Simple Network Management Protocol

Vincent LeVeque, Teaching Intern

March 29, 2014

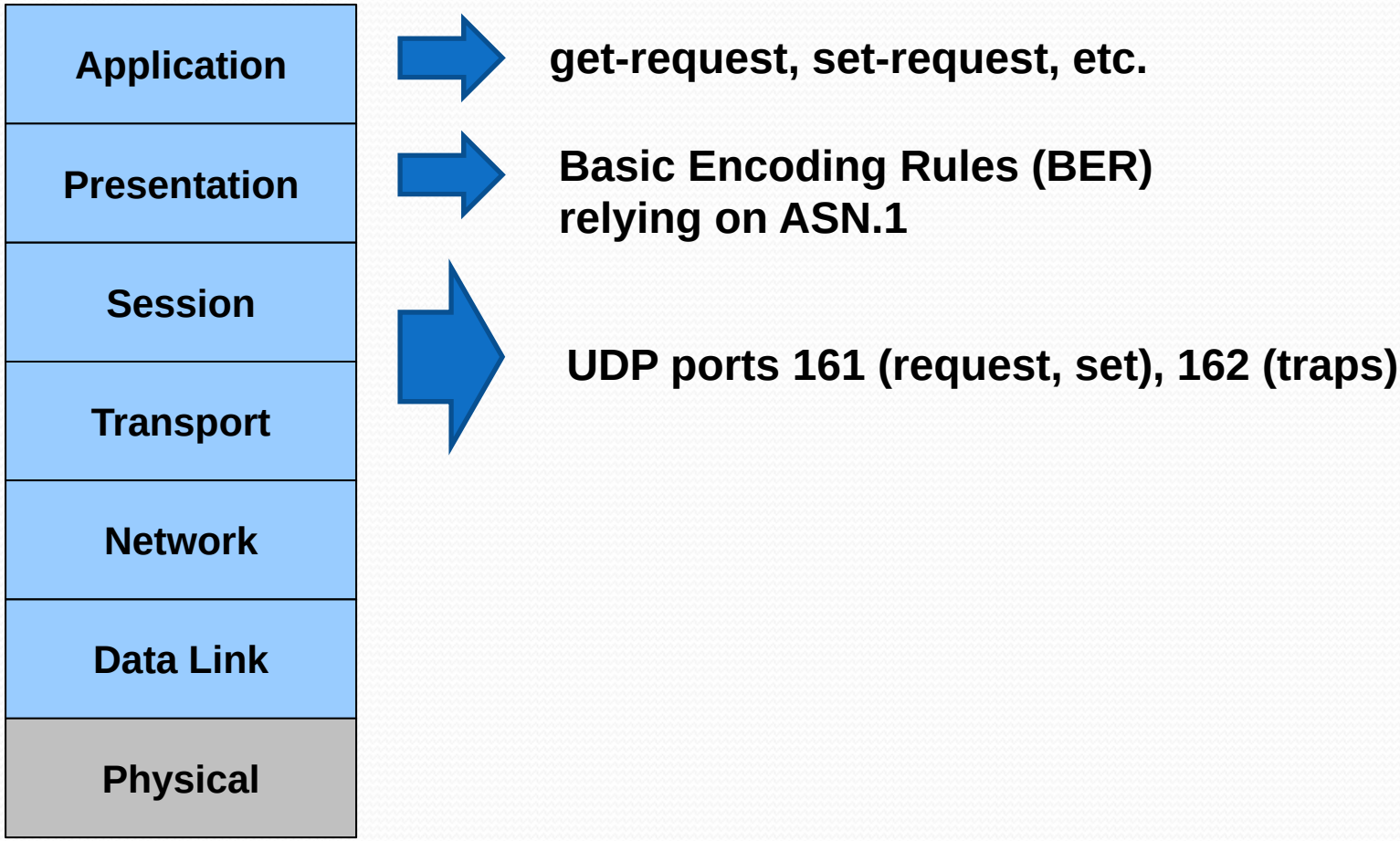
What is SNMP?

