

SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

Mohammad S. Hasan

Agenda

2

- Looking at Today
 - ▣ What is a management protocol and why is it needed
 - ▣ Simple Network Management Protocol (SNMP)
 - ▣ Addressing a variable within SNMP
 - ▣ Differing versions

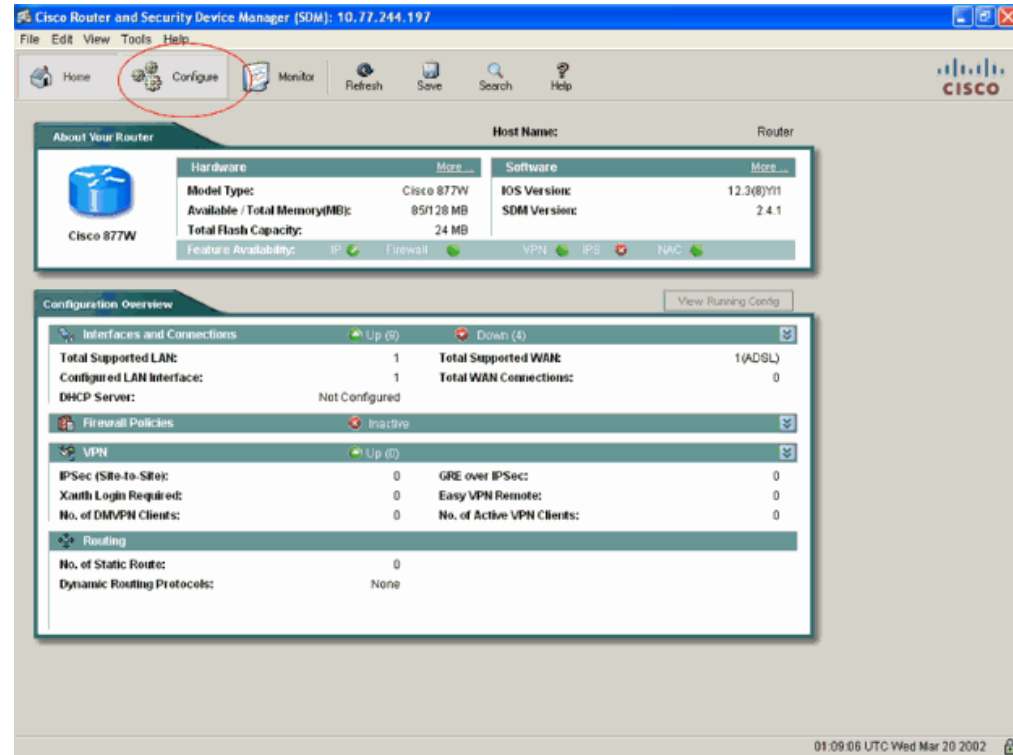
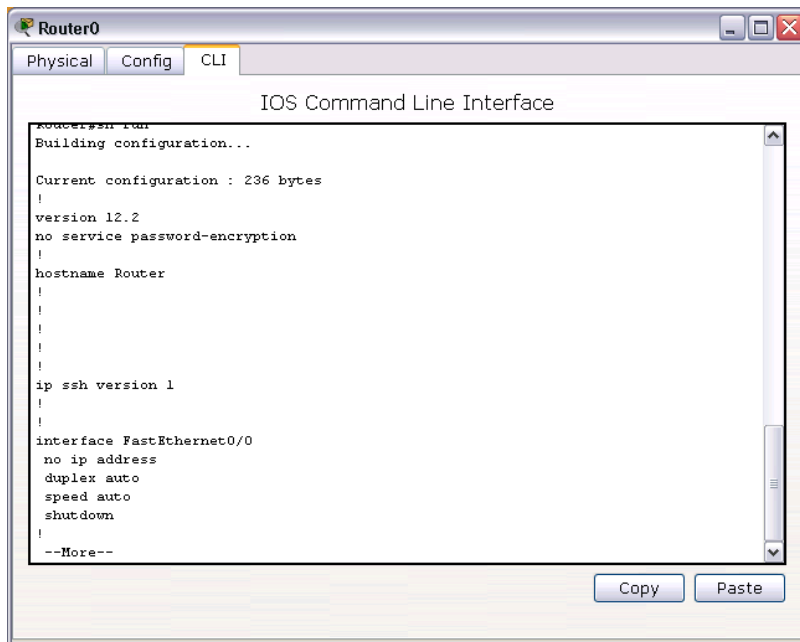
Ad-hoc Network Management

3

- The easiest management method - Ad-hoc approach
 - ▣ Sending messages to each devices and measuring the response
 - ▣ Check if the response is different to what you would expect
 - The OS will provide these utilities
 - PING
 - Traceroute (Tracert)
 - Netstat
 - ▣ If you then need more specific info from remote systems
 - Remotely logon to the systems to get detailed information
 - Each piece of equipment though needs to be contacted

Telnet – Web Interface

4



Simple Network Management Protocol (SNMP)

Why Manage at all ?

