IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 3, Ver. II (May-Jun. 2016), PP 75-88
www.iosrjournals.org

Snmp Implementaton on Hp Routers with Ovpi (Openview Performance Insight) and Network Management

Enis Çerri[1]
[1](*Department of Information Technology / Aleksander Moisiu University of Durres, Albania)*

Abstract: *This study is a practical application of the informatics laboratory applied and gives us the score about how the SNMP protocol is brought together with OVPI (OpenView Performance Insight) in traffic protocol packets within a virtual network. This application was made on the basis of the study made before the Base Station and I have brought a practical applicable version. SNMP is an application-layer protocol of the OSI model that realizes information exchange network management between the NMS (Network Management System), managed agents and equipment. SNMP managed network consists of three main components that are provided: Managed devices, Agents, NMS.*

Keywords: *SNMP, OVPI, network management, NMS.*

I. Introduction

SNMP is an application-layer protocol of the OSI model that realizes information exchange network management between the NMS (Network Management System), managed agents and equipment. It uses TCP / IP as support. There are three types of SNMP: SNMP version 1 (SNMPv1), SNMPv2, SNMPv3.

SNMP managed network consists of three main components that are provided: Managed devices, Agents, NMS (Network Management System) which is also the network management system.

1.1 Materials and Methods

- Equipment managed:

a) Contains an SNMP agent that is within the managed network.
b) Collects and stores management information and makes it available for NMS using SNMP.
c) Includes router, switch, bridge, access servers, hosts, or printers.

- Agents:

It is a software module management network to a device that is manageable. An agent has knowledge of information management and makes it available via SNMP.

- NMS (Network Management Systems):

Implement applications that monitor and control managed devices. It provides the necessary management resources. Some of the applications of NMS are: UCD-SNMP, MRTG, HPOV, CW2000RME.

The following figure illustrates the connections between the three main components of SNMP.

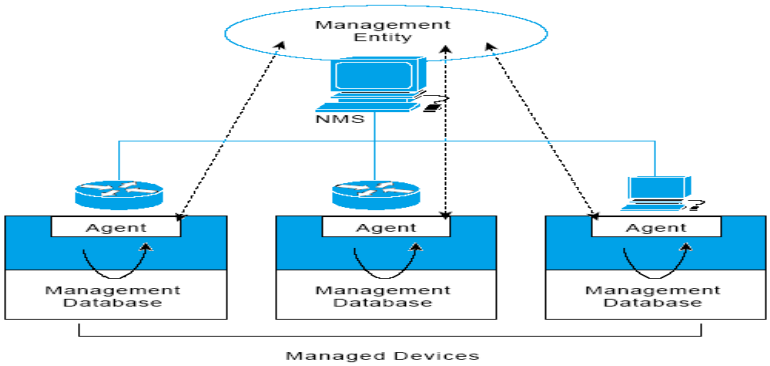


Fig.1 Structure of SNMP

There are three main types of messages in SNMP:

• get - There are several requirements that makes NMS used by it to monitor equipment. NMS examines different variables held by the device to be managed.

• set - there are some commands that sends NMS to manage devices. NMS in this case changing the values of variables that are stored on devices.

• raft - agents kick some messages sent from managed devices which report the event to the NMS. Through these messages in the network operations center NOC informed on events such as:

- Changes the link Up / Down,
- Changes in configuration,
- Temperature verge of equipment,
- CPU Overload.

The figure below shows the interaction between NMS and agents.

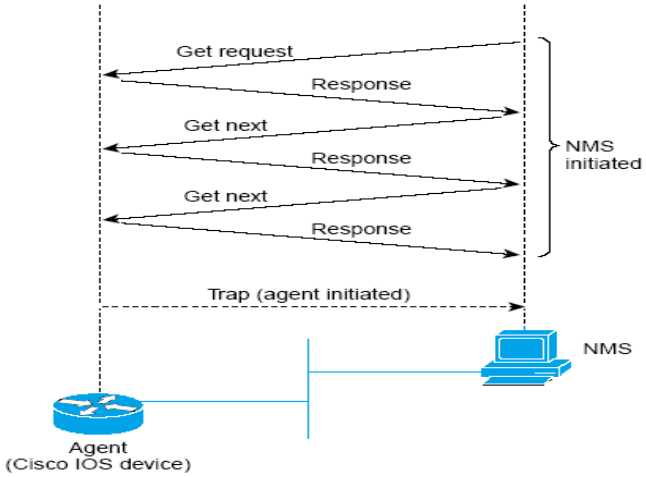


Fig.2 Interaction between the NMS and the agents

1.2 HP OpenView

That is fundamentally a software manufactured by Packard Hewlett company that controls all the nodes of a network that however great. It consists of two main parts provided:

a) NNM (Network Node Manager) that detects all points of the network through a process called Network Discovery Polling and controls the state of the traffic network nodes that runs on them etc.

b) OVPI (Open View Performance Insight) to collect data from NNM and creates some reports that monitors network administrator and others responsible for managing the network.

- NNM (Network Node Manager) MANAGEMENT NETWORK BY NNM

NNM (Network Node Manager) is the essence of any other product to HP Open View, as when installing other products of HP Open View is recognized only as additional features to NNM's. So NNM is the starting point for network management solution. NNM performs these functions are provided:

a) NNM shows the current state of the network, what devices are present, as these devices are configured, as is their performance, not good etc. NNM what makes these through a process called polling is a "poll" that NNM It makes all network devices.

b) NNM helps us to tell us the history of the device. We use these historical data for network analysis.

c) NNM by monitoring the threshold values that put critical equipment allows us to anticipate and prevent various problems in these devices.

Here's how the devices appear maps were discovered by NNM.

There are two versions of NNM provided:

I - First, is NNM Starter Edition (NNM SE) that enables only the detection and monitoring of joints that support third layer protocols.

II - The second is NNM Advanced Edition (NNM AE) discovers and monitors all devices that are in the network.

