr/local/lib/nprobe/plugins
23/May/2020 17:01:11 [nprobe.c:4611] ERROR: Invalid license (/etc/nprobe.license) [Missing license file]
23/May/2020 17:01:11 [nprobe.c:4618] ERROR: ************************************************
23/May/2020 17:01:11 [nprobe.c:4619] ERROR: **                                            **
23/May/2020 17:01:11 [nprobe.c:4620] ERROR: **  Switching to DEMO MODE (missing valid license) **
23/May/2020 17:01:11 [nprobe.c:4621] ERROR: **                                            **
23/May/2020 17:01:11 [nprobe.c:4623] ERROR: **  Purchase your license at                  **
23/May/2020 17:01:11 [nprobe.c:4624] ERROR: **       https://shop.ntop.org/               **
23/May/2020 17:01:11 [nprobe.c:4625] ERROR: **                                            **
23/May/2020 17:01:11 [nprobe.c:4627] ERROR: ************************************************
23/May/2020 17:01:11 [nprobe.c:6666] WARNING: The output interfaceId is set to 0: did you forget to use -Q perhaps ?
23/May/2020 17:01:11 [nprobe.c:6669] WARNING: The input interfaceId is set to 0: did you forget to use -u perhaps ?
23/May/2020 17:01:11 [nprobe.c:6756] Welcome to nProbe v.9.1.200522 ($Revision: 6872 $) for x86_64-pc-linux-gnu with native PF_RING acceleration
23/May/2020 17:01:11 [nprobe.c:6767] Running on Ubuntu 20.04 LTS
23/May/2020 17:01:11 [nprobe.c:6778] [LICENSE] nProbe SystemId: 3B8E8846760B6B22
23/May/2020 17:01:11 [nprobe.c:6849] Sample rate [packet: 1][flow collection/export: 1/1]
23/May/2020 17:01:11 [nprobe.c:9717] ERROR: ************************************************************
23/May/2020 17:01:11 [nprobe.c:9718] ERROR: * NOTE: This is a DEMO version limited to 25000 flows export.  *
23/May/2020 17:01:11 [nprobe.c:9719] ERROR: ************************************************************
23/May/2020 17:01:11 [nprobe.c:9726] Welcome to nProbe v.9.1.200522 for x86_64-pc-linux-gnu
23/May/2020 17:01:11 [nprobe.c:8539] WARNING: Adding %EXPORTER_IPV4_ADDRESS to the template as nProbe is working as collector
23/May/2020 17:01:11 [nprobe.c:8657] Using NetFlow Packet Payload Len: 1472
23/May/2020 17:01:11 [nprobe.c:8577] @NTOPNG@ expanded to " %IN_SRC_MAC %OUT_DST_MAC %INPUT_SNMP %OUTPUT_SNMP %SRC_VLAN %IPV4_SRC_ADDR %IPV4_DST_ADDR
%L4_SRC_PORT %L4_DST_PORT %IPV6_SRC_ADDR %IPV6_DST_ADDR %IP_PROTOCOL_VERSION %PROTOCOL %L7_PROTO %IN_BYTES %IN_PKTS %OUT_BYTES %OUT_PKTS %FIRST_SWITCH
ED %LAST_SWITCHED %CLIENT_TCP_FLAGS %SERVER_TCP_FLAGS   %EXPORTER_IPV4_ADDRESS"
23/May/2020 17:01:11 [nprobe.c:8692] Flow export type: bidirectional flows
23/May/2020 17:01:11 [plugin.c:1171] 0 plugin(s) enabled
23/May/2020 17:01:11 [nprobe.c:9159] Each flow is 104 bytes long
23/May/2020 17:01:11 [nprobe.c:9160] The # flows per packet has been set to 13
23/May/2020 17:01:11 [nprobe.c:9163] IP TOS is ignored
23/May/2020 17:01:11 [nprobe.c:10009] Flows ASs will not be computed (no GeoDB files loaded)
23/May/2020 17:01:11 [nprobe.c:10114] Not capturing packet from interface (collector mode)
23/May/2020 17:01:11 [util.c:5099] Initializing ZMQ as server
23/May/2020 17:01:11 [util.c:5176] ERROR: Unable to bind ZMQ endpoint tcp://*:5556: Address already in use
23/May/2020 17:01:11 [util.c:4114] WARNING: Skept UDP socket buffer enlargement: lack of privileges
23/May/2020 17:01:11 [util.c:4115] WARNING: Flow collection drops are possible with bursty exporters!
23/May/2020 17:01:11 [util.c:4123] Privileges are not dropped as we're not superuser
23/May/2020 17:01:11 [collect.c:192] Flow collector listening on port 2055 (IPv4/v6)
23/May/2020 17:01:11 [export.c:540] Using TLV as serialization format
23/May/2020 17:01:11 [nprobe.c:10377] nProbe started successfully
```

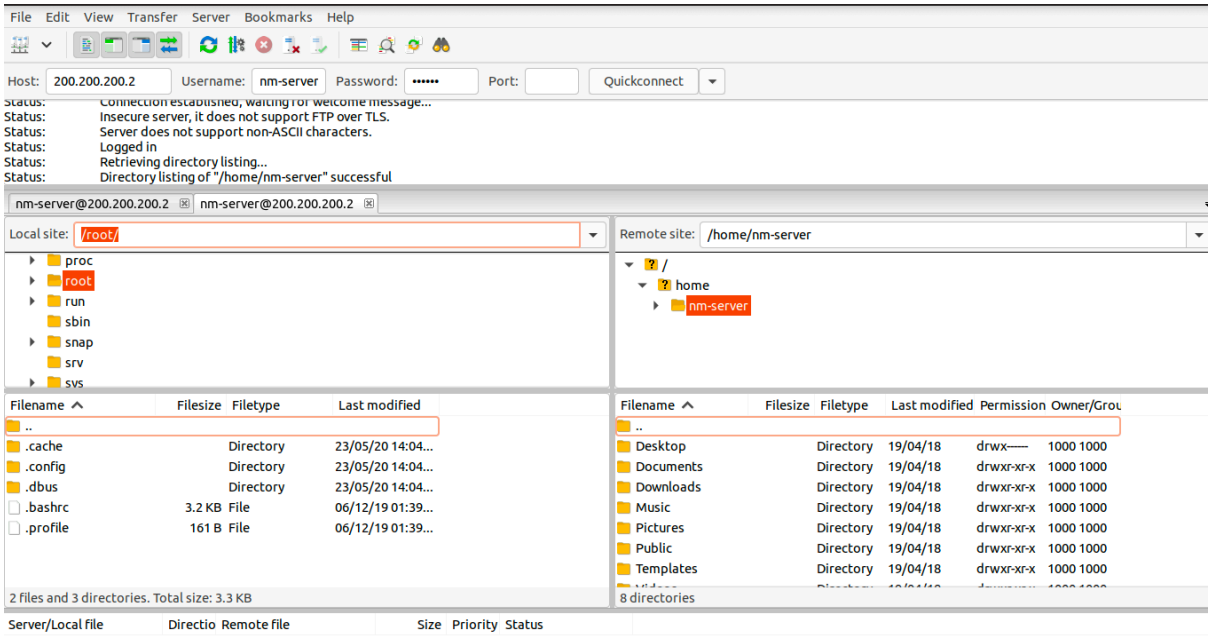
nprobe executed to collect flows for ntopng