5

- The network hardware is built to run 24/7 and rarely fails
 - ▣ The reason is that equipment does fail in reality
 - ▣ Simple checking – the network / device working or NOT
 - More commonly - the network is not performing well
 - Slow downs for parts of the company

Why Manage at all ? Cont.

6

- The impact of a failure can be considerable on a commercial organisation
 - ▣ Responses need to be arranged quickly
 - ▣ The relevant technician needs to be informed quickly
 - Starting the investigation before the complaints are raised
- Number of devices
 - ▣ There are diverse and increasing number of devices
 - ▣ A common method is needed to communicate with them to get information
 - In addition management can be done from one location reducing the costs of keeping technicians at each location within a company

Characteristics of Network Management: IETF and ISO

7

□ IETF

- ▣ Management should be simple
- ▣ Variable Orientated approach
- ▣ Management Information exchanges may be unreliable

□ ISO

- ▣ Management should be powerful
- ▣ Object Orientated approach
- ▣ Management information must be exchanged in a reliable fashion

ISO Network Management Model – Five Components

8

- Configuration Management
 - ▣ Tracking and monitoring the details of all of the hardware and software within the network
- Fault Management
 - ▣ Detection of faults within the network and is what most users think of when considering network management
- Performance Management
 - ▣ Monitoring and adjusting of the network to ensure it is working as well as it can do.
 - ▣ Highlighting when performance drops below an acceptable level

ISO Network Management Model – Five Components

9

- Accounting Management
 - ▣ Monitors the usage of the network and services for example billing purposes or just to record what the usage of a component is
- Security Management
 - ▣ This is responsible for monitoring and preventing unauthorized users within the network, preventing them before they cause problems for authorized users

Goals for a Management Protocol

10

□ Ubiquity

- ▣ Operate on a PC through to a super computer
- ▣ Monitoring a diverse number of devices
 - The number of devices and relative computing power is changing all of the time
- ▣ Extendible
 - Hard to predict what networks will look like in 15 years
- ▣ Standardised so that a number of different operators can support the protocol

Goals for a Management Protocol cont.

11

- Low overheads
 - ▣ Limited functionality giving what is needed alone
 - ▣ Small network impact for all of the communications
- Robust
 - ▣ The design needs to continue operating in environment where components have failed

Simple Network Management Protocol (SNMP) Versions

12

□ SNMP Version 1

- ▣ The most widely used version still at the moment is version 1
- ▣ There are number of RFC's which are defined as a part of this a list of some of them can be found at
 - http://www.snmp.com/protocol/snmp_rfcs.shtml

□ SNMP Version 2

- ▣ Additional features for SNMP e.g. the ability to get large amounts of data
- ▣ Security was added to version 2, but this was not widely used as it was a complex method
- ▣ The version 2 without security which was used is referred to as SNMPv2c

Simple Network Management Protocol (SNMP) Versions

13

□ SNMP Version 3

- ▣ Introduces full security to the protocol defined in 2004 and is the current latest standard
- ▣ Usernames and passwords have been added allowing encryption/decryption of the data which is transferred between the devices

SNMP Basic Components

14

- Managed Device
 - ▣ The devices that require monitoring
 - ▣ An example could be a router or a switch
- Agents
 - ▣ The agent is a piece of software which is installed on the device
 - ▣ This software will record and monitor the activities it has been told to on the device writing the information to the Management Database
 - ▣ The information stored will be kept in a format which is compatible with SNMP
- Network Management Stations
 - ▣ This is a computer will run the software which will monitor and control the devices. The majority of the processing of the information will be done at this location as well as the processors and memory is a lot better.