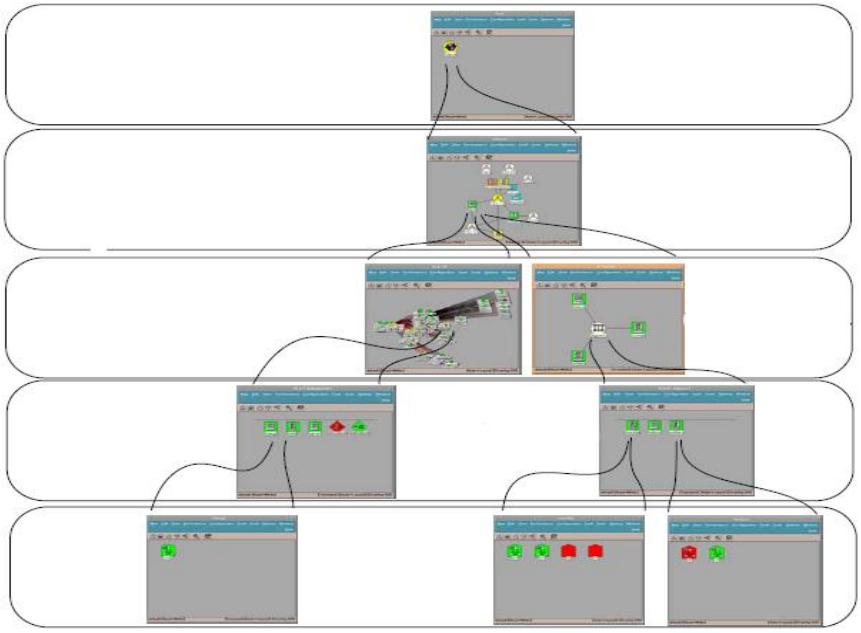


Fig. 3 Maps of equipment discovered by NNM

- OVPI (OpenView Performance Insight)

OVPI is a network management system that performs the following functions:

✓ Collect data
✓ Processes data
✓ Report data

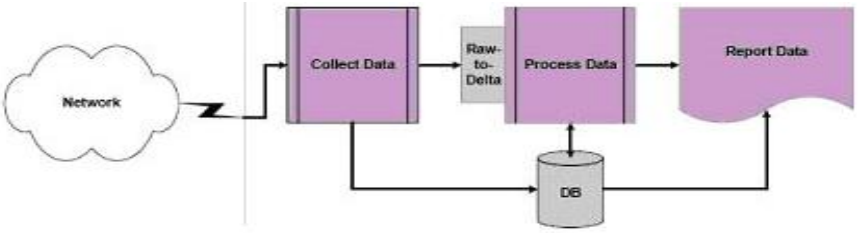


Fig. 4 Functions of OVPI

✓ Data Collection

• Devices that have SNMP (Simple Network Management Protocol)
• OpenView performance agents and operations
• Devices that do not have SNMP

✓ Data Processing:

With the collected data sets system saves time and materials data in the data tables. The system will then convert the raw data in the delta data. Data delta changes between two values.

✓ Reporting data:

Once the data are processed they are ready to produce relevant reports. Reports can be made in two ways:

1) Auto: This mode uses OVPI packages to generate various reports.
2) Manual: In this way we can create specific reports using Report Builder.

Both these ways create some instructions that describe reports. Reports can only be in the following formats:

• Report definition file (.rep)
• Dataset file (.srep)
• Form (.frep)

By installing a package of reports for a particular technology system will be able to create, schedule and generate reports.

• Terms of tables to store data to deal with settlement.
• Information on data collection (including scripts, commands the policies of "polls" etc.).
• Includes a batch of instructions to generate comprehensive data for solving the problem.
• Instructions reports to generate reports.
• Distribution instructions to identify the location of instructions reports.
• Instructions and for programming commands and automatic generation of reports.

II. Some Examples Of Packages Reports

2.1 Cisco ping report pack

Network performance is usually measured by the delay and reliability. If delays are small, then data packets move from source to destination as soon as possible. Many of the packages OVPI reports use a data gathering mechanism of the joints that is built inside the OVPI. While the package of reports of Ping Cisco has its own mechanism of data collection that collects data from some nodes and not just from a node. Before the start of data collection must be defined nodes to be "asked". An example shows how OVPI report shows the figure below.

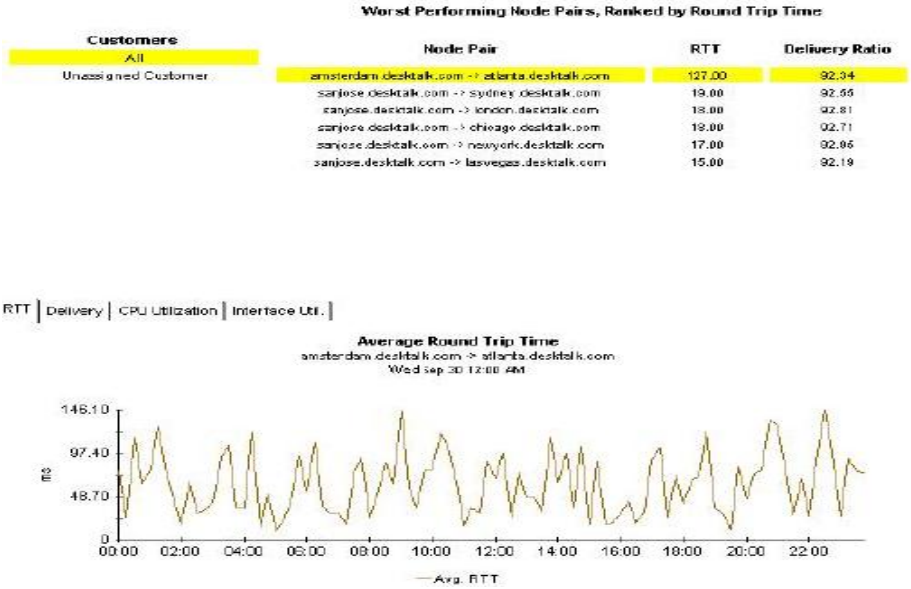


Fig. 5 Cisco Ping Report

Interpretation provided:

The above report shows which nodes in the network have been the most problematic in terms of communication with each other. RTT see what he is and what is the ratio of shipments at any time of day and draw a conclusion on the effectiveness of the joints.