- A scalable method to monitor large numbers of networked devices
- A method to actively manage these devices
- A UDP-based protocol for performing these functions
- A set of commands for inquiring and setting device status
- A way of organizing and presenting system status information

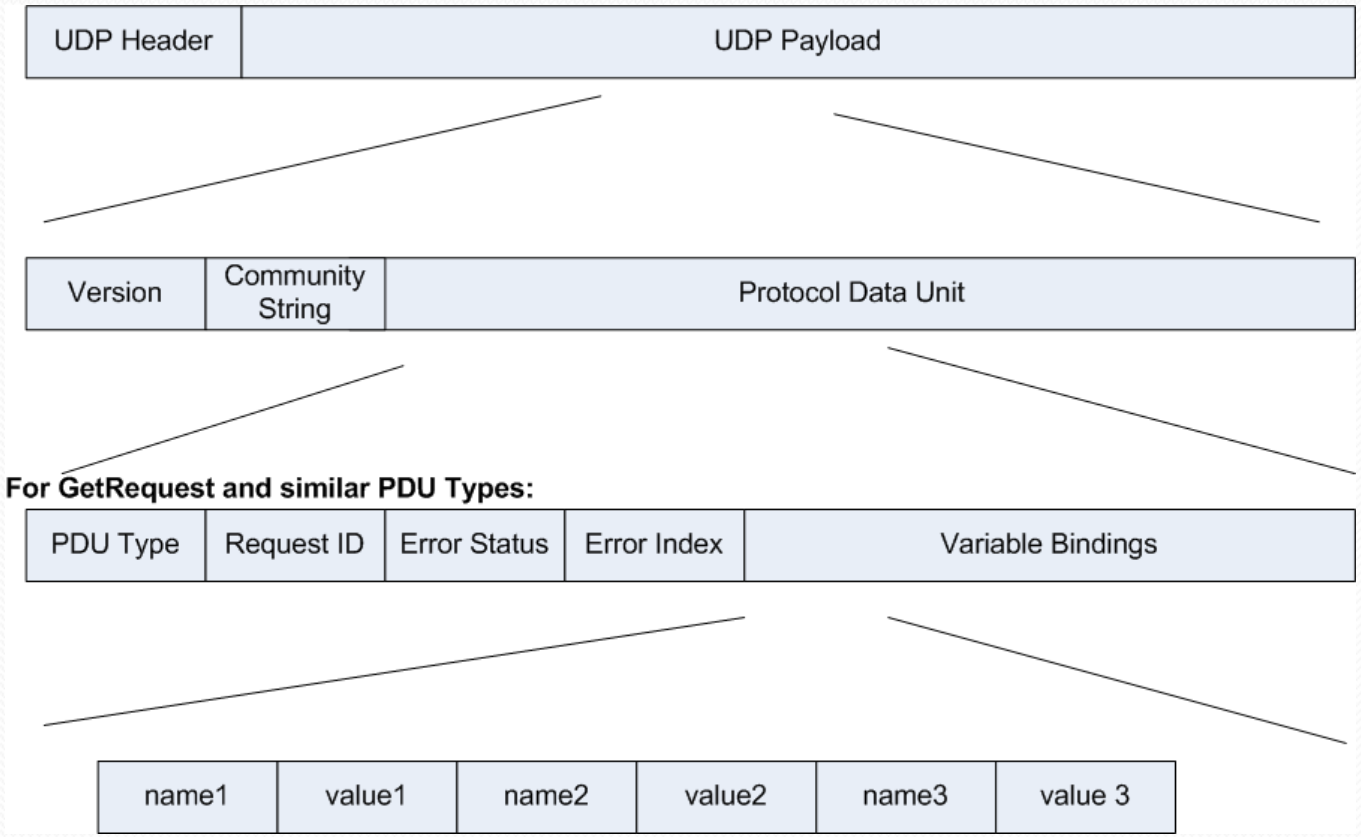
Key terms

- PDU – Protocol Data Unit, all the information sent and received in an snmp transaction (a packet and payload).
- ASN.1 – Abstract Syntax Notation One, a formal language for describing the data that makes up an snmp transaction.
- UDP – User Datagram Protocol, a simple transport protocol useful for sending short, self contained messages (like snmp)
- MIB – Management Information Base, a standardized tree-like structure organizing the data used by snmp and for referencing specific values.