SNMP - Variables

15

- SNMP uses the concept of variables like programming
- There is a variable which contains the values which you need to return or update
 - ▣ An example would be the packet dropping rate variable
 - ▣ You can then query this value and then return it
 - ▣ In addition you can then set a value in the variable for example to reset the packet dropping rate to a value of 0

Basic SNMP Message Types

16

- GET
 - ▣ Request information for a specific variable
- GET-NEXT
 - ▣ Request information for the next variable in the object Identifier (OID) tree
- GET-RESPONSE
 - ▣ This is returned from the device with either the variable or an error to say that it does not have the information
- SET
 - ▣ This informs the agent to make a change to a variable which is being stored
- TRAP
 - ▣ The trap message is if the agent recognizes an event has occurred and the information is sent to the management station
- Version 2 and 3 have extended these messages with new specific messages
 - ▣ For example GET-BULK

SNMP Traps

17

- The traps are unrequested data
- A request does not need to be sent for a Trap to operate
- A trap will be defined on a device and when a variable has moved beyond a threshold the information can be sent back to the Management device
 - ▣ A good example could be the packet dropping rate
 - ▣ A packet will be sent to the defined management device

SNMP Traps cont.

18

- The management console will listen on port 162 for the events
- The agent can be configured to throttle the number of traps which are sent rather than sending one each time a threshold is crossed
 - ▣ This is done to reduce the traffic loading on the network
 - ▣ If additional information is required then a get request can be sent to the host
- This is the only information which is sent within SNMP which is not specifically requested by the Management device

Management Information Base (MIB)

19

- The MIB defines a devices management information
 - ▣ RFC 1213 <http://tools.ietf.org/html/rfc1213>
- The information is written in a standard format of Abstract Syntax Notation 1 (ASN.1)
- The actual files will be located in different places depending on the OS and the software used
 - ▣ On Unix based systems the default is `/usr/share/snmp/mibs`
- The structure of the variables is given by the Structure management Information (SMI)
- This describes the object and the details of what is stored within it
- An example for the IP datagram discarded can be seen below

ipInDiscards OBJECT-TYPE

SYNTAX Counter

ACCESS read-only

STATUS mandatory

DESCRIPTION

"The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly."

Simple Network Management Protocol (SNMP)

SNMP specifying the variable – Object Identifier (OID)

20

- ❑ A large number of variables can be stored on a particular device
- ❑ What is needed is a standard method of getting this information back from the device once it has been asked
- ❑ The method of defining which variable among all of them which are stored is given as an hierarchal tree
- ❑ Using this method a specific instance of a variable can be specified

SNMP specifying the variable cont.