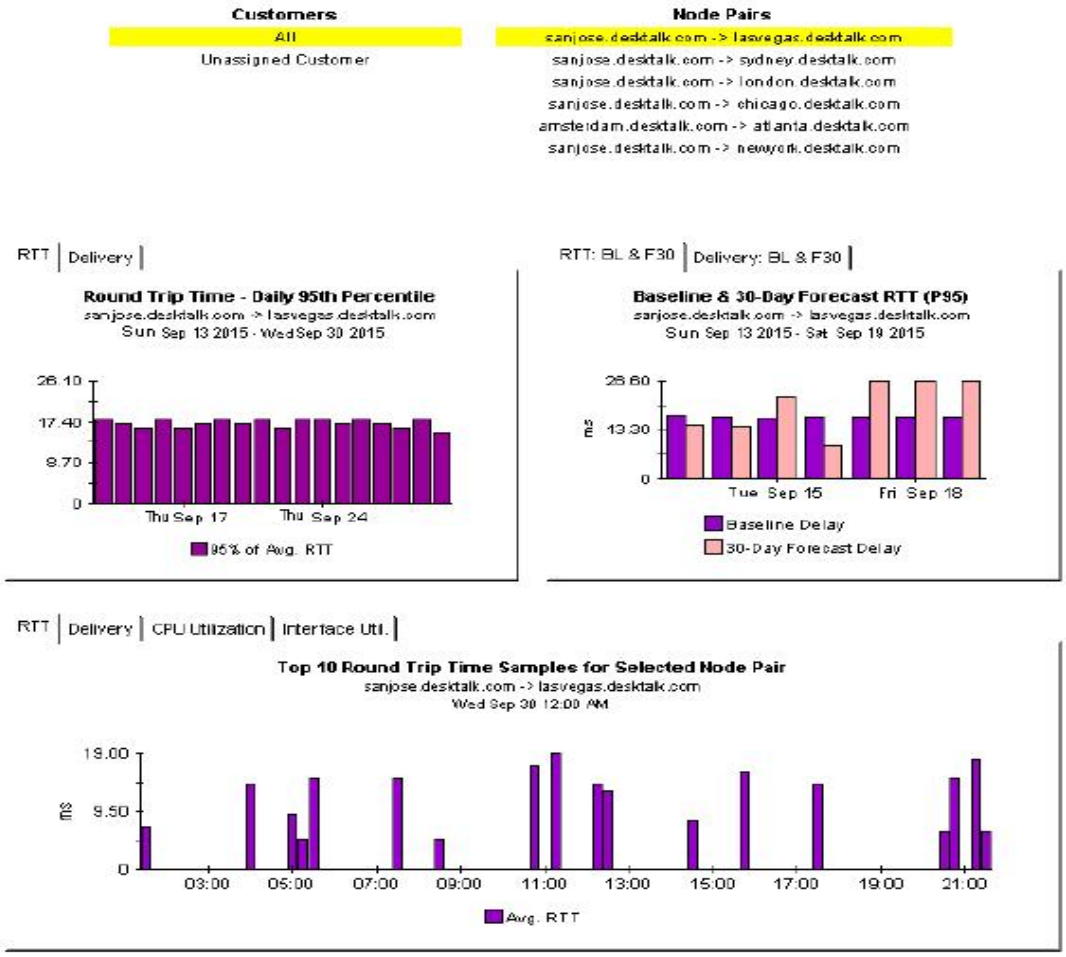


Fig.6 Charts for nodes communication

To see how the chart last two nodes have communicated with each other during a given day. We see the greatest delays have ping about 11:30 am and during most of the time they have been able pause with each other.

2.2 Package reports of device resources

This package installed OVPI. Reports in this package monitor CPU, memory cards that can be installed in equipment etc. Source operates independently. An example of how the show OVPI report shows below. This figure installed OVPI package. It shows statistics for the devices:

• use of CPU,
• use buffer,
• use of memory,
• the volume of traffic on the equipment interface.

Highest Average CPU Utilization
Wed Apr 01 2015

Customer	Average CPU Util	Busy Hour CPU Util
NetRadix	60.94	71.38
Trinagy	59.49	74.75

CPU Utilization Forecast
Sorted by Highest 90 Day Forecasted Value

Customer	Baseline	30th Day	60th Day	90th Day
Trinagy	65.00	67.42	59.59	51.75
NetRadix	84.25	67.49	56.76	50.06

Highest Average Memory Utilization
Wed Apr 01 2015

Customer	Average Memory Util	Busy Hour Memory Util
NetRadix	52.38	81.47
Trinagy	44.37	66.70

Memory Utilization Forecast
Sorted by Highest 90 Day Forecasted Value

Customer	Baseline	30th Day	60th Day	90th Day
NetRadix	89.16	97.16	113.20	129.23
Trinagy	89.42	72.44	67.36	62.28

Highest Average Buffer Utilization
Wed Apr 01 2015

Customer	Average Buffer Util	Busy Hour Buffer Util
NetRadix	96.53	97.47
Trinagy	96.12	96.46

Buffer Utilization Forecast
Sorted by Highest 90 Day Forecasted Value

Customer	Baseline	30th Day	60th Day	90th Day
NetRadix	97.58	97.38	97.56	97.74
Trinagy	96.00	95.96	94.91	93.86

Fig. 7 Report of the device resource

Interpretation provided:

This report shows the use of all resources of the network devices such as CPU, memory etc. In this example shown 10 users who use more resources and equipment. For instance, we see greater use of CPU has NetRadix firm that has average daily CPU utilization around 60%. While use in load hours amounts to about 75%. We see that the use of higher memory has but this firm, which reaches 81.5% in the hours under load. While use of the buffer amounts to 97.5% in the hours under load. While below we see that the average data are provided for the equipment and not to users.