```
netman@netman-virtual-machine:~$ sudo ntopng -Z /myntopng
23/May/2020 17:02:51 [Ntop.cpp:2253] Setting local networks to 127.0.0.0/8
23/May/2020 17:02:51 [Redis.cpp:157] Successfully connected to redis 127.0.0.1:6379@0
23/May/2020 17:02:51 [Redis.cpp:157] Successfully connected to redis 127.0.0.1:6379@0
23/May/2020 17:02:51 [NtopPro.cpp:296] [LICENSE] Reading license from Redis
23/May/2020 17:02:51 [NtopPro.cpp:424] [LICENSE] Unable to validate license [Empty license file]
23/May/2020 17:02:51 [NtopPro.cpp:492] WARNING: [LICENSE] Invalid license [Empty license file]
23/May/2020 17:02:51 [NtopPro.cpp:509] WARNING: [LICENSE] ntopng will now run in Enterprise L edition for 10 minutes
23/May/2020 17:02:51 [NtopPro.cpp:511] WARNING: [LICENSE] before returning to community mode
23/May/2020 17:02:51 [NtopPro.cpp:513] WARNING: [LICENSE] You can buy a permanent license at http://shop.ntop.org
23/May/2020 17:02:51 [NtopPro.cpp:515] WARNING: [LICENSE] or run ntopng in community mode starting
23/May/2020 17:02:51 [NtopPro.cpp:516] WARNING: [LICENSE] ntopng --community
23/May/2020 17:02:52 [PF_RINGInterface.cpp:53] Reading packets from PF_RING v.7.7.0 interface ens33...
23/May/2020 17:02:52 [Ntop.cpp:2358] Registered interface ens33 [id: 1]
23/May/2020 17:02:52 [PF_RINGInterface.cpp:53] Reading packets from PF_RING v.7.7.0 interface lo...
23/May/2020 17:02:52 [Ntop.cpp:2358] Registered interface lo [id: 2]
23/May/2020 17:02:52 [main.cpp:316] PID stored in file /var/run/ntopng.pid
23/May/2020 17:02:52 [Geolocation.cpp:150] Running without geolocation support.
23/May/2020 17:02:52 [Geolocation.cpp:151] To enable geolocation follow the instructions at
23/May/2020 17:02:52 [Geolocation.cpp:152] https://github.com/ntop/ntopng/blob/dev/doc/README.geolocation.md