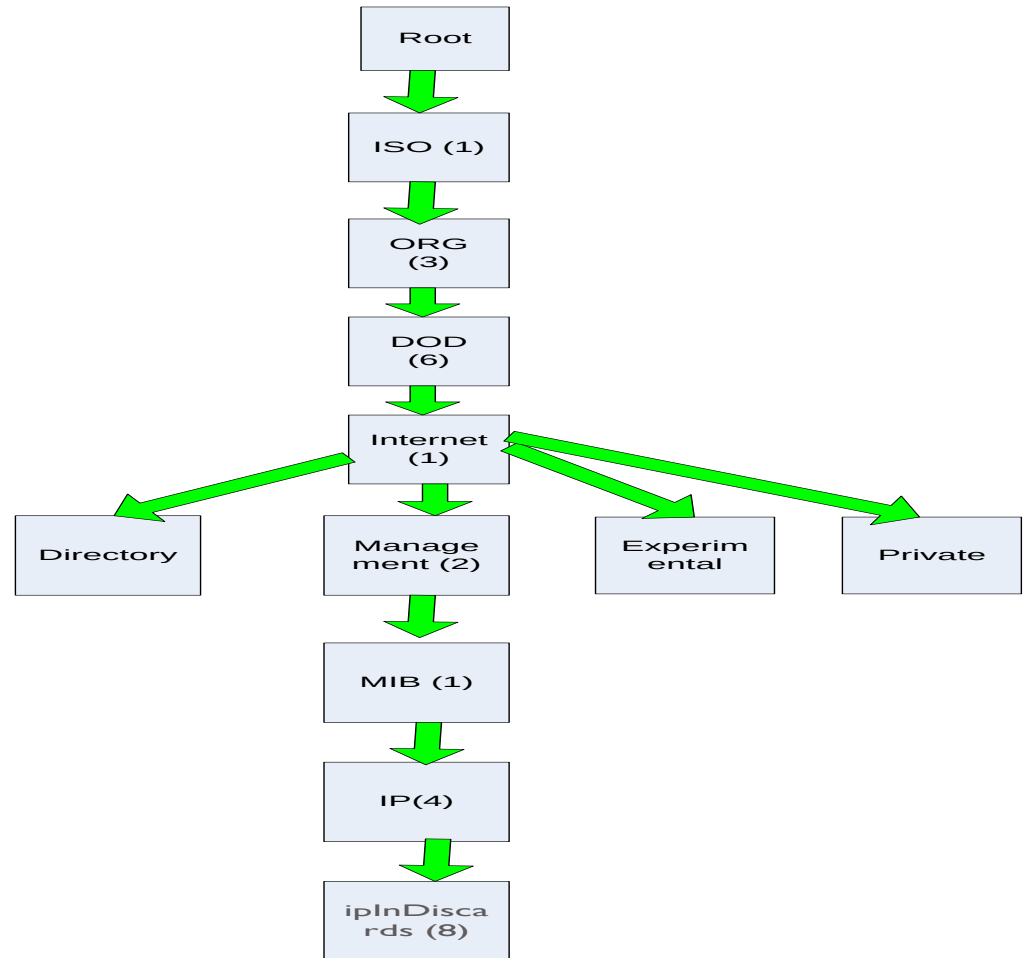
21

- The tree is given a dotted notation iso.org.dod.internet
 - 1 iso
 - 1.3 org
 - 1.3.6 dod
 - 1.3.6.1 internet
- ▣ A further example if you want information about the TCP ports
 - It is found under 1.3.6.1.2.1.6
 - A complete list can be found here
 - <http://www.iana.org/assignments/smi-numbers>
 - An example would be
 - 1.3.6.1.2.1.4.8 which contains the number of IP datagram's discarded

Hierarchy Example

22

- 1.3.6.1.2.1.4.8
 - ▣ IP Datagram Discarded



Simple Network Management Protocol (SNMP)

SNMP Transport

23

- SNMP is intended as a lightweight protocol
 - ▣ adds very little overhead to the network
- Memory or processor overhead
- SNMP uses the User Datagram Protocol (UDP) to transfer messages
 - ▣ This protocol is connectionless in its operation
 - ▣ Has very little in term of overhead for sender or receiver
 - ▣ The agent simply need to listen on port 161
 - For get/set messages being sent to the agent
 - ▣ The management needs to listen on port 162
 - For trap messages being returned

SNMP Community Name

24

- ❑ In version 1
- ❑ This is the authorization method which ties together several devices
- ❑ It is effectively the password which is transferred to the devices to authenticate them
- ❑ The issue with this though is that the actual password is sent each time

SNMP Community Name

25

- The password is passed between devices in clear text
 - ▣ Anyone using a sniffing tool such as Wireshark can listen for the packets and recover the text
 - ▣ The original version of SNMP was only supposed to be a temporary solution to the problem and was supposed to be replaced
 - ▣ Here is a link to a discussion of security issues within the use of SNMP
 - <http://www.cert.org/advisories/CA-2002-03.html>
- In version 3 this has been replaced with encrypted traffic making it much more secure

SNMP Community Name

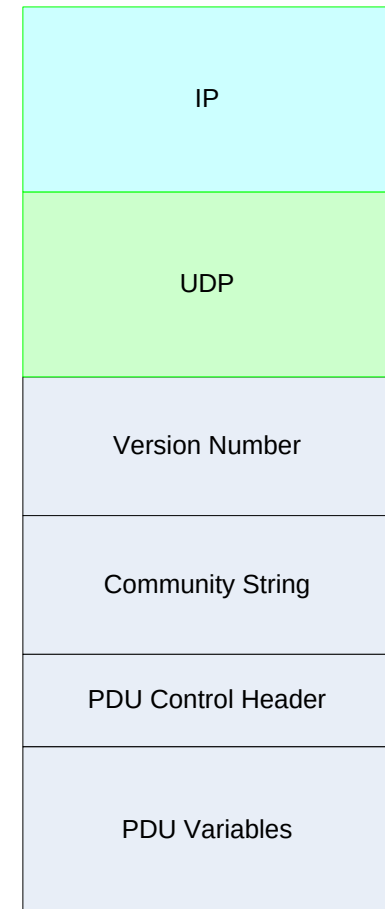
26

- There are three community names that can be used
- Read only
 - ▣ Return the variables without any updates to them
 - ▣ Commonly the default for this is the word “public”
- Read-Write
 - ▣ Allows the return of the variables and allow the update of the data using the SET command
 - ▣ Commonly the default for this is the word “private”
- Trap
 - ▣ Used when receiving/sending a trap to a management device