Customer	Average CPU Util	Average Memory Util	Average Buffer Util
Trinagy	59.49	44.37	96.12
NetRadix	60.94	52.38	96.53

Highest Average CPU Utilization
Wed Apr 01 2015

Device	Average CPU Util	Busy Hour CPU Util
Cisco_01	62.29	74.75
Cisco_02	56.70	75.50

CPU Utilization Forecast
Sorted by Highest 90 Day Forecasted Value

Device	Baseline	30th Day	60th Day	90th Day
Cisco_02	90.00	79.33	76.60	73.67
Cisco_01	90.25	70.61	62.01	53.42

Highest Average Memory Utilization
Wed Apr 01 2015

Device	Average Memory Util	Busy Hour Memory Util
Cisco_01	55.16	90.34
Cisco_02	33.57	62.22

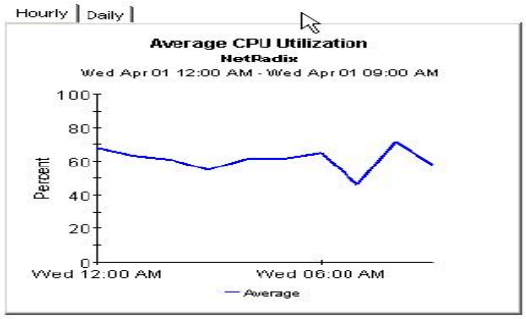
Memory Utilization Forecast
Sorted by Highest 90 Day Forecasted Value

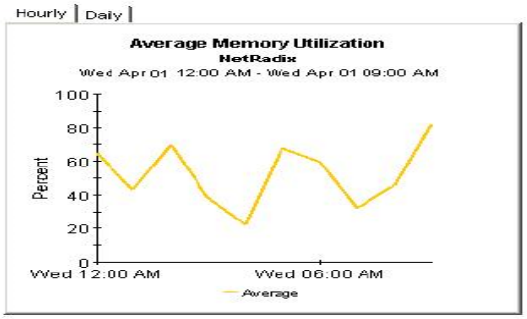
Device	Baseline	30th Day	60th Day	90th Day
Cisco_01	90.41	99.02	108.60	114.56
Cisco_02	98.35	75.41	67.16	57.90

Fig. 8 Report the average data provided for the equipment.

As the charts below show the CPU or memory usage by the user during a full day. From this report we draw what are the peak traffic hours, in order to take measures to prevent any possible failure due to overload of device resources.

Customer	Total Exceptions	CPU Util Exceptions	Memory Util Exceptions	Buffer Util Exceptions
NetRadix	46	4	4	38
Trinagy	44	2	4	38





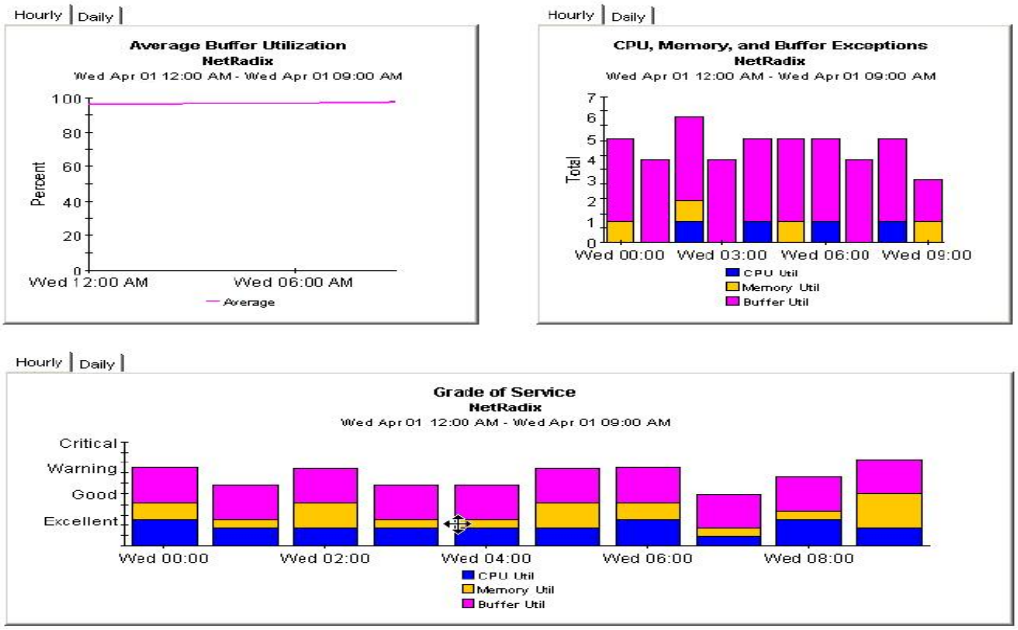


Fig. 9 Report the CPU or memory usage by the user during a day.

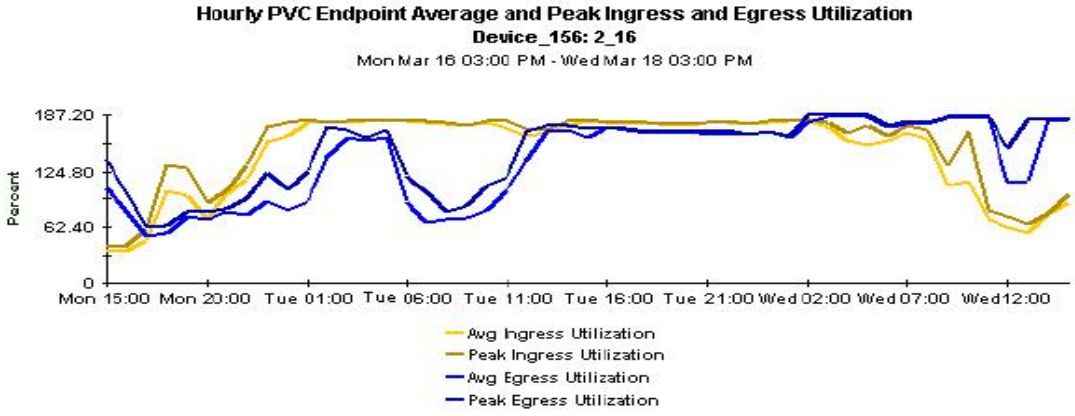
2.3 Frame Relay Package reports

Frame Relay networks eliminate error control (error) of the link layer being given responsibility for retransmission of packets protocols at higher levels. To avoid overloading the network Frame Relay network nodes send signals to control flow through neighboring nodes. If you can not prevent network overload alarms via node changes the status of DE (Discard-Eligibility) for different frames. Raports located at the gates folder display data for logical port located on the device, which usually corresponds to the entrances tables of MIB-II. Reports in this folder provide the following statistics provided:

• the use of inputs and outputs;
• number of frames transmitted and the number of frames received;
• the number of octets sent and received number of octets;
• number of frames of "discarded".

Reports in the folder PVC (Permanent Virtual Circuit) display the following statistics:

• use input and output sources;
• number of frame-burst committed;
• the number of excess-burst frame;
• frame Number DE (Discard Eligible);
• number of frames that show overflow in the forward direction;
• number of frames that show overflow towards back.