23/May/2020 17:02:52 [HTTPserver.cpp:1495] Web server dirs [/usr/share/ntopng/httpdocs][/usr/share/ntopng/scripts]
23/May/2020 17:02:52 [HTTPserver.cpp:1498] HTTP server listening on 3000
23/May/2020 17:02:52 [Utils.cpp:761] User changed to ntopng
23/May/2020 17:02:52 [main.cpp:386] Working directory: /var/lib/ntopng
23/May/2020 17:02:52 [main.cpp:388] Scripts/HTML pages directory: /usr/share/ntopng
23/May/2020 17:02:52 [Ntop.cpp:454] Welcome to ntopng x86_64 v.4.1.200522 - (C) 1998-20 ntop.org
23/May/2020 17:02:52 [Ntop.cpp:464] Built on Ubuntu 20.04 LTS
23/May/2020 17:02:52 [NtopPro.cpp:698] [LICENSE] System Id:     3B8E8B46760B6B22
23/May/2020 17:02:52 [NtopPro.cpp:699] [LICENSE] Edition:       Enterprise L
23/May/2020 17:02:52 [NtopPro.cpp:700] [LICENSE] License Type:  Time-Limited [Empty license file] License
23/May/2020 17:02:52 [NtopPro.cpp:720] [LICENSE] Validity:      Until Sat May 23 17:12:51 2020
23/May/2020 17:02:52 [Ntop.cpp:855] Adding 127.0.0.1/32 as IPv4 interface address for lo
23/May/2020 17:02:52 [Ntop.cpp:864] Adding 127.0.0.0/8 as IPv4 local network for lo
23/May/2020 17:02:52 [Ntop.cpp:855] Adding 100.100.100.2/32 as IPv4 interface address for ens33
23/May/2020 17:02:52 [Ntop.cpp:864] Adding 100.100.100.0/24 as IPv4 local network for ens33
23/May/2020 17:02:52 [Ntop.cpp:886] Adding ::1/128 as IPv6 interface address for lo
23/May/2020 17:02:52 [Ntop.cpp:896] Adding ::1/128 as IPv6 local network for lo
23/May/2020 17:02:52 [PeriodicActivities.cpp:105] Started periodic activities loop...
```

ntopng execution on terminal to access web interface



ntopng web interface showing active flows



Filezilla to carry out simple ftp between client and server

POLLING:

Active monitoring of network is performed using polling. The following parameters is used for active monitoring of the network components:

Measurement: Continuous ICMP

