



No.D2/ BB / O&M / 2010-11 / 71 Dated at Ch-8 the 17.3.2011

To
The Head of SSAs
BSNL,
Tamilnadu Circle.

Sub: Detailed procedure for Monitoring GE port of DSLAM/OCLANand RPR monitoring.

Several requests are coming from the node in charges regarding the Band Width utilisation of the universities connected under NMEICT Project.

Detailed procedure for monitoring the GE port of DSLAM/OCLAN.and RPR using private software is annexed,which may be used, till such time M/s UTStarcom provides a permanent one for BSNL.

The instructions given over through the attachment may please be followed.

For any additional clarification please contact the officers furnished below.

Shri. Ramakrishna SDE / NOC Mobile No. 09448388100

Shri. Sateesh JTO / NOC Mobile No. 09449011784

signed

R. Babu Srinivasa Kumar
Deputy General Manager (Tx)
BSNL, Chennai – 600 008.

Procedure to monitor traffic through PRTG

1. Download PRTG Network Monitor software from Internet and install in the PC**.
2. Open PRTG Network Monitor and create a Group

Creating Groups

To create new groups go to the devices list ("Devices" under the main menu) and either choose a probe or group that is intended to contain the new group. Right click the object and then choose "Add Group" from the context Enter a name for the new group and then click "Continue".

Add Group to Group "Group 1"

Group Name and Tags	
Group Name:	<input type="text" value="Group 5"/> : The name of the Group.
Tags	<input type="text"/> : Enter a list of comma separated tags (case insensitive) for filtering purposes
<input checked="" type="checkbox"/> Inherit Credentials for Windows Systems from parent object (Group) (Domain or Computer Name: <empty>, Username: <empty>)	
<input checked="" type="checkbox"/> Inherit Credentials for SNMP Devices from parent object (Group) (SNMP Version: V1, SNMP Port: 161, SNMP Timeout (s): 5s)	
<input type="button" value="Continue >"/> <input type="button" value="Cancel"/>	

3. Create a Device

Creating Devices

To create a new device, right-click a device and select "Add Device" from the context menu. There are two settings that you must enter for a device: The name and the IP address. Enter Device name and particular Network element IP address (DSLAM/OCLAN IP) in the corresponding column.

Add Device to Group "Group 1"

Device Name and Address	
Device Name	<input type="text" value="Device 6"/> : Choose a new name of your choice to describe the device
Ip-Address/DNS Name:	<input type="text"/> : Enter a DNS name (e.g. "server.mycompany.com") or the IP address (e.g. "10.0.0.15")
Tags	<input type="text"/> : Tags are keywords or descriptive terms associated with an object as means of classification.
Device Type	
Sensor Management	<input checked="" type="radio"/> Manual (No Autodiscovery) : Choose the "Manual" option if you want to create and manage sensors manually. The other settings will scan your network for available sensors and create the appropriate sensors. "Automatic Device Identification" is mainly based on PING, SNMP and WMI. It should only be used in LANs and is not suitable for WAN connections. <input type="radio"/> Automatic Device Identification (Standard, recommended) <input type="radio"/> Automatic Device Identification (Detailed, may create many sensors) <input type="radio"/> Automatic Sensor Creation with specific Device Template(s)
<input checked="" type="checkbox"/> Inherit Credentials for Windows Systems from parent object (Group) (Domain or Computer Name: <empty>, Username: <empty>)	
<input checked="" type="checkbox"/> Inherit Credentials for SNMP Devices from parent object (Group) (SNMP Version: V1, SNMP Port: 161, SNMP Timeout (s): 5s)	
<input type="button" value="Continue >"/> <input type="button" value="Cancel"/>	

Click on **Inherit Credentials for SNMP Devices** change the Community string if necessary (NSN ZTE DSLAMs and OCLANs it is “**public**”) and then click "Continue"

Inherit Credentials for VMware/XEN Servers from 1st group (visible to all user accounts) (User: <empty>)

Inherit Credentials for SNMP Devices from 1st group (visible to all user accounts) (SNMP Version: V1, SNMP Port: 161, SNMP Timeou...)