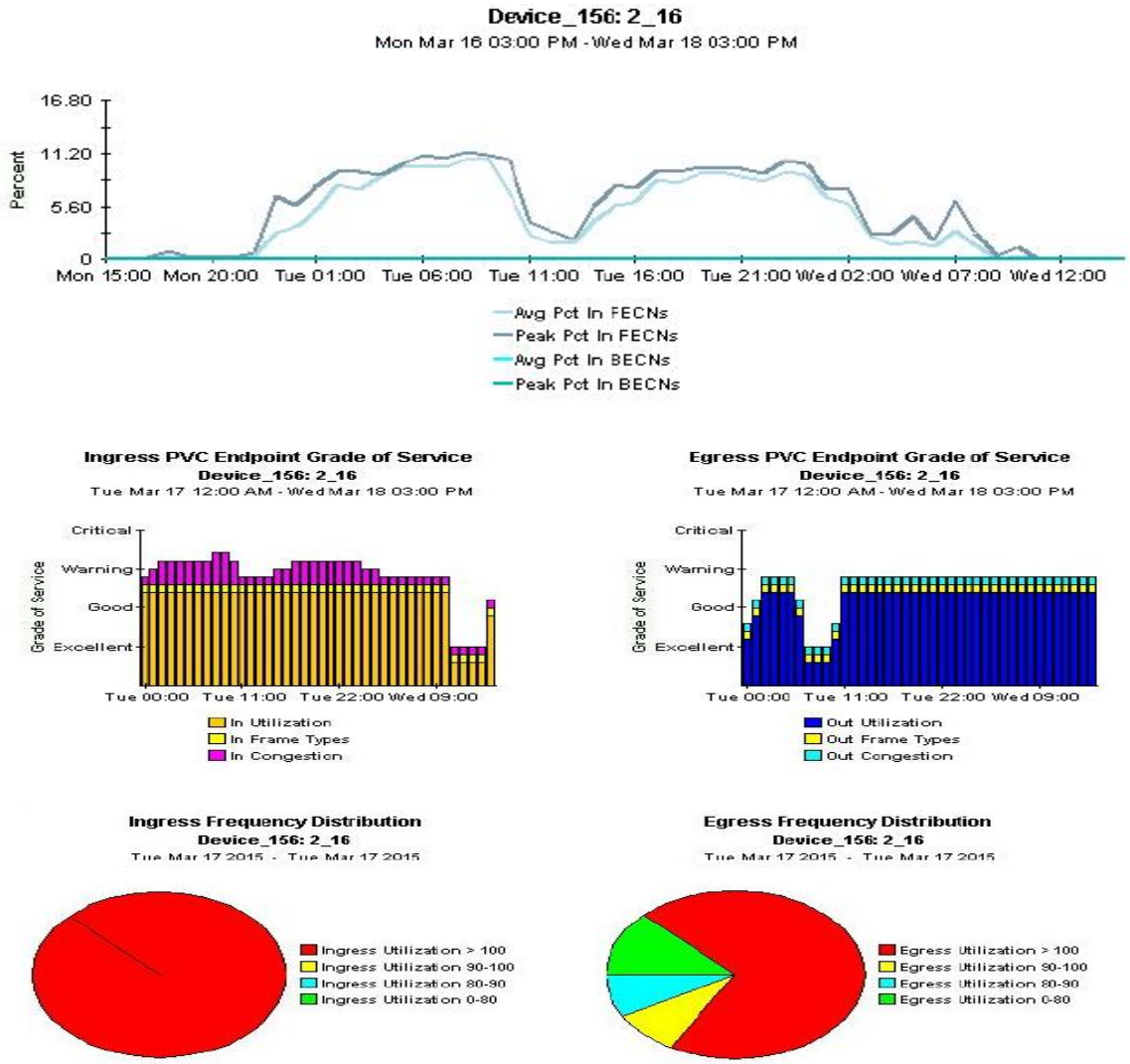


Fig. 10 Report Frame Relays services

Interpretation provided:

The following report shows all statistical data such as a PVC. CIR, the use of inputs, use of outflows cast frame number of cases of overload that occurred at the entrance or exit and these appear with the corresponding graphs. By studying these charts we draw conclusions for peak times of overload. For examle for device 158 having overload time worrying entrance is 10am. While the overloaded output is almost constant peak value during the day but still is not as disturbing as input overload.

2.4 Interface Package reports

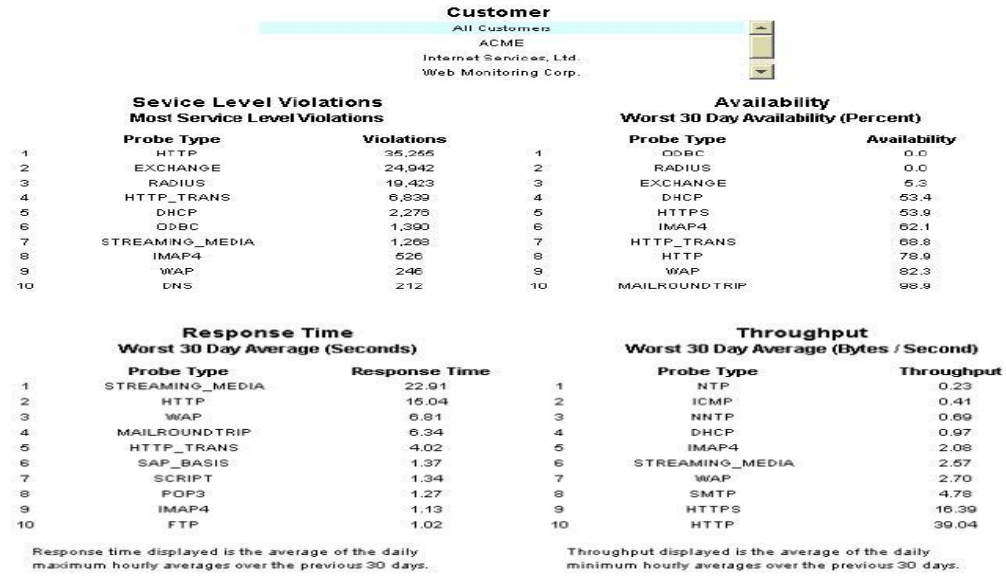
Reporting on the interface helps to maintain service levels, to determine the capacity to solve problems before they become serious.