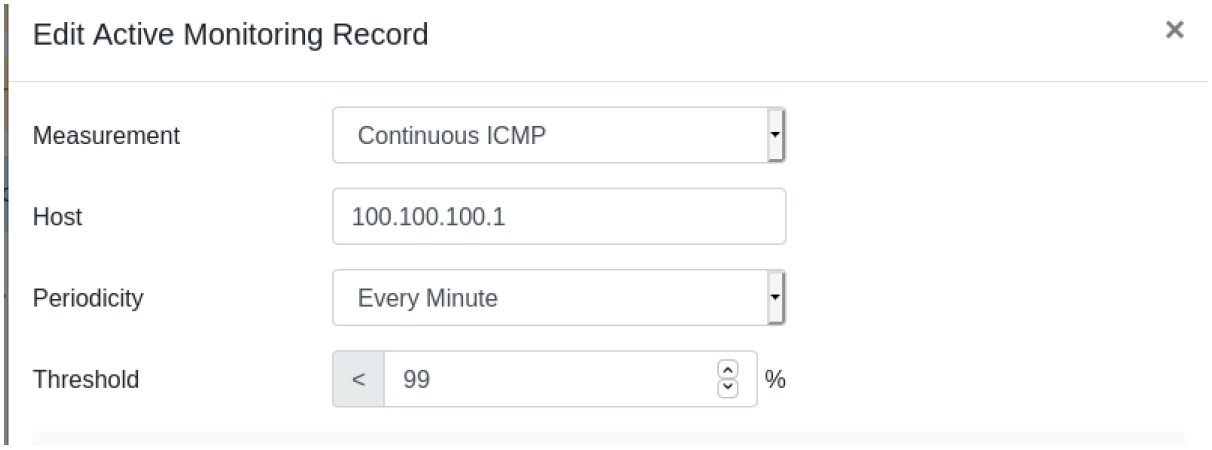
Continuous ICMP is used because it tests the host status on an ongoing basis by continuously pinging the host.

Host: The IP of the host to check its status.

Periodicity: Every Minute

It is to delete the old timeseries data and avoid data accumulation. Since, the web interface of ntopng tool is not as fast as an enterprise network monitoring tool, the periodicity of data deletion has been set to every minute.

Threshold: The threshold is set to <99%. If the threshold increases than the set value an alert would be generated.

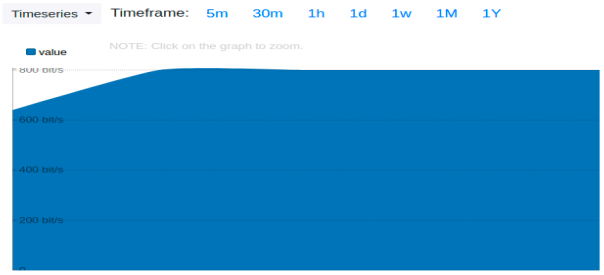


Statistics of router1(100.100.100.1) shown below.

The RTT (round trip time) and jitter of router1 can be observed as 0.7 and 0.5ms respectively.

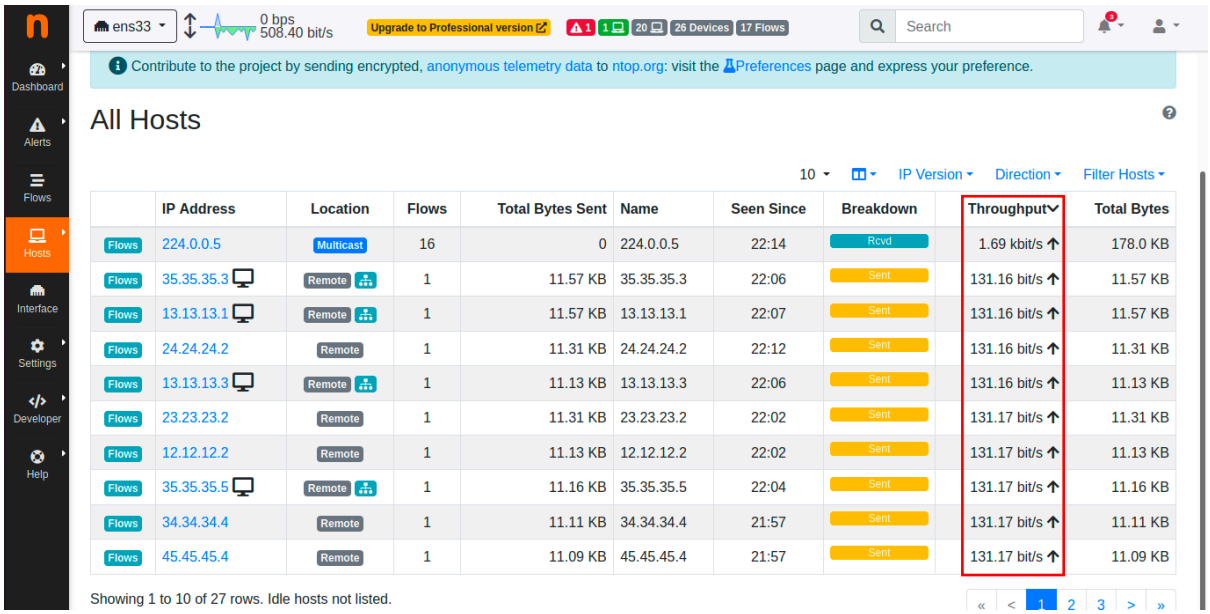
URL	Chart	Threshold	24H Availability	Last Measurement	Last IP	Measurement	Mean RTT / Jitter	Actions
cicmp://100.100.100.1		99 %		01:01 ago	100.100.100.1	100 %	0.7 / 0.5 ms	Edit Delete

The chart below depicts the minimum, maximum and average data flowing through router1.



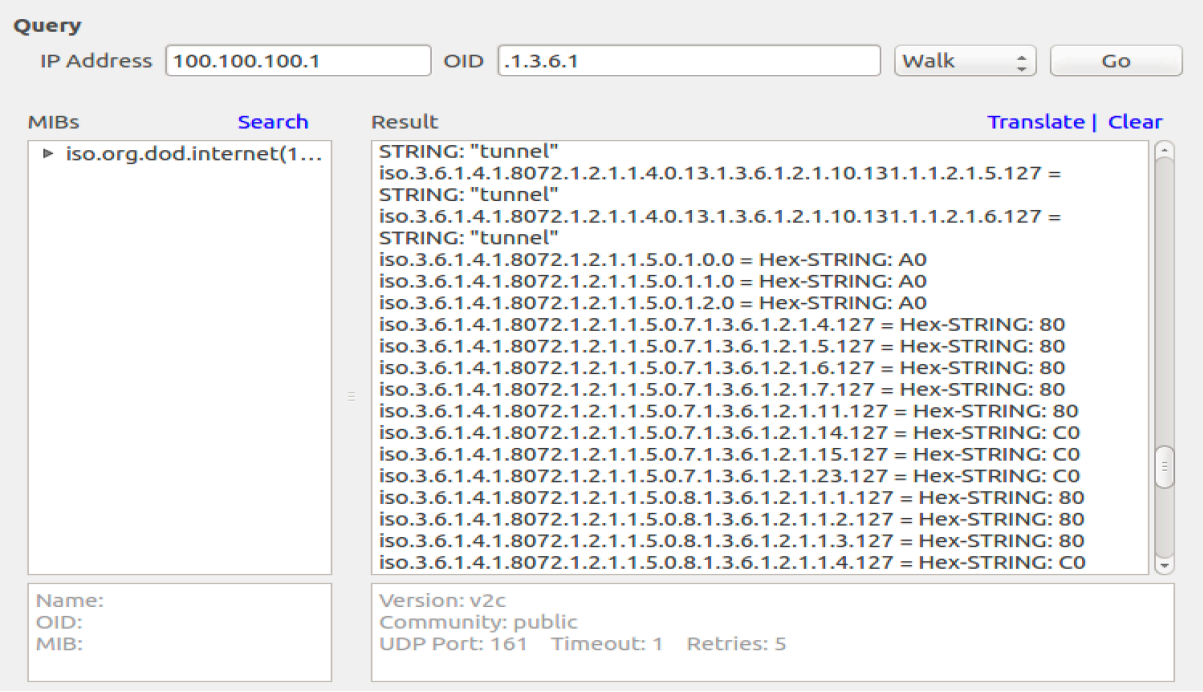
	Time	Value
Min	05/24/20 14:12:00	640 bit/s
Max	05/24/20 14:13:00	800 bit/s
Last	05/24/20 14:16:00	800 bit/s
Average	768 bit/s	
95th Percentile	800 bit/s	
Total Traffic	0	
Selection Time	Sun May 24 2020 14:14:00 GMT+1000 (Australian Eastern Standard Time)	
Minute Interface Top Talkers	• Senders [Avg Traffic/sec] 1. 172.16.7.2 (590.13 bit/s) 2. 100.100.100.2 (565.73 bit/s) 3. 172.16.7.155 (342.67 bit/s) 4. Other (2.49 Kbit/s) • Receivers [Avg Traffic/sec] 1. 224.0.0.5 (1.04 Kbit/s) 2. 172.16.7.155 (642.4 bit/s) 3. 172.16.7.153 (447.07 bit/s) 4. Other (1.85 Kbit/s)	

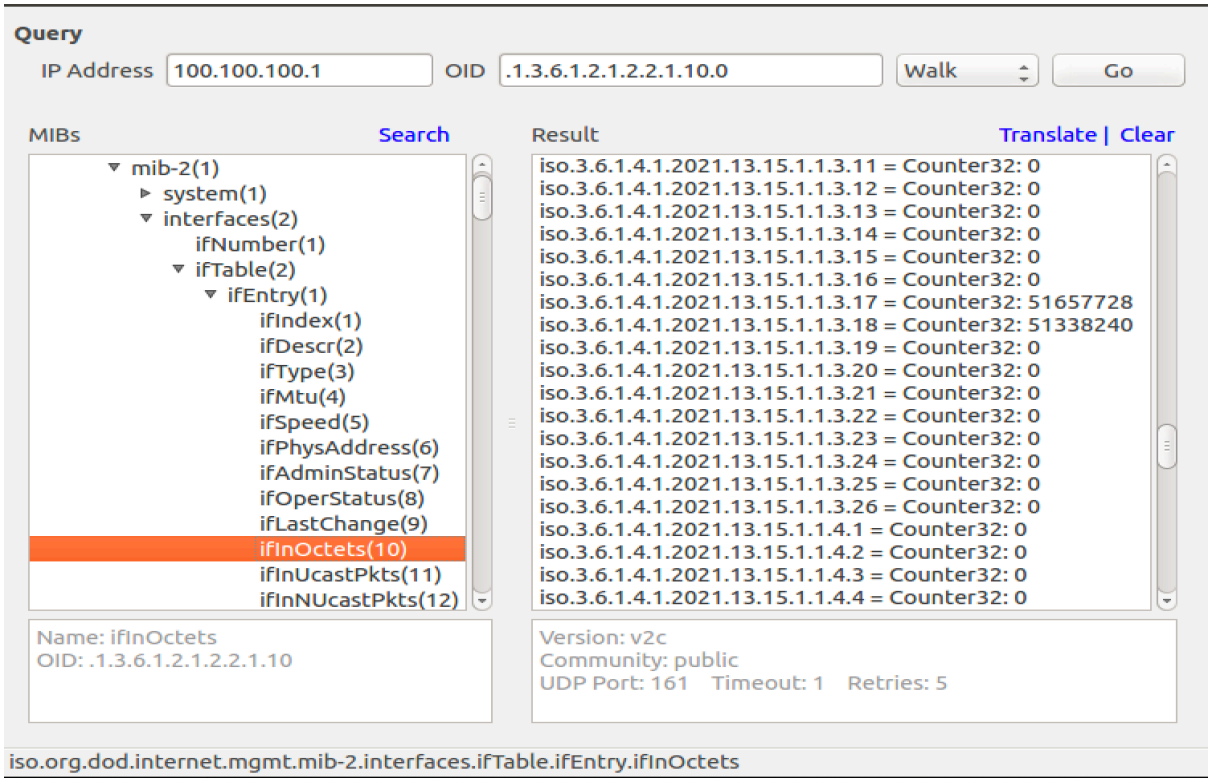
When the Hosts in the network are observed, ntopng calculates and displays the **throughputs.**