SNMP Version

- v1
- v2c
- v3

Community String

public

SNMP Port

161

SNMP Timeout (sec)

5

Depending on the target device you can use advanced features if you select SNMP V2c or SNMP V3. Standard is SNMP V1. Use SNMP V2c for 64bit counters and SNMP V3 if you want secure authentication and SNMP data encryption

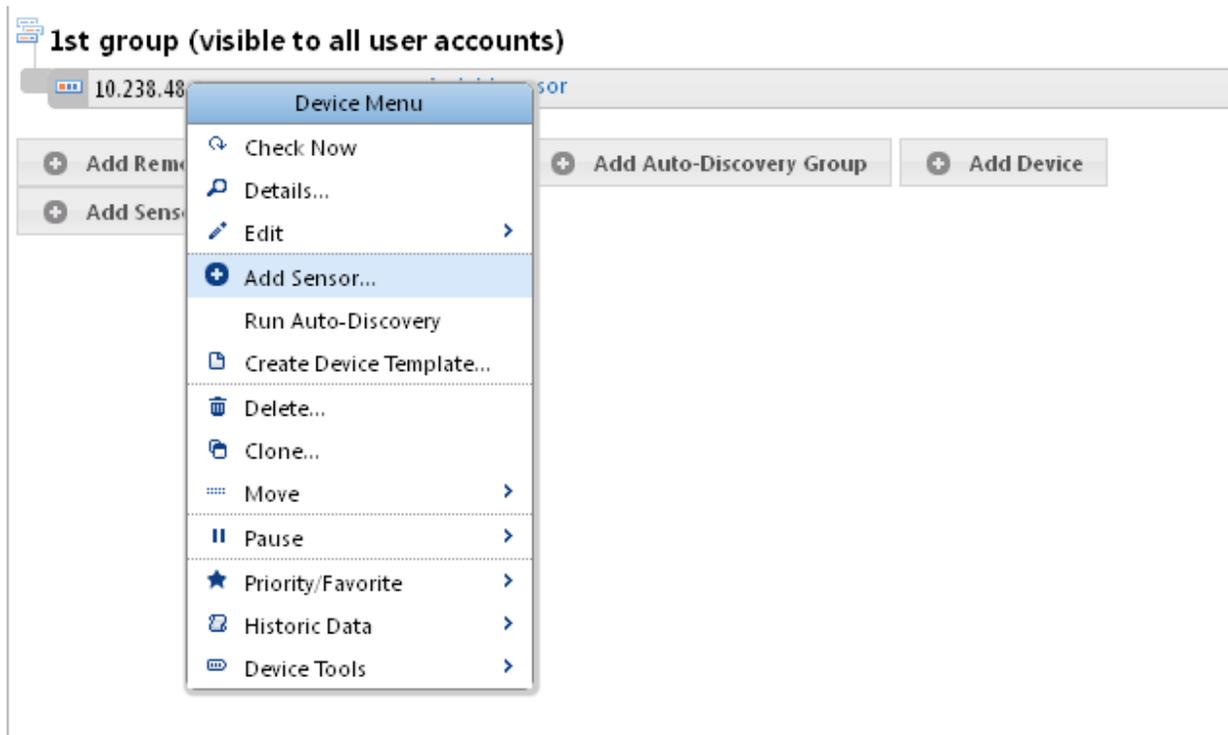
The device's community string. Standard is 'public'.

The device's SNMP port. Standard is '161'.

If the reply takes longer than this value the request is aborted and you get an error message. If two consecutive requests fail (for whatever reason) the sensor enters a

4. Add Sensors to the Device (add DSLAM/OCLAN port)

In order to add new sensors, right-click on the device where the new sensor is to be added and choose "Add Sensor" from the context menu.