2.5 Package reports of access speeds of IP

This pack monitors the performance of the interface configured with RLO. This package is used to identify interface with high traffic report filter. A RLO is one rule for one-way traffic. If a byte or a package exceeding a limit that would "collapse" in the interface, then filtered. If this traffic report filter is high and such is the level of service it is not appropriate for the client. An example of how show the OVPI report shows the figure below.

2.6 The package of Internet service reports

Packs of internet service reports give detailed information about the services that are critical to a business. This service pack allows distributors to monitor services to solve problems and predict how performance will be in the future. An example of how show the OVPI report shows the figure below.



Customer

All Customers
ACME
Internet Services, Ltd.
Web Monitoring Corp.

Sevice Level Violations
Most Service Level Violations

	Probe Type	Violations
1	HTTP	35,255
2	EXCHANGE	24,942
3	RADIUS	19,423
4	HTTP_TRANS	6,839
5	DHCP	2,276
6	ODBC	1,390
7	STREAMING_MEDIA	1,268
8	IMAP4	526
9	WAP	246
10	DNS	212

Availability
Worst 30 Day Availability (Percent)

	Probe Type	Availability
1	ODBC	0.0
2	RADIUS	0.0
3	EXCHANGE	5.3
4	DHCP	53.4
5	HTTPS	53.9
6	IMAP4	62.1
7	HTTP_TRANS	68.8
8	HTTP	78.9
9	WAP	82.3
10	MAILROUNDTRIP	98.9

Response Time
Worst 30 Day Average (Seconds)

	Probe Type	Response Time
1	STREAMING_MEDIA	22.91
2	HTTP	15.04
3	WAP	6.81
4	MAILROUNDTRIP	6.34
5	HTTP_TRANS	4.02
6	SAP_BASIS	1.37
7	SCRIPT	1.34
8	POP3	1.27
9	IMAP4	1.13
10	FTP	1.02

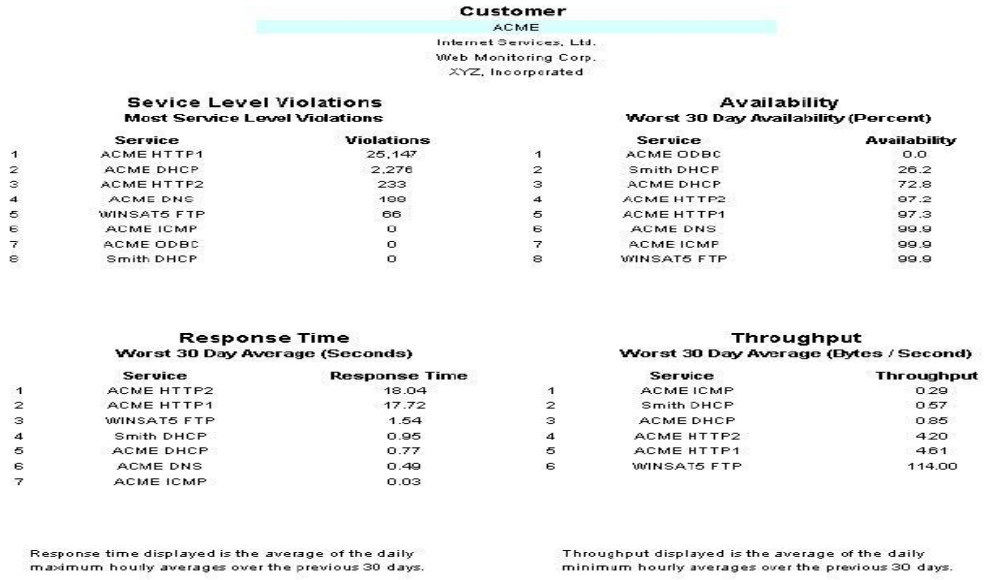
Response time displayed is the average of the daily maximum hourly averages over the previous 30 days.

Throughput
Worst 30 Day Average (Bytes / Second)

	Probe Type	Throughput
1	NTP	0.23
2	ICMP	0.41
3	NNTP	0.69
4	DHCP	0.97
5	IMAP4	2.08
6	STREAMING_MEDIA	2.57
7	WAP	2.70
8	SMTP	4.78
9	HTTPS	16.39
10	HTTP	39.04

Throughput displayed is the average of the daily minimum hourly averages over the previous 30 days.

Fig. 11 Report all customer of the internet services



Customer

ACME
Internet Services, Ltd.
Web Monitoring Corp.
XYZ, Incorporated

Sevice Level Violations
Most Service Level Violations

	Service	Violations
1	ACME HTTP1	25,147
2	ACME DHCP	2,276
3	ACME HTTP2	233
4	ACME DNS	199
5	WINSAT5 FTP	66
6	ACME ICMP	0
7	ACME ODBC	0
8	Smith DHCP	0

Availability
Worst 30 Day Availability (Percent)

	Service	Availability
1	ACME ODBC	0.0
2	Smith DHCP	26.2
3	ACME DHCP	72.8
4	ACME HTTP2	97.2
5	ACME HTTP1	97.3
6	ACME DNS	99.9
7	ACME ICMP	99.9
8	WINSAT5 FTP	99.9

Response Time
Worst 30 Day Average (Seconds)

	Service	Response Time
1	ACME HTTP2	18.04
2	ACME HTTP1	17.72
3	WINSAT5 FTP	1.54
4	Smith DHCP	0.95
5	ACME DHCP	0.77
6	ACME DNS	0.49
7	ACME ICMP	0.03

Response time displayed is the average of the daily maximum hourly averages over the previous 30 days.

Throughput
Worst 30 Day Average (Bytes / Second)

	Service	Throughput
1	ACME ICMP	0.29
2	Smith DHCP	0.57
3	ACME DHCP	0.85
4	ACME HTTP2	4.20
5	ACME HTTP1	4.61
6	WINSAT5 FTP	114.00

Throughput displayed is the average of the daily minimum hourly averages over the previous 30 days.