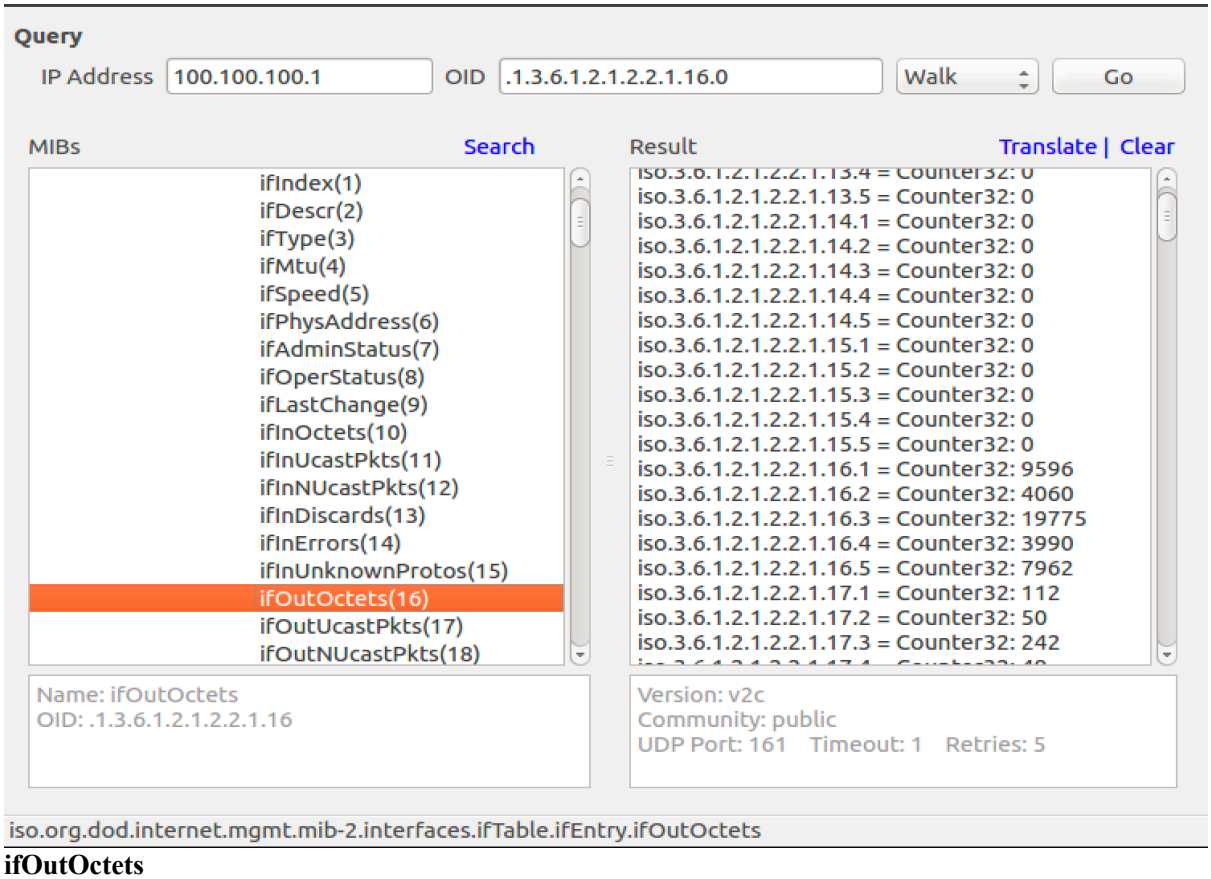
QTMIB SNMP walk for router1:

SNMP walk, performed for data collection and check all the OID parameters available for the SNMP device.

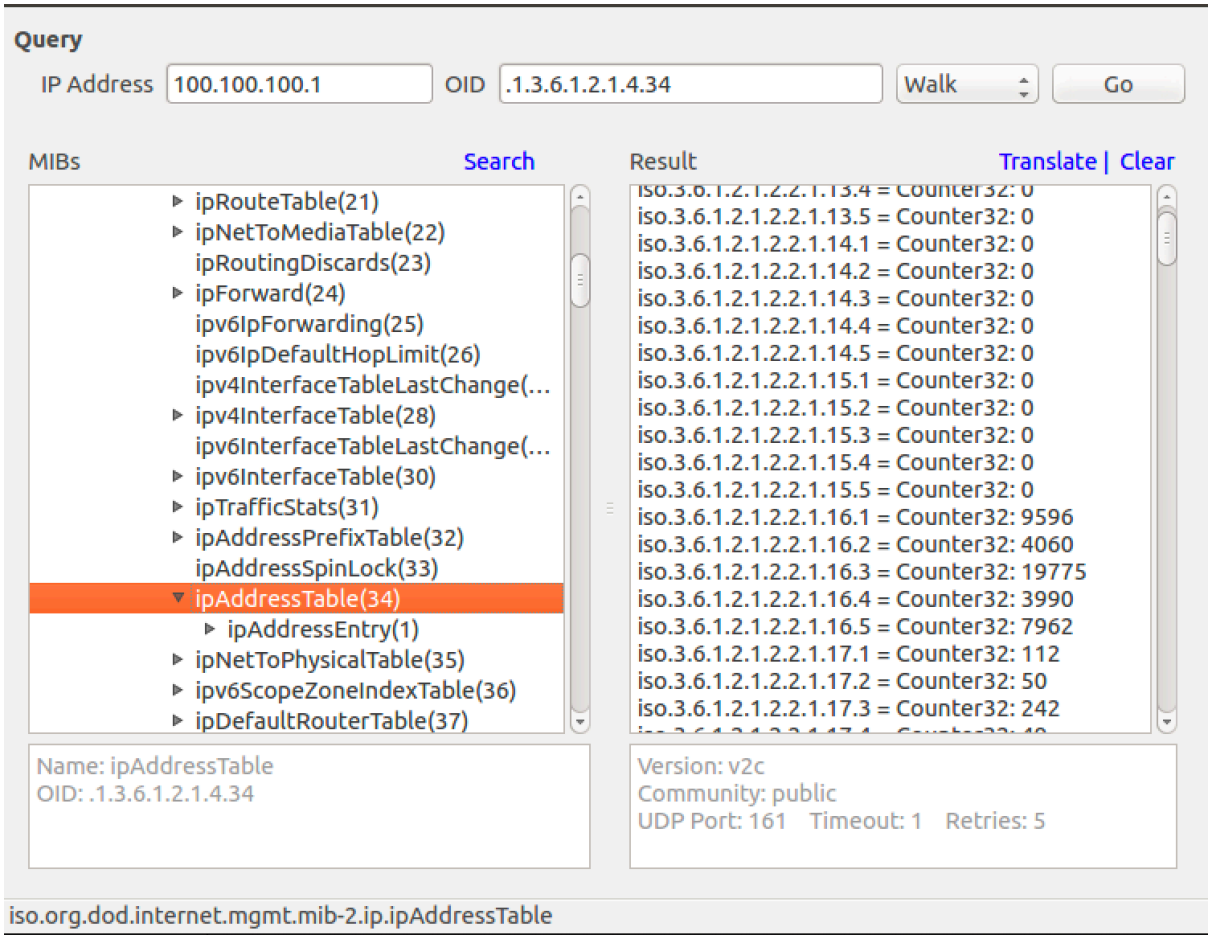




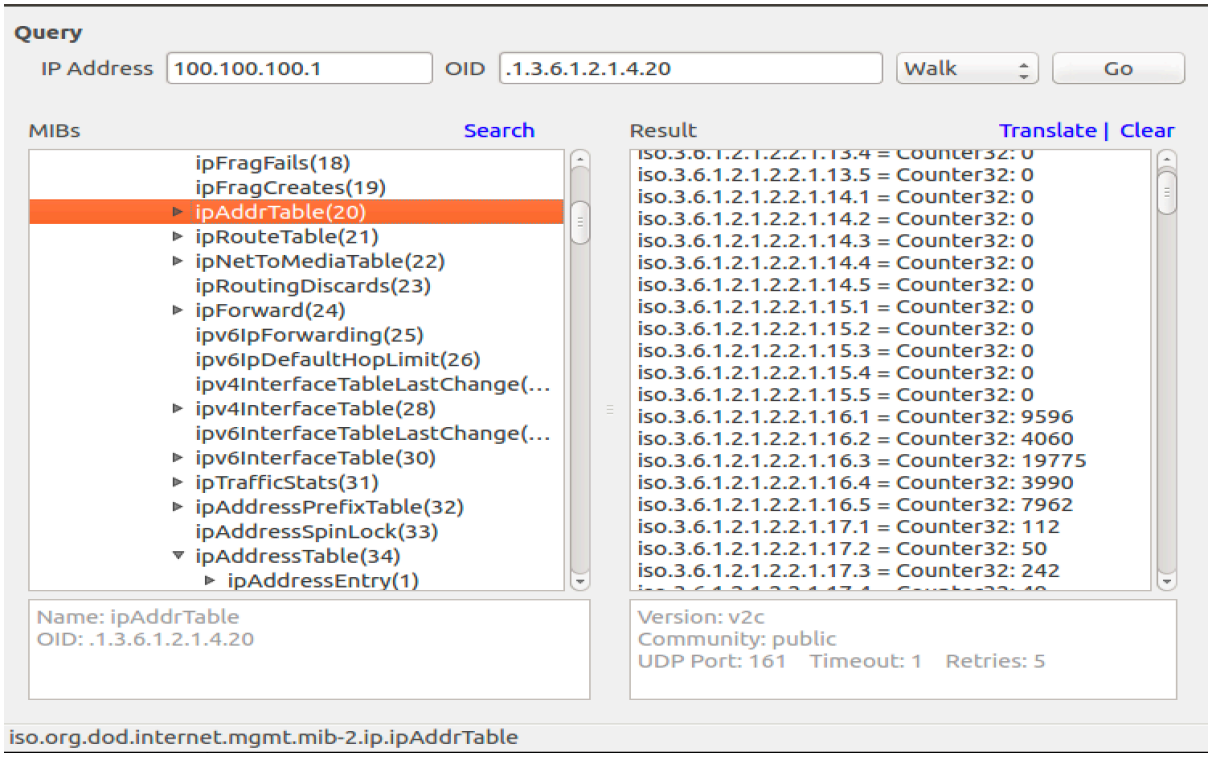
ifinOctets



ifOutOctets



ipAddressTable

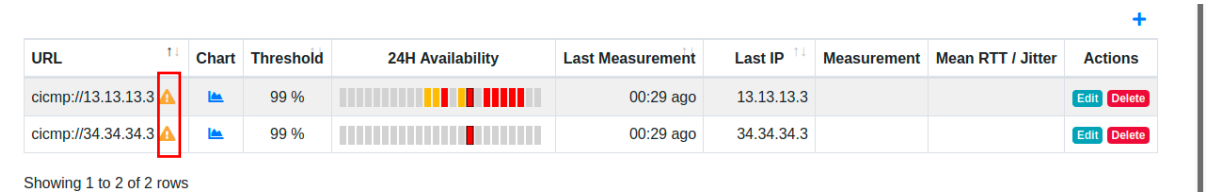


ipAddrTable

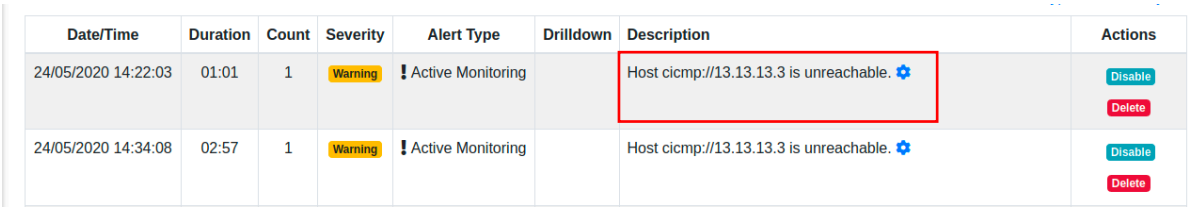
3. FAULT MANAGEMENT:

Failure of a network component or loss of connectivity can cause fault in a network. According to (Subramanian 2000), fault management involves fault detection, fault location, service restoration, identifying the root cause of the problem and resolving the problem.

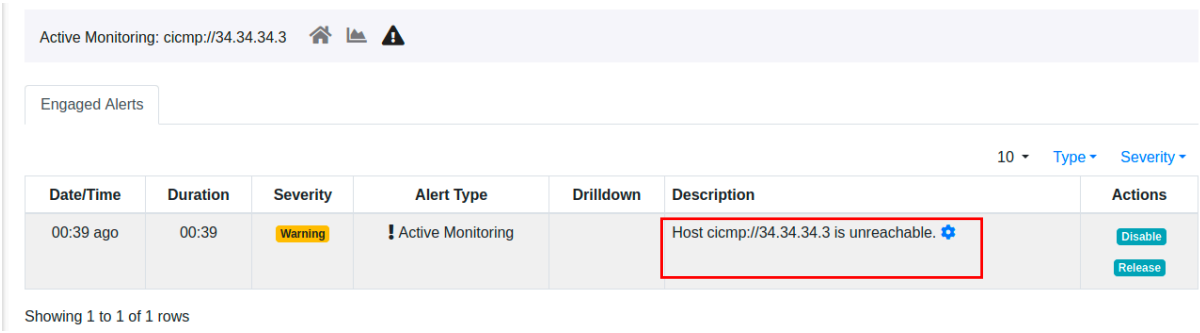
Here, router3 ethernet interfaces eth10(13.13.13.3) and eth12(34.34.34.3) were disabled. The monitoring system generated the alarms and identified the location and cause of alarm.



Alerts generated

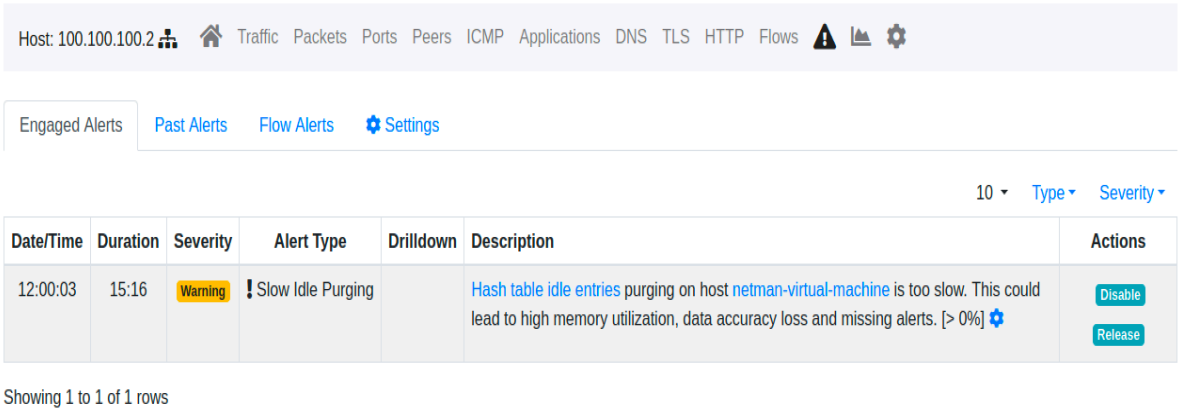


Host 13.13.13.3 unreachable

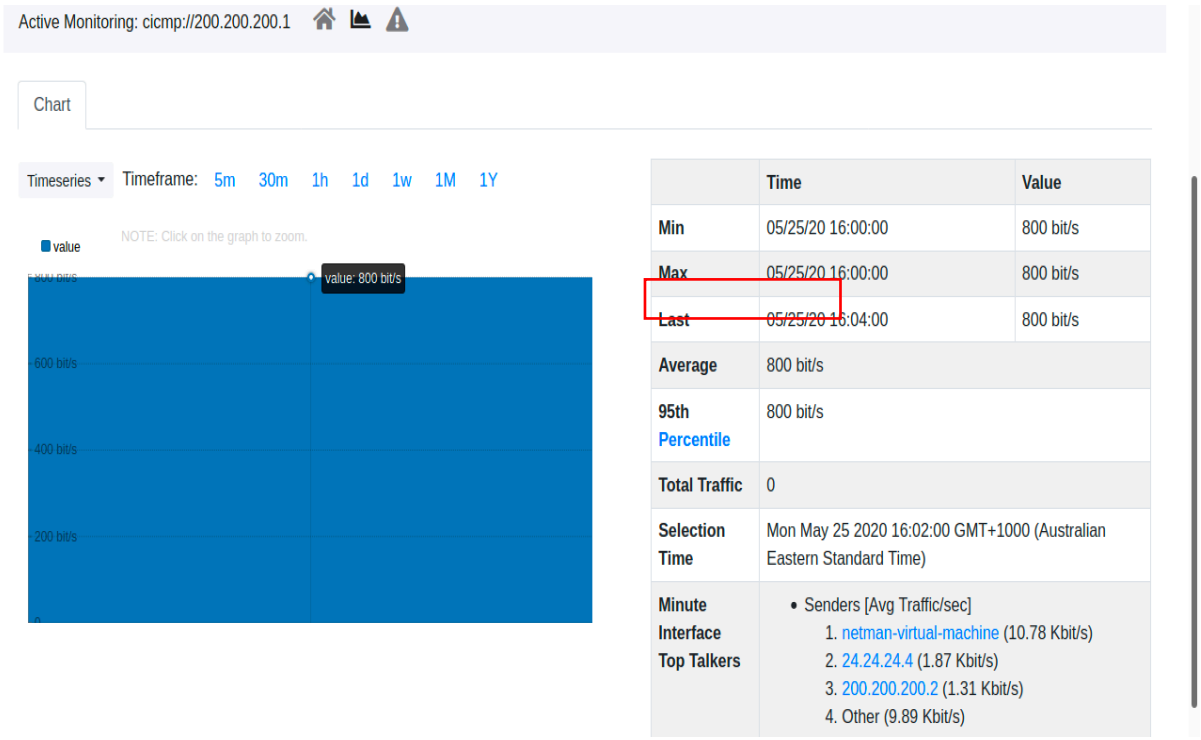


Host 34.34.34.3 unreachable

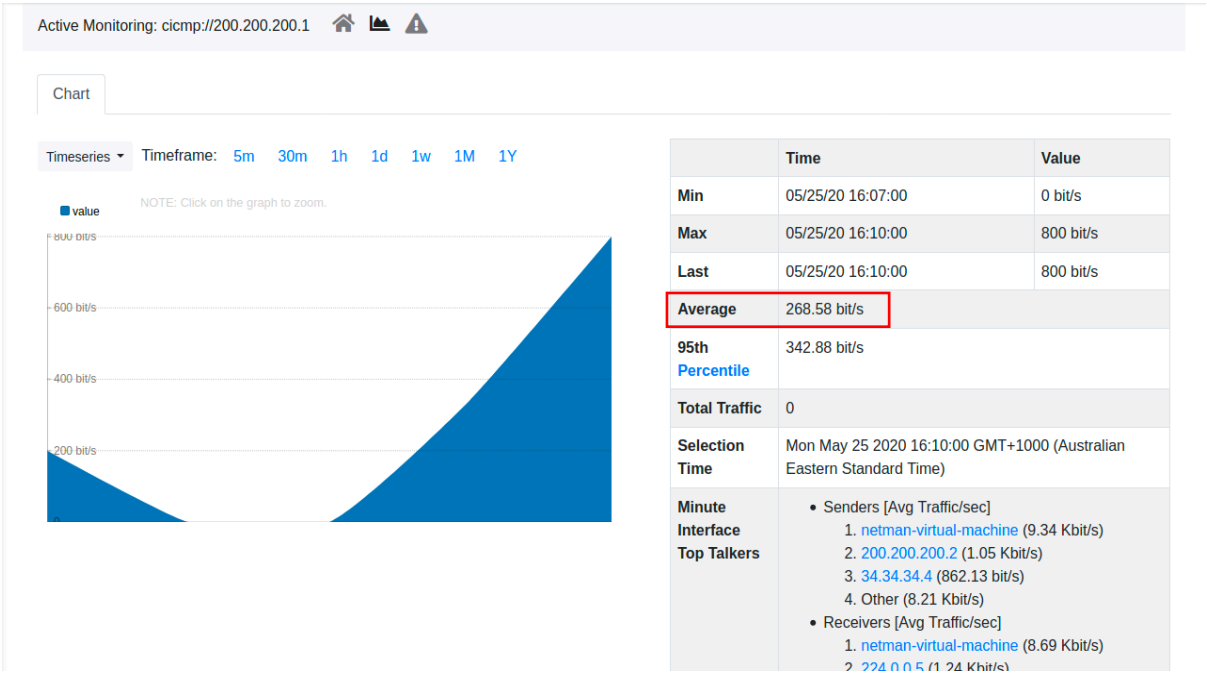
The flows hash table entries are periodically purged when they are idle for a while with no new entry. Due to the link down, an alert could be seen showing that the purging of hash-table entries is too slow.

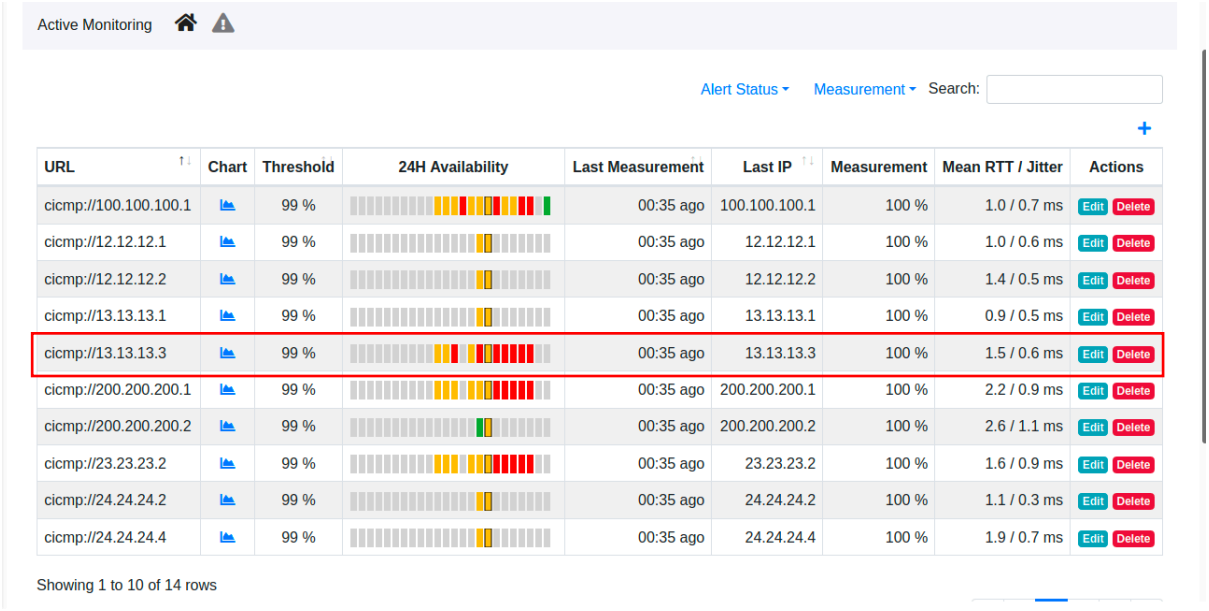


Congestion and increased load can be seen when router3 links were down.



After solving the issue, and bringing up the links of Router3, there was a drastic change in the results.





Status after fixing the issue

4. SECURITY MANAGEMENT:

It is the task of network manager to provide access to the user. In the following procedure, user credentials and their access level on routers is created.

Setting up system user.