Basic Message Format for SNMP

27

- Version Number
 - ▣ The version number for SNMP used(Version 1 = 0)
- Community String
 - ▣ The password being exchanged to validate the users
- PDU Control Header
 - ▣ Protocol Data Unit (PDU) control information
- PDU Variables
 - ▣ The actual information to be exchanged



Basic Message Format SNMPv3

28

- Version3 is a lot more complex with more fields allowing better control
 - ▣ This is defined in RFC 3412 (<http://www.isi.edu/in-notes/rfc3412.txt>)
- Message Version
 - ▣ 4 bytes – value of 3 for SNMPv3
- Message ID
 - ▣ 4 bytes – unique ID for the message
- Message Maximum Size
 - ▣ 4 bytes – maximum size of message supported by the sender

Basic Message Format SNMPv3

29

- Message Flags
 - ▣ 1 byte – control messages
- Message Security Model
 - ▣ 4 bytes – describes which model is used
- Message Security Parameters
 - ▣ Variable in size- defined in RFC 3414
<http://www.ietf.org/rfc/rfc3414.txt>
- Scoped PDU
 - ▣ Length variable – PDU to be transferred

The Need for SNMPv3 Authentication

30

- Modification of the information
 - ▣ Changing the value of the variables which are transferred
- Impersonation of a device/user
 - ▣ Ensuring that the devices communicating are aware that they are the correct devices and not another device sending false information
- Message adjustment
 - ▣ Adjust a value to indicate an interface has failed or to replay a previous set of messages to confuse the software
- Recording the contents of the communication
 - ▣ Keeping recording of the communication for future usage for example gaining the IP address information or routing information from the kit