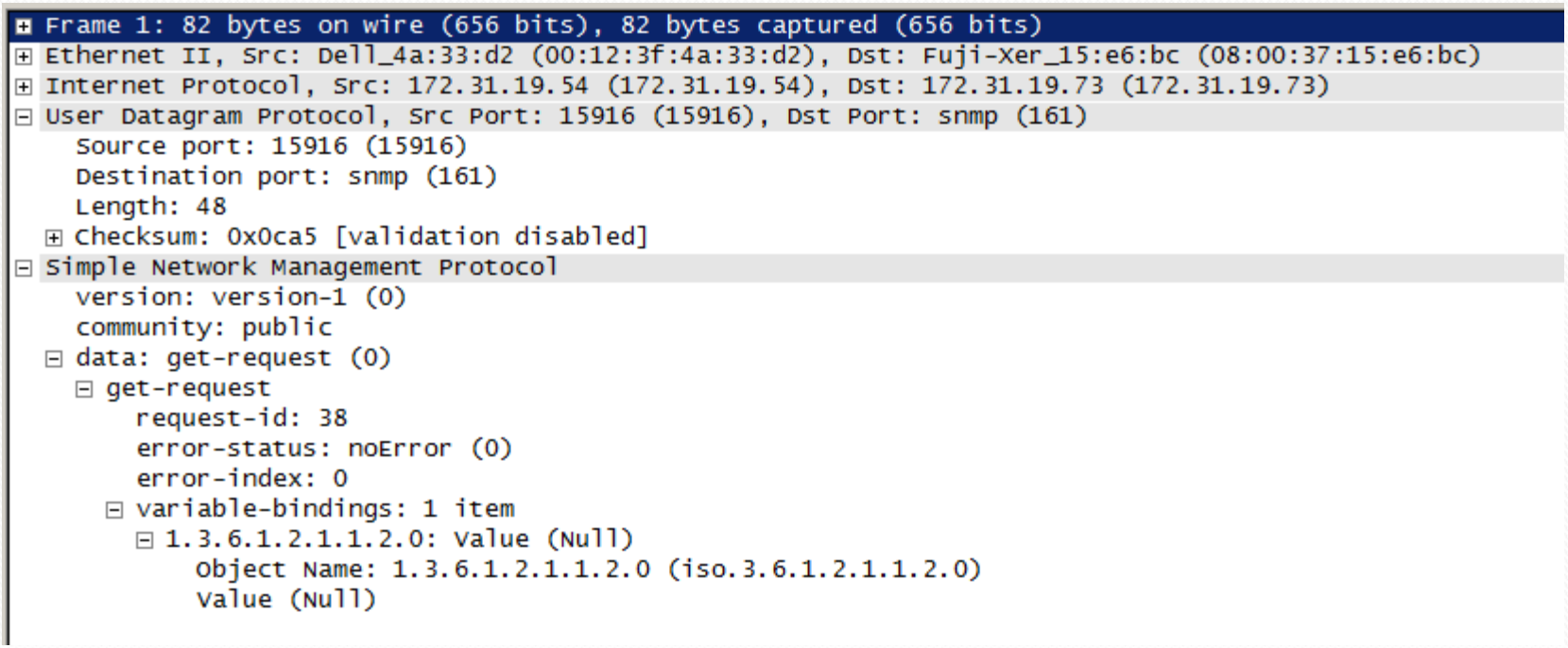
SNMP and the protocol stack



SNMP data format



SNMP Packet example



Traps and Polls

- Poll – manager requests information from an agent. Agent replies with the requested information.
- Trap – agent send message or alert to manager based on some event in the agent's system (e.g. free disk below threshold, communication error, etc.)