```
vyos@vyos# set system login user vishal
Possible completions:
 > authentication
                Authentication password
   full-name    Full name of the user (use quotes for names with spaces)
+  group        Additional group membership
   home-directory
                Home directory
   level        User privilege level


[edit]
```

User vishal is created and admin level privileges are given to the user.

```
vyos@vyos# set system login user vishal level
Possible completions:
   admin        Administrators
   operator     Operators
```

User authentication is critical part of security management.

```
vyos@vyos# set system login user vishal authentication
Possible completions:
   encrypted-password
                Encrypted password
   plaintext-password
                Plaintext password for encryption
+> public-keys  Remote access public keys
```

Here, user **vishal** will login using a **plaintext-password** which is later saved in encrypted format**.**

```
vyos@vyos# set system login user vishal authentication plaintext-password vishal
[edit]
vyos@vyos# compare
[edit system login]
+user vishal {
+    authentication {
+        plaintext-password vishal
+    }
+    level admin
+}
[edit]
```

Another user **test1** is created and given operator level privileges.

```
vyos@vyos# set system login user test1 level operator
[edit]
vyos@vyos# compare
[edit system login]
+user test1 {
+    authentication {
+        plaintext-password test1
+    }
+    level operator
+}
+user vishal {
+    authentication {
+        plaintext-password vishal
+    }
+    level admin
+}
```

System login users using command: **show system login**

```
 user test1 {
     authentication {
         encrypted-password $6$dVnGK4UR$ge5z9r2LH6HT1JcMozMJ/6PcoQYnxDk2htWplqw1
ZkerOWnVX1nJDggw/ZZAE92DeFudYWnzgtmVDHllamvZF/
         plaintext-password ""
     }
     level operator
 }
 user vishal {
     authentication {
         encrypted-password $6$/jvIhmGn6WX$jvVKEc4q9.iqTu18auKeUDkqSdvPktlj7ae6d
brZ/PjHVsa2BLZUr4H6gjYoOg7IuI2CrkxfBUMA2orczJLxL/
         plaintext-password ""
     }
     level admin
 }
 user vyos {
     authentication {
         encrypted-password $1$lgotECFe$7KTVLG2urpHZ/H9DXKoAX.
         plaintext-password ""
     }
     level admin
 }
```

Executing Telnet session in client system on router2:

```
netman@netman-virtual-machine:~$ telnet 12.12.12.2
Trying 12.12.12.2...
Connected to 12.12.12.2.
Escape character is '^]'.

Welcome to VyOS
vyos login: vishal
Password:
Linux vyos 3.13.11-1-586-vyos #1 SMP Wed Aug 12 01:58:45 UTC 2015 i686
Welcome to VyOS.
This system is open-source software. The exact distribution terms for
each module comprising the full system are described in the individual
files in /usr/share/doc/*/copyright.
vishal@vyos:~$ config
[edit]
vishal@vyos#
```

```
netman@netman-virtual-machine:~$ telnet 12.12.12.2
Trying 12.12.12.2...
Connected to 12.12.12.2.
Escape character is '^]'.

Welcome to VyOS
vyos login: test1
Password:
Linux vyos 3.13.11-1-586-vyos #1 SMP Wed Aug 12 01:58:45 UTC 2015 i686
Welcome to VyOS.
This system is open-source software. The exact distribution terms for
each module comprising the full system are described in the individual
files in /usr/share/doc/*/copyright.
test1@vyos> config

  Invalid command: [config]

test1@vyos>
```

Setting up ssh service on router:

```
vyos@vyos# set service ssh
Possible completions:
   allow-root    Enable root login over ssh
   ciphers       Allowed ciphers
   disable-host-validation
                 Don't validate the remote host name with DNS
   disable-password-authentication
                 Don't allow unknown user to login with password
+  listen-address
                 Local addresses SSH service should listen on
   macs          Specifies the available MAC (message authentication code) algor
thms. The MAC algorithm is used in protocol version 2 for data integrity protec
ion. Multiple algorithms must be comma-separated. See 'man sshd_config' for sup
orted MACs.
   port          Port for SSH service
```

Executing ssh session using client system on router2:

```
netman@netman-virtual-machine:~$ ssh vishal@12.12.12.2
The authenticity of host '12.12.12.2 (12.12.12.2)' can't be established.
RSA key fingerprint is SHA256:i6yqQoM1tEtW/2r4splsNQRDBXU2gCzsWcNXgURceFk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '12.12.12.2' (RSA) to the list of known hosts.
Welcome to VyOS
vishal@12.12.12.2's password:
Linux vyos 3.13.11-1-586-vyos #1 SMP Wed Aug 12 01:58:45 UTC 2015 i686
Welcome to VyOS.
This system is open-source software. The exact distribution terms for
each module comprising the full system are described in the individual
files in /usr/share/doc/*/copyright.
Last login: Sun May 24 14:41:26 2020
vishal@vyos:~$ config
[edit]
vishal@vyos#
```

```
netman@netman-virtual-machine:~$ ssh test1@12.12.12.2
The authenticity of host '12.12.12.2 (12.12.12.2)' can't be established.
RSA key fingerprint is SHA256:i6yqQoM1tEtW/2r4splsNQRDBXU2gCzsWcNXgURceFk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '12.12.12.2' (RSA) to the list of known hosts.
Welcome to VyOS
test1@12.12.12.2's password:
Linux vyos 3.13.11-1-586-vyos #1 SMP Wed Aug 12 01:58:45 UTC 2015 i686
Welcome to VyOS.
This system is open-source software. The exact distribution terms for
each module comprising the full system are described in the individual
files in /usr/share/doc/*/copyright.
Last login: Sun May 24 14:43:17 2020
test1@vyos> config

  Invalid command: [config]

test1@vyos>
```

SNMP Security:

SNMPv1:

SNMPv1 pairs the SNMP agent with SNMP managers and forms an SNMP community. A community name is provided for each community formed using SNMP agent and managers. In the below screenshot, **community public** which is **read-only** is assigned for the SNMP community created. The other common names are **private(read-write)** and **trap.** The read-write and read-only permissions are for SNMP managers, to access MIB of the community agents. In SNMPv1 community names are considered as passwords to access agents (VmWare 2019).