SNMPv3 Authentication

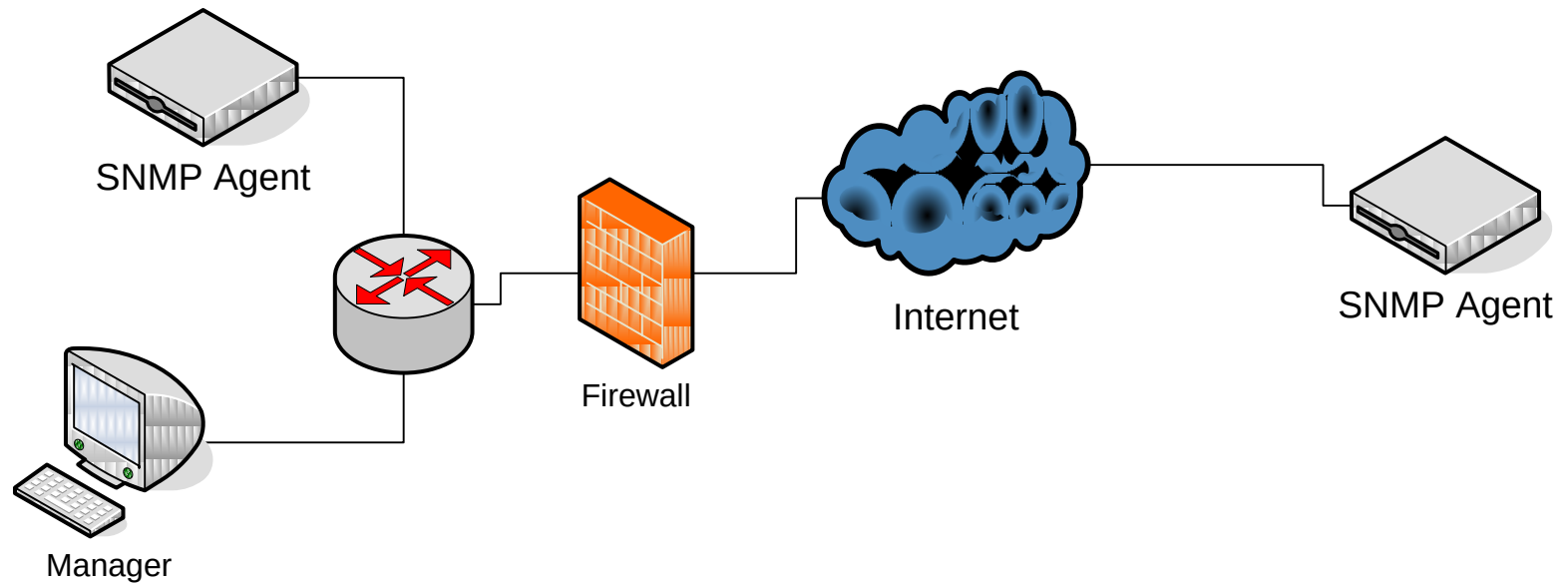
31

- Security within SNMPv3 is defined within the RFC 3414
 - ▣ <http://www.isi.edu/in-notes/rfc3414.txt>
- Encryption and authentication of the traffic
- SNMPv3 also supports Access Control Lists (ACL)
 - ▣ These are defined within RFC 3415
 - ▣ <http://www.isi.edu/in-notes/rfc3415.txt>
- The ACL defines who is able to gain access to the information and what level of access
 - ▣ For example an office manager maybe able to use the GET command to retrieve some information regarding the state of the network
 - ▣ Only the users within the networking group though have the access rights to be able to reset this value back to 0
 - ▣ This gives a lot more control over what is being done on the network and what is being monitored

SNMPv3 Authentication

32

- Remote locations can be inspected rather than just restricting your communications the local LAN



Simple Network Management Protocol (SNMP)

Considerations for usage

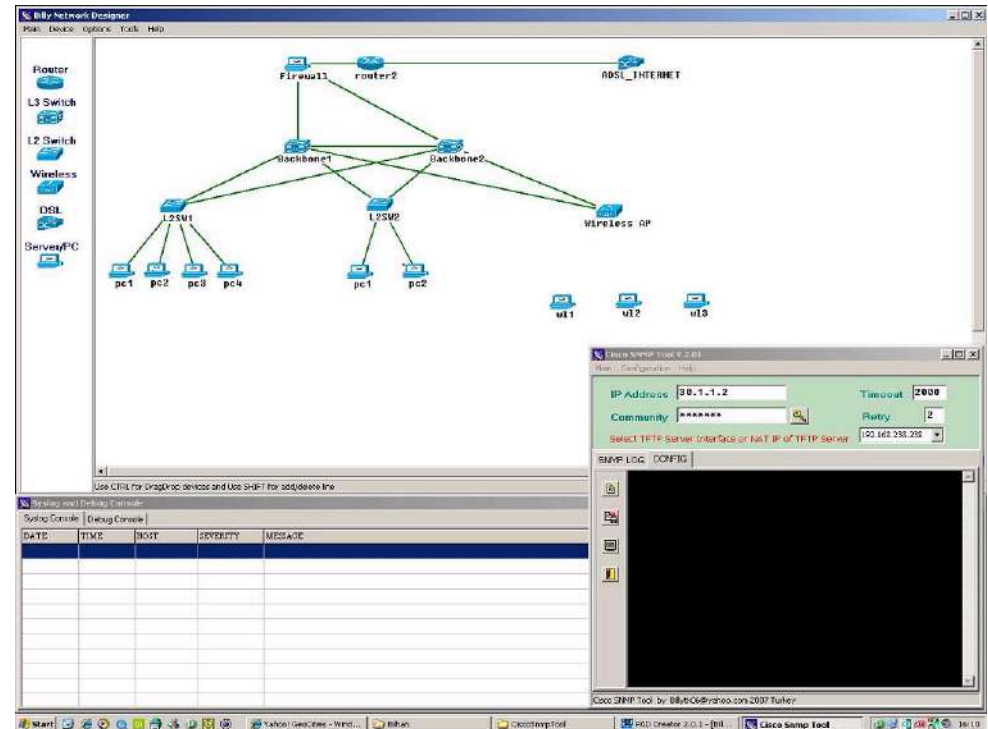
33

- SNMPv1 allows the information to flow using clear text
 - ▣ Still the mostly widely supported version simply for simplicity
 - ▣ Many configure SNMP to not allow updates and simply use it to return information to the manager
- The MIB have been added to with proprietary equipment extending the standard values which are defined
 - ▣ Here is a list of the Cisco ones which are available for each piece of equipment
 - <http://tools.cisco.com/ITDIT/MIBS/servlet/index>
- Very small amount of additional traffic added to the network
- If the number of network devices increase this can be adjusted by changing the polling frequency to reduce the traffic loading