Then click on SNMP Icon



Add Sensor to Device 10.238.48.1 [10.248.48.1] (Step 1 of 2)

Search Enter a search string: <input type="text"/>	Your Top 10 Sensors The sensor types you are using the most	Common Sensors Most common sensor types for network monitoring	Bandwidth Monitoring SNMP, Packet Sniffing, NetFlow, sFlow, WMI
Web Servers (HTTP) HTTP, HTTPS, Transaction, Full Page	SNMP Devices that support the Simple Network Management Protocol	Windows/WMI Windows Management Instrumentation for Windows computers	Linux/Unix/OS X SSH, SNMP, WBEM
Virtual Servers VMWare, Hyper-V, XEN, Amazon EC2	Mail Servers SMTP, POP3, IMAP, Exchange, Round-Trip	SQL Servers MySQL, Microsoft SQL, Oracle SQL, ADO	File Servers Shares, Files, Folders, Disk Space, FTP
Various Servers PING, PORT, FTP, DNS, RDP, Syslog, Traps, Radius, NTP	VoIP and QoS VoIP, QoS, IP-SLA	Custom Sensors Define your own sensor scripts	All Sensors A complete list of all sensors

< Cancel sensor creation Haven't found what you need? [Find more custom sensors online](#) or [send your feedback to Paessler!](#)

Click on SNMP Traffic .



Add Sensor to Device 10.238.48.1 [10.248.48.1] (Step 1 of 2)

SNMP	
Devices that support the Simple Network Management Protocol	
SNMP Linux Load Average	Monitors System Load average of a Linux/Unix system using SNMP
SNMP Linux Meminfo	Monitors memory usage of a Linux/Unix system using SNMP
SNMP Linux Disk Free	Monitors free space on disks of a Linux/Unix system using SNMP
SNMP Traffic	Monitors bandwidth and traffic on servers, PCs, switches, etc. using SNMP
SNMP Library	Monitors a device using SNMP and compiled MIB files ("SNMP Libraries")
SNMP Uptime	Monitors the uptime of a device using SNMP
SNMP Custom	Monitors a numerical value returned by a specific OID using SNMP
SNMP Custom String	Monitors a string returned by a specific OID using SNMP
SNMP Trap Receiver	Receives and analyzes SNMP Traps This sensor type is only available for probe devices!

After sensor preparation it will be giving all the ports in the particular Network elements.

5. Select particular port which is to be monitored and click "Continue"

Select all connected interfaces	Select all disconnected interfaces	Deselect all interfaces				
	Name	Status	Speed	Type	64bit	Internal name
<input type="checkbox"/>	(001) Siemens-hiX5625-CXUC2GE:4	Connected	1 GBit/s	Ethernet	No	
<input type="checkbox"/>	(002) Siemens-hiX5625-CXUC2GE:4	Connected	1 GBit/s	Ethernet	No	
<input type="checkbox"/>	(003) Siemens-hiX5625-CXUC2GE:4	Not Connected	0 KBit/s	Ethernet	No	
<input type="checkbox"/>	(004) Siemens-hiX5625-CXUC2GE:4	Not Connected	0 KBit/s	Ethernet	No	
<input type="checkbox"/>	(021) Siemens-hiX5635-CXUGE:4E	Undefined		(not defined)	No	
<input type="checkbox"/>	(022) Siemens-hiX5635-CXUGE:4E	Undefined		(not defined)	No	
<input type="checkbox"/>	(272) Siemens-hiX5625-IUADSL:72A	Undefined		(not defined)	No	

Additional Channels

- Errors In & Out
- Discards In & Out
- Unicast Packets In & Out
- Non Unicast Packets In & Out (32bit only)
- Multicast Packets In & Out (64bit only)
- Broadcast Packets In & Out (64bit only)
- Unknown Protocols

Connection State Handling

- Show alarm when disconnected (recommended)
- Ignore interface when disconnected

Description "IN" Channel: Traffic In

Description "OUT" Channel: Traffic Out

Description "TOTAL" Channel: Traffic Total

Select channels to monitor additionally to "Traffic In" & "Traffic Out". Note: Channels enabled once will remain visible when disabled (only monitoring will be stopped). Use the "Channels" tab to hide the channels.

Choose how a disconnected interface (eg. cable is unplugged) will be handled.

Inherit Scanning Interval from 10.224.178.16 (Scanning Interval: 60 seconds)

It will open the graph page and there you can select different tabs like Overview, Live Data, etc. Live Data will give the live graph for the particular selected port.

**Note: PC should have access to the particular Network element (DSLAM/OCLAN)