```
    snmp {
        community public {
            authorization ro
            client 100.100.100.2
        }
        trap-target 100.100.100.2 {
        }
```

SNMPv3:

SNMPv3 was introduced with new security features which were missing in the previous versions of SNMP which were known for weak security. Community strings sent in clear text were the only authentication procedure between manager and agent until SNMPv3 got introduced.

In SNMPv3 the message parameters are encoded as an octet string and these parameters were decoded according to the security model used in the network. The SNMPv3 aims to accomplish the CIA triad of security.

Here, SNMPv3 has been setup for router1 using the following commands:

- **set service snmp v3 engineid '0x0aa0d6'**
- **set service snmp v3 group defaultgroup mode 'ro'**
- **set service snmp v3 group defaultgroup seclevel 'priv'**
- **set service snmp v3 group defaultgroup view 'defaultview'**
- **set service snmp v3 view defaultview oid '1'**

```
vyos@vyos# compare
[edit service snmp]
+v3 {
+    engineid 0x0aa0d6
+    group defaultgroup {
+        mode ro
+        seclevel priv
+        view defaultview
+    }
+    view defaultview {
+        oid 1 {
+        }
+    }
+}
[edit]
```

```
service {
    snmp {
        community public {
            authorization ro
            client 100.100.100.2
        }
        trap-target 100.100.100.2 {
        }
        v3 {
            engineid 0x0aa0d6
            group defaultgroup {
                mode ro
                seclevel priv
                view defaultview
            }
            view defaultview {
                oid 1 {
                }
            }
        }
    }
```

Setting up SNMPv3 for a user:

- **set service snmp v3 user vishal auth plaintext-key testuser**
- **set service snmp v3 user vishal auth type 'md5'**
- **set service snmp v3 user vishal engineid '0x0aa0d6'**
- **set service snmp v3 user vishal group 'defaultgroup'**
- **set service snmp v3 user vishal mode 'ro'**
- **set service snmp v3 user vishal privacy type aes**
- **set service snmp v3 user vishal privacy plaintext-key testuser**

```
vyos@vyos# compare
[edit service snmp v3]
+user vishal {
+    auth {
+        plaintext-key testuser
+        type md5
+    }
+    engineid 0x0aa0d6
+    group defaultgroup
+    mode ro
+    privacy {
+        plaintext-key testuser
+        type aes
+    }
+}
[edit]
vyos@vyos# _
```

```
        v3 {
            engineid 0x0aa0d6
            group defaultgroup {
                mode ro
                seclevel priv
                view defaultview
            }
            user vishal {
                auth {
                    encrypted-key 0xcc4a2de066e6e4652fd880ba56fbba60
                    type md5
                }
                engineid 0x0aa0d6
                group defaultgroup
                mode ro
                privacy {
                    encrypted-key 0xcc4a2de066e6e4652fd880ba56fbba60
                    type aes
                }
            }
            view defaultview {
                oid 1 {
                }
            }
```

FIREWALL:

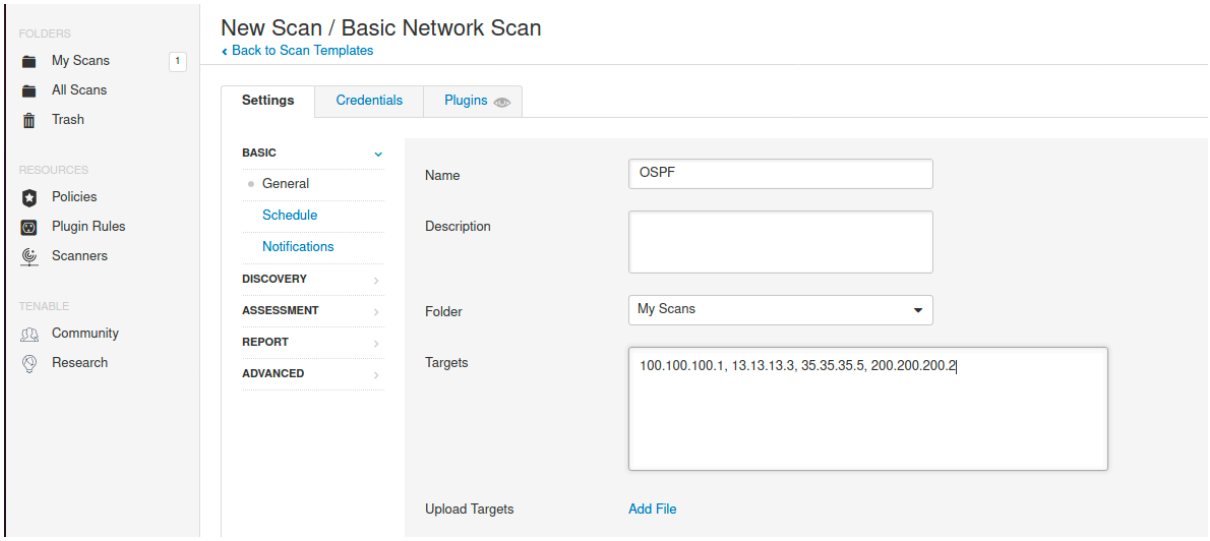
Router1 was configured with firewall since it is the first point of contact with the client to access any other network elements.

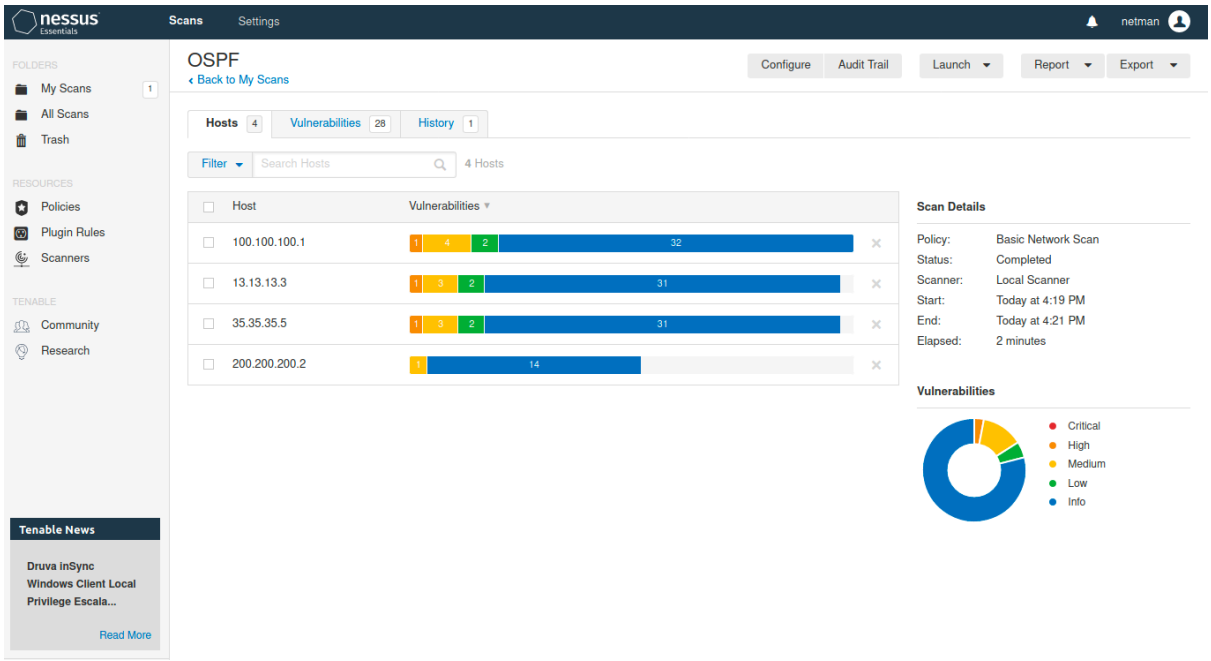
```
firewall {
    group {
        address-group allowed {
            address 100.100.100.2
        }
    }
    name firewall1 {
        default-action accept
        description router1_firewall
    }
}
/* Router1 interfaces configured */
interfaces {
    ethernet eth12 {
        address 100.100.100.1/24
        hw-id 00:0c:29:c5:35:99
        vif 100 {
            firewall {
                in {
                    name firewall1
                }
            }
        }
    }
```