Available Software

34

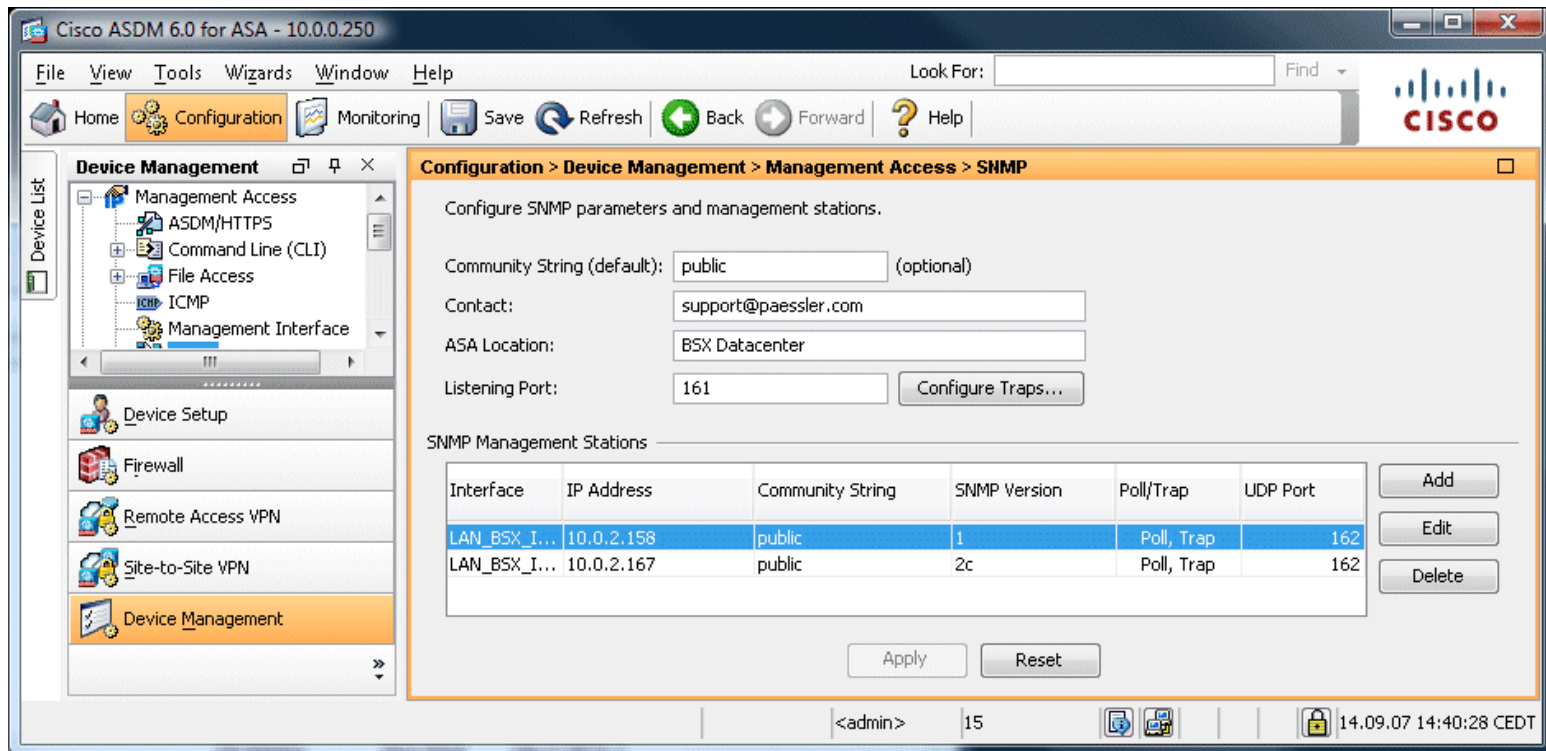
- There is a large amount of commercial and free software available to monitor the SNMP protocol
- In addition for customised applications written in house a lot programming API's are available
 - ▣ Here is a link for one which will work with Java
 - ▣ <http://www.snmp4j.org/>



Simple Network Management Protocol (SNMP)

Available Software

35



Simple Network Management Protocol (SNMP)

Summary

36

- Automated Network Management - SNMP
 - ▣ Rather than having a person going through each component and getting information
 - ▣ Looking at SNMP which is the most commonly used network management method
 - ▣ The consideration of its usage and the different versions of SNMP which are available