**CN8861 Lab 1**

(Due June 9th, 2013)

1. The objective of this exercise is to identify relevant MIBs and object instances, read MIB files, navigate MIB objects using a MIB browser, issuing SNMP protocol requests, enabling traps on Cisco devices, and understanding the SMI. It is expected that you explore MIBs supported in the Cisco Routers/Switches in selected PODs (3, 6, or 24). Use SNMP command-lines or a MIB browser (available on the HP NNMi) to retrieve managed object instances.

Enable SNMP agent on the Cisco IOS and on the Windows Server. Setup read-only and read-write community strings.

1. Compile network inventory information (for your POD) by SNMP querying devices on your network. The Inventory information of interest to us include:

a) System Object Identifier

b) System name and description

c) Interfaces, types, speed and IP Addresses

1. Choose a network element and perform the following:
2. Set ‘System Contact’ and ‘System Object Identifier’ to new values. Verify if updates are successful. If not, explain why.
3. Find supported MIBs using SNMP. Classify the MIBs into IETF standard MIBs and Vendor Proprietary MIBs.
4. Enable the authentication failure trap on the network element. Generate an “authentication failure” trap is generated.
5. Retrieve SNMP traffic statistics on the network element

**Deliverable**: Document or save the screen shots of the output.

1. During SNMP device monitoring, SNMP traffic consumes large amount of network bandwidth. RMON is a technique to reduce management traffic by transferring the monitoring task from management station to managed devices. In this lab, we will monitor Cisco routers' traffic by using RMON. The task is to configure routers so that when traffic on an interface exceeds a certain value the router will fire an Event alarm and the NNM will receive, process, and display the alarm.
2. On NNM management station load RFC2819-RMON-MIB into NNM (if not already loaded).
3. Select a router (say, R2) from NNM map.
4. Use MIB Browser to find the object ‘ifInOctets’.
5. Click button "Graph" to get a real-time chart of IfInOctets.
6. Configure threshold-based RMON interface traffic event on the Cisco router:
   * Generate an alarm when ifInOctet value becomes greater than some percentage of its max bandwidth limit. The threshold value, for example, can be the long time average of an interface’s ifInOctets.
7. Test your configured event by generating some extra traffic on that interface (for example, you can use extended ping command)
8. Record the alarming process on the NNM station
9. We want to be notified when somebody is maliciously trying to access SNMP agent with a false community name. At the same time we also don’t want to be annoyed by events due to accidental operation mistakes.
10. Use OBJECT .iso.org.dod.internet.mgmt.mib-2.snmp.snmpInBadCommunityNames. Generate an alarm when there are more than 10 incoming snmp commands with "bad community name" occur within 5 minutes.
11. Test your configuration by sending enough snmp requests to the configured router, watch the alarm on the NNM management station
12. Record all processes.
13. Show the configuration of routers and screen shots
14. Issue some snmpget command from management station to the router with bad community name.
15. Take screen shots of alarms on management station

1. Retrieve running configuration for a Cisco router via SNMP

Download “tftpd32.exe” from the Internet. Install, configure and run tftp daemon on the server. Study Cisco MIB OLD-CISCO-SYS-MIB.my and understand how to use MIB object ‘writeNet’ to write running configuration to NNM station using TFTP.

1. This lab is designed for the purpose to understand the management of basic traps and to manually generate a trap event.
2. Make sure the NNMi has finished the discovery process - all the routers are managed and displayed in the NNMi Map.
3. Open the NNMi Alarm Browser and read through existing alarms
4. Login to a router (say R2) and shutdown one interface (say, loopback0)
   * Wait for a few seconds and see whether ‘linkdown’ alarm shows up in NNM alarm browser
   * Watch R2 symbol’s color change from green in the map
   * Back to router R2, turn on the shutdown interface
   * Wait for a few seconds and see whether ‘linkup’ alarm shows up in NNM alarm browser
   * Watch R2 symbol’s color change back to green in the map
5. On interface e0 (R2), repeat the steps above. Observe and explain secondary failures, if any.

Record all steps on routers and take screen shot for the NNM station.