Fig. 12 Report identify interface with high traffic report filter of the internet services

Interpretation provided:

Internet service report gives us a clear view of all services offered as well as statistical data for these services as such availability, where we see the most available have been Winstat5 FTP, DNS ACME, ACME ICMP. Recently responses provided these services where Speedy is ACME ICMP. Given the average values lower speeds of days that are kept under surveillance.

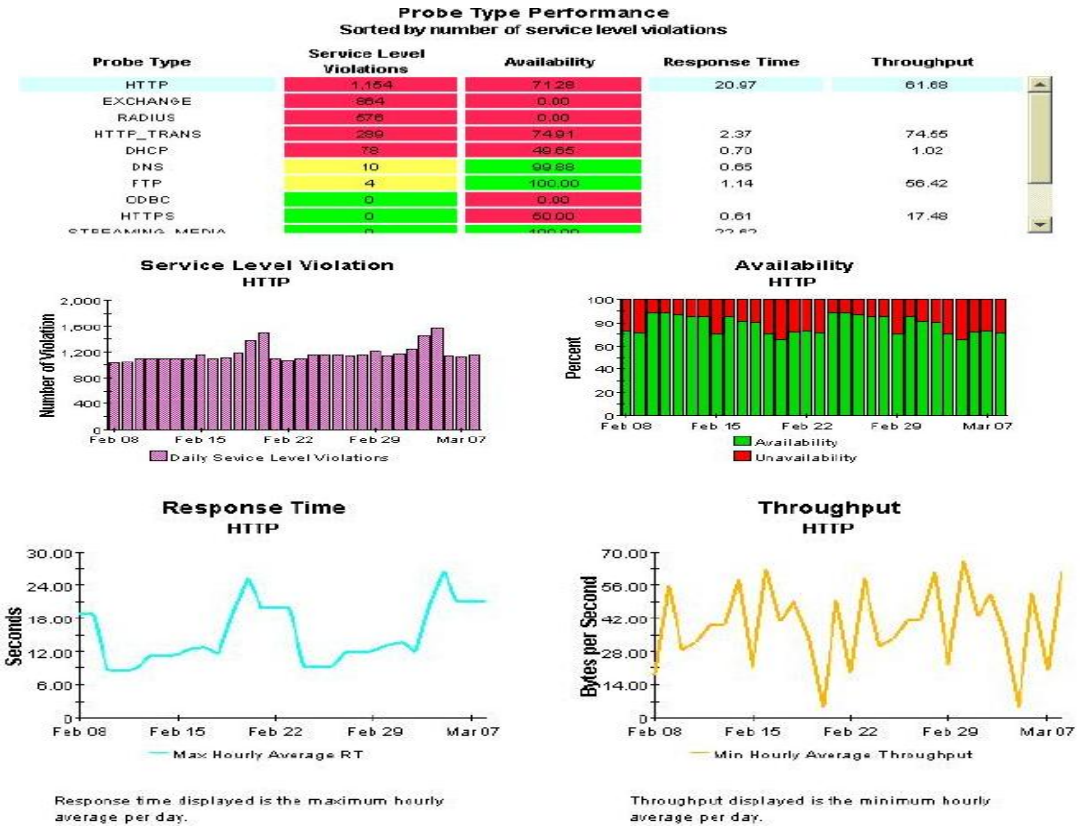


Fig. 13 Report of the internet services

2.7 The package reports of IP QoS Statistics

QoS (Quality of Service) is the ability of each node to give priority to the processing of high priority traffic to the detriment of that low priority. QoS provides the following benefits:

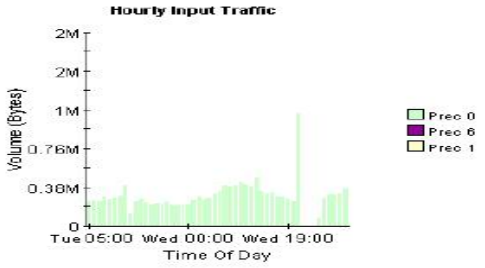
- greater bandwidth for specific types of traffic,
- problems of traffic delays can be controlled,
- loss characteristics can be improved.

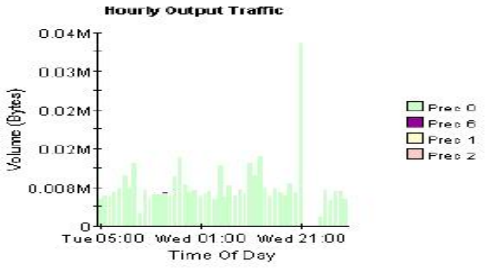
QoS can be implemented by configuring a router interface to check-in the second byte in the IP packet header. Three bits of the first byte indicate the level of priority. Level Lowest priority is 0 while the highest is 7. An example of how show the OVPI report shows the figure below.

IP QoS Statistics Interfaces

Active Interfaces With IP QoS Statistics Data Over Previous 6 Hours

Customer	Device	Interface	ifSpeed	Location	Admin Status	Switched Pkts	Switched Bytes
Customer Unassigned	65.212.180.1	FastEthernet0/0	100 Mb/s	Location Unassigned	Up	11,964	1,891,336





Rate Input | Rate Output

Polled IP QoS Statistics Data - Input

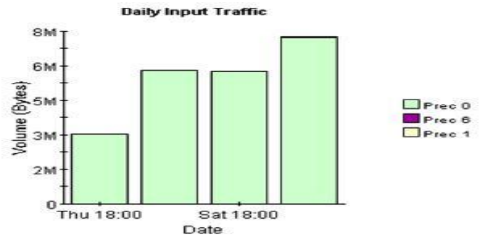
Over Previous 6 Hours

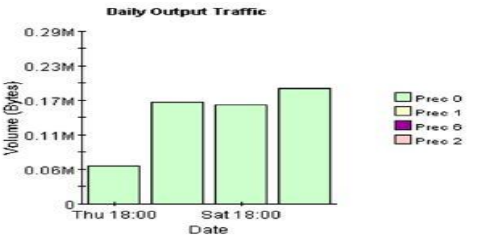
Direction	IpPrecedence	Switched Bytes	Switched Pkts	Time Period
Input	0	105,688	675	Thu Oct 29 07:00 AM
Input	1	0	0	Thu Oct 29 07:00 AM
Input	2	0	0	Thu Oct 29 07:00 AM
Input	3	0	0	Thu Oct 29 07:00 AM
Input	4	0	0	Thu Oct 29 07:00 AM
Input	5	0	0	Thu Oct 29 07:00 AM
Input	6	600	5	Thu Oct 29 07:00 AM
Input	7	0	0	Thu Oct 29 07:00 AM
Input	0	98,334	638	Thu Oct 29 06:45 AM