```
firewall {
    all-ping enable
    broadcast-ping disable
    config-trap disable
    group {
        address-group allowed {
            address 100.100.100.2
        }
    }
    ipv6-receive-redirects disable
    ipv6-src-route disable
    ip-src-route disable
    log-martians enable
    name firewall1 {
        default-action accept
        description router1_firewall
    }
    receive-redirects disable
    send-redirects enable
    source-validation disable
    syn-cookies enable
    twa-hazards-protection disable
}
```

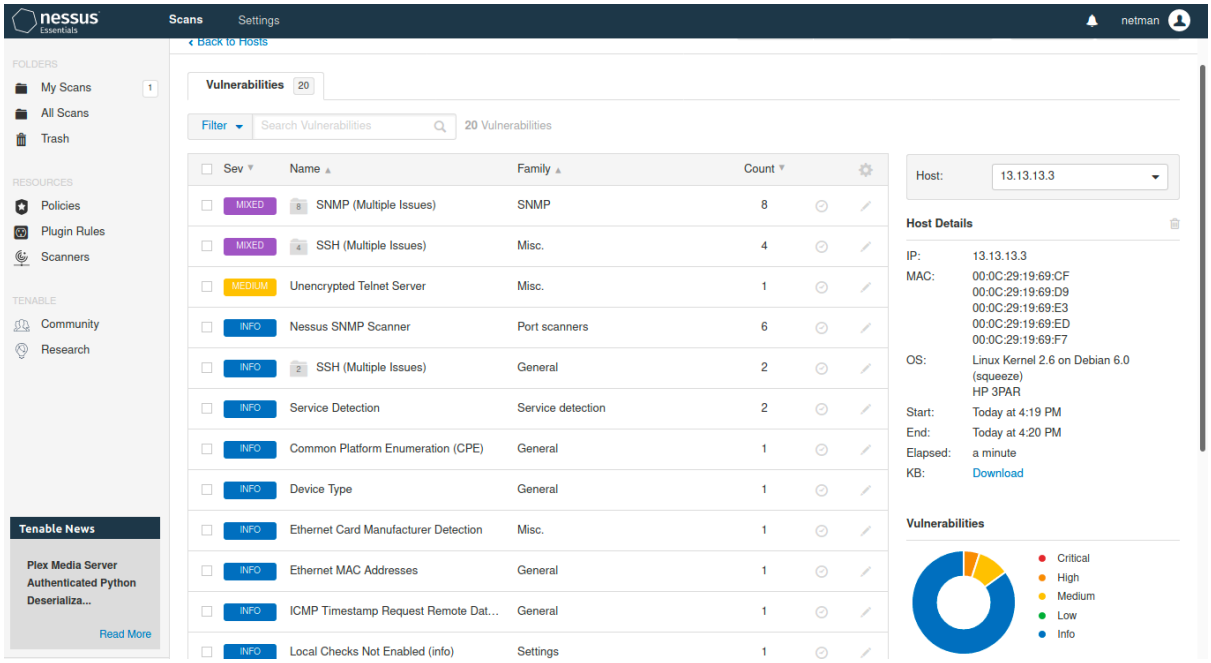
Network Security Scan:

Nessus tool by Tenable was used for network security scan and address the vulnerabilities in the network.

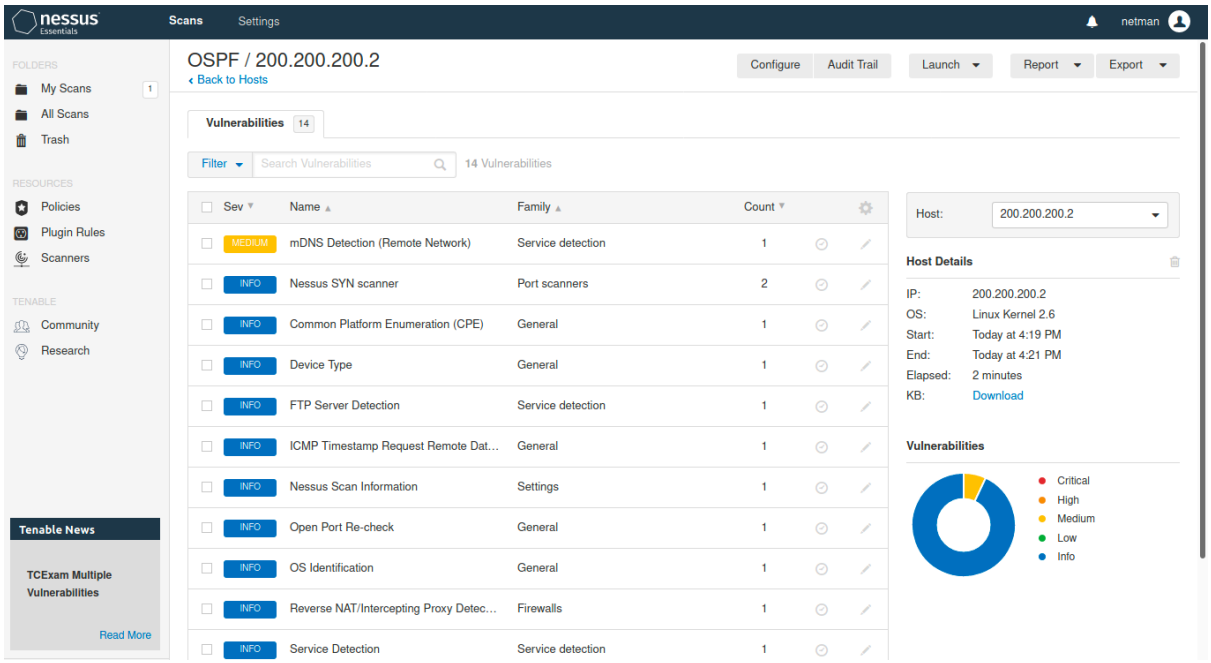




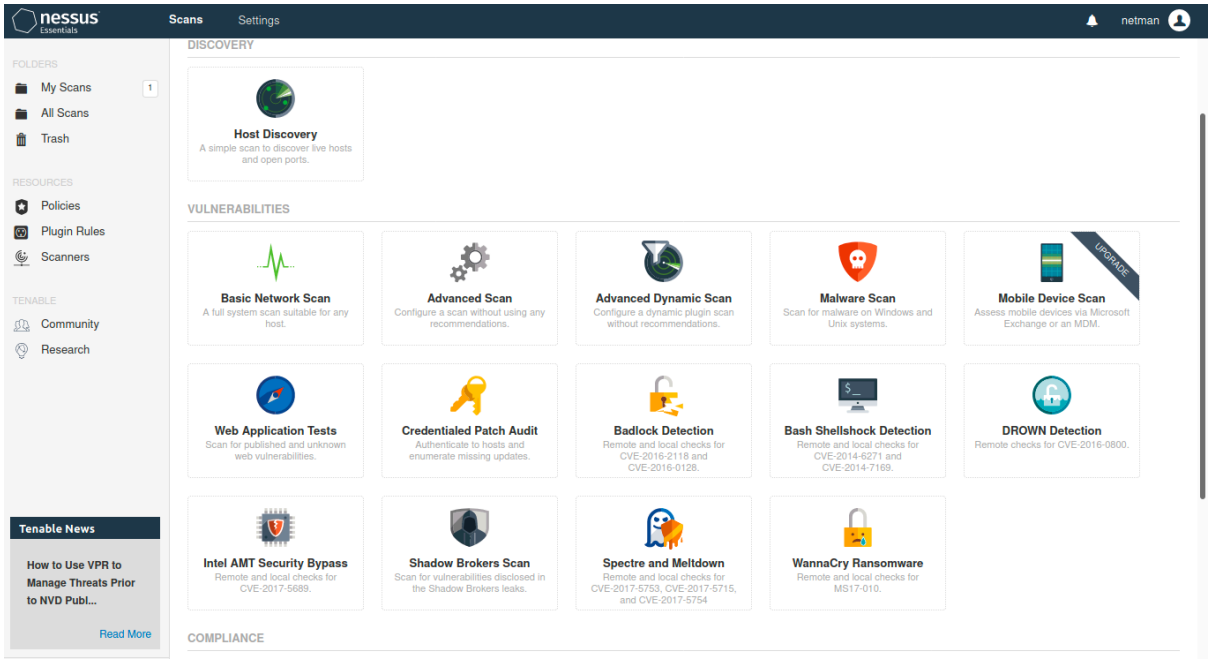
Client to server OSPF security



Vulnerabilities in Router3 eth10, 13.13.13.3



Vulnerabilities in Server 200.200.200.2



Nessus Dashboard

CONCLUSION:

A detailed network management strategy was performed successfully on the required topology. The network plan was successfully implemented with the desired results.

REFERENCES:

- Mani Subramanian. (2010). *Network Management, 2nd Edition*. Pearson Education India.

- Vmware. (2019), SNMPv1, SNMPv2c, and SNMPv3 security, <https://docs.vmware.com/en/VMware-Smart-Assurance/10.1.0/ip-manager-concepts-guide-101/GUID-DD5E42DA-DFCA-4593-A6D8-533B5666A5DE.html>

VIDEO LINK:

https://youtu.be/ap87_ru5Ev4

PRESENTATION LINK:

https://drive.google.com/file/d/11mWcWZ14Sq85OPFL6kJGkRm4Xv6sbcVk/view?usp=sharing