IP QoS Statistics Interfaces

Active Interfaces With IP QoS Statistics Data Over Previous 6 Hours

Customer	Device	Interface	ifSpeed	Location	Admin Status
Customer Unassigned	65.212.180.1	FastEthernet0/0	100 Mb/s	Location Unassigned	Up





Hourly | Daily | Monthly

Hourly Aggregate Data for 65.212.180.1: FastEthernet0/0

Time Period	0 In	1 In	2 In	3 In	4 In	5 In	6 In	7 In	0 Out	1 Out	2 Out	3 Out	4 Out	5 Out	6 Out	7 Out
Thu Oct 29 06:00 AM	390,392	0	0	0	0	0	120	0	5,512	0	0	0	0	0	0	0
Thu Oct 29 05:00 AM	335,655	0	0	0	0	0	720	0	7,061	0	0	0	0	0	102	0
Thu Oct 29 04:00 AM	324,204	0	0	0	0	0	283	0	7,249	0	0	0	0	0	0	0
Thu Oct 29 03:00 AM	331,896	0	0	0	0	0	480	0	5,428	0	0	0	0	0	0	0
Thu Oct 29 02:00 AM	285,461	0	0	0	0	0	830	0	7,323	0	0	0	0	0	0	0
Thu Oct 29 01:00 AM	78,642	0	0	0	0	0	0	0	1,794	0	0	0	0	0	0	0
Wed Oct 28 09:00 PM	1,154,381	0	0	0	0	0	12,430	0	37,884	0	0	0	0	0	119	0
Wed Oct 28 08:00 PM	261,345	0	0	0	0	0	120	0	7,026	0	0	0	0	0	0	0
Wed Oct 28 07:00 PM	280,334	0	0	0	0	0	523	0	8,799	0	0	0	0	0	0	0
Wed Oct 28 06:00 PM	292,606	0	0	0	0	0	120	0	6,446	0	0	0	0	0	0	0
Wed Oct 28 05:00 PM	295,977	0	0	0	0	0	728	0	6,911	0	0	0	0	0	0	0
Wed Oct 28 04:00 PM	344,292	0	0	0	0	0	744	0	7,885	0	0	0	0	0	0	0
Wed Oct 28 03:00 PM	333,442	50	0	0	0	0	512	0	6,194	0	0	0	0	0	0	0
Wed Oct 28 02:00 PM	356,423	0	0	0	0	0	0	0	8,091	0	0	0	0	0	0	0
Wed Oct 28 01:00 PM	504,321	0	0	0	0	0	643	0	14,316	0	0	0	0	0	0	0
Wed Oct 28 12:00 PM	408,226	0	0	0	0	0	240	0	10,379	120	0	0	0	0	0	0

Fig. 14 Report QoS Statistics

Interpretation provided:

65.212.180.1 we see that the device is an interface FastEthernet0 / 0 is given speed 100 Mbps administrative and her condition is active. The protocol that uses Ethernet-osmacd. We also see that the peak of incoming and outgoing traffic has around 19:30, where the input goes around 1MB and outgoing traffic goes 0.04 MB.

III. Conclusion

SNMP is an application-layer protocol of the OSI model that realizes information exchange network management between the NMS (Network Management System), managed agents and equipment.
SNMP managed network consists of three main components that are provided:

- managed devices,
- agents,
- NMS (Network Management System) which is also the network management system.

There are three main types of messages in SNMP:

• get - There are several requirements that makes NMS used by it to monitor equipment. NMS examines different variables held by the device to be managed.
• set - There are some commands that sends NMS to manage devices. NMS in this case changing the values of variables that are stored on devices.
• raft - Agents kick some messages sent from managed devices which report the event to the NMS. Through these messages in the network operations center NOC informed on events such as:

- changes the link Up / Down,
- changes in configuration,
- temperature verge of equipment,
- CPU Overload.

MIB (Management Information Base) is an information base for network management and performs these functions are provided:

- Give a summary of the information hierarchically
- Accessible only by a network management protocol such as SNMP.
- Addresses of managed objects and object identifiers.

HP Openview is a software produced by Packard Hewlett company that controls all the nodes of a network that however great. It consists of two main parts provided:

1. NNM (Network Node Manager) that detects all points of the network through a process called Network Discovery Polling and controls the state of the traffic network nodes that runs on them etc.

2. OVPI (Open View Performance Insight) to collect data from NNM and creates some reports that monitors network administrator and others responsible for managing the network.

- NNM (Network Node Manager) is the essence of any other product to HP Open View, as when installing other products of HP Open View is recognized only as additional features to NNM's. So NNM is the starting point for network management solution. NNM performs these functions are provided:

a) NNM shows the current state of the network, what devices are present, as these devices are configured, as is their performance, not good etc. NNM what makes these through a process called polling is a "poll" that NNM It makes all network devices.
b) NNM helps us to tell us the history of the device. We use these historical data for network analysis.
c) NNM by monitoring the threshold values that put critical equipment allows us to anticipate and prevent various problems in these devices.

- OVPI is a network management system that performs the following functions:

• Collect data
• Processes data
• Report data

References

[1] M Ozaki, Y. Adachi, Y. Iwahori, and N. Ishii, Application of fuzzy theory to writer recognition of Chinese characters, *International Journal of Modelling and Simulation, 18(2),* 1998, 112-116.
[2] R.E. Moore, *Interval analysis* (Englewood Cliffs, NJ: Prentice-Hall, 1966).
[3] P.O. Bishop, Neurophysiology of binocular vision, in J.Houseman (Ed.), *Handbook of physiology,* 4 (New York: Springer-Verlag, 1970) 342-366.
[4] D.S. Chan, *Theory and implementation of multidimensional discrete systems for signal processing*, doctoral diss., Massachusetts Institute of Technology, Cambridge, MA, 1978.
[5] W.J. Book, Modelling design and control of flexible manipulator arms: A tutorial review, *Proc. 29th IEEE Conf. on Decision and Control*, San Francisco, CA, 1990, 500-506