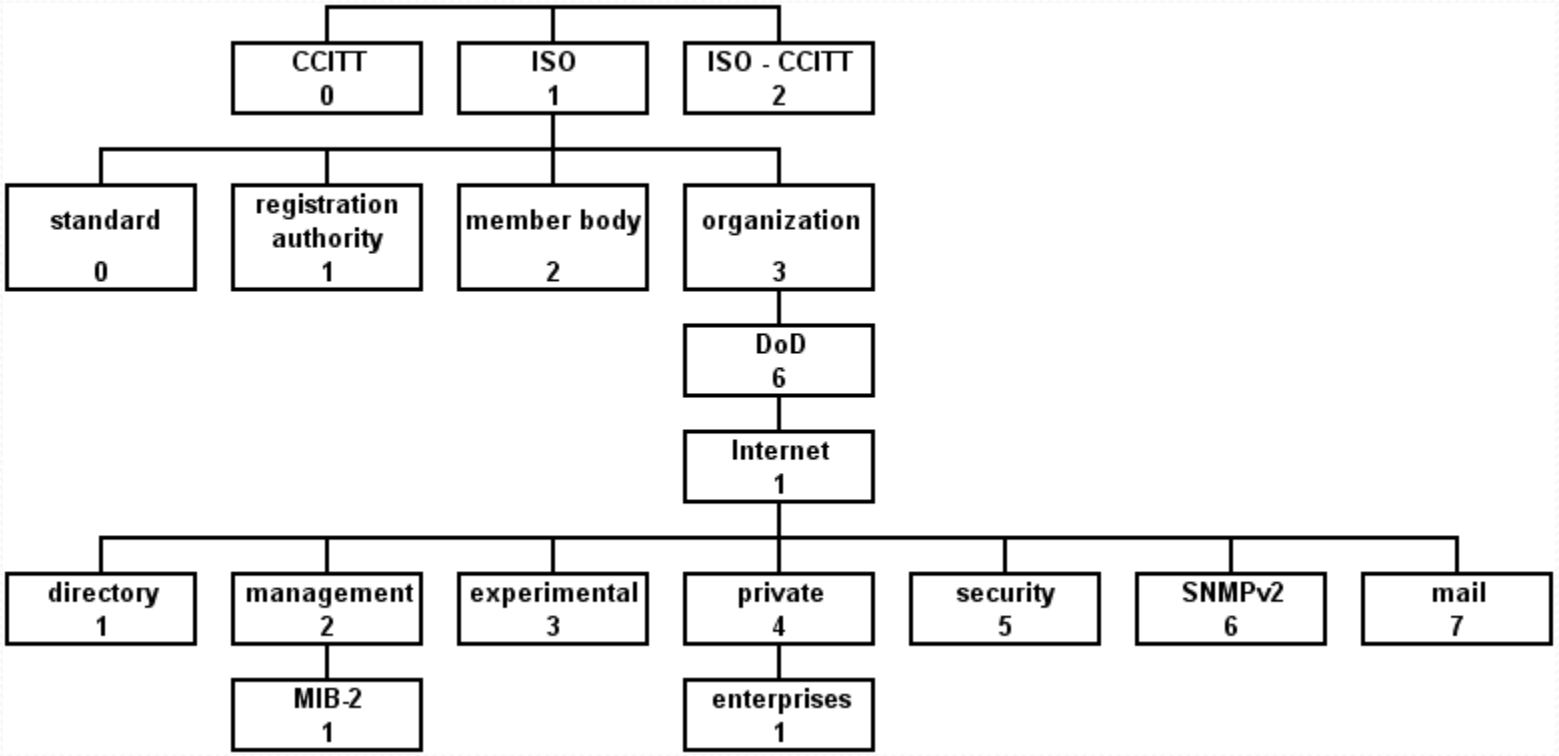
Managers and Agents

- Managers – monitor or manage devices on a network.
  - Polls devices for status
  - Receives traps
  - Provides summary information to network management staff.
- Agents – on the managed systems, agents expose system information
  - Map system metrics to the MIB hierarchy
  - Respond to manager requests using a MIB

SNMP Commands/PDU Types

- **GetRequest** – manager requests the value of a variable from an agent
- **SetRequest-** manager requests a change in an agent's variable
- **GetNextRequest** – manager wants agent to return next variable and its value
- **GetBulkRequest** – many GetnextRequests at once (snmp v2)
- **Response** – Agent returns variable bindings and and/or acknowledgement to manager for any of the above requests
- **Trap** – agent communicates information without prompting
- **InformRequest** – acknowledgement without prompting (snmpv2)

The MIB


CCITT
0
ISO
1
ISO - CCITT
2
standard
0
registration authority
1
member body
2
organization
3
DoD
6
Internet
1
directory
1
management
2
experimental
3
private
4
security
5
SNMPv2
6
mail
7
MIB-2
1
enterprises
1

The MIB

- System information is referenced by a dotted numeric string, referring to is location in the hierarchical MIB (the Object Identifier or OID)
- For example, the count of octets coming in a given interface is referenced as 1.3.6.1.2.1.2.2.1.10
- MIB objects are defined using ASN.1 notation.

The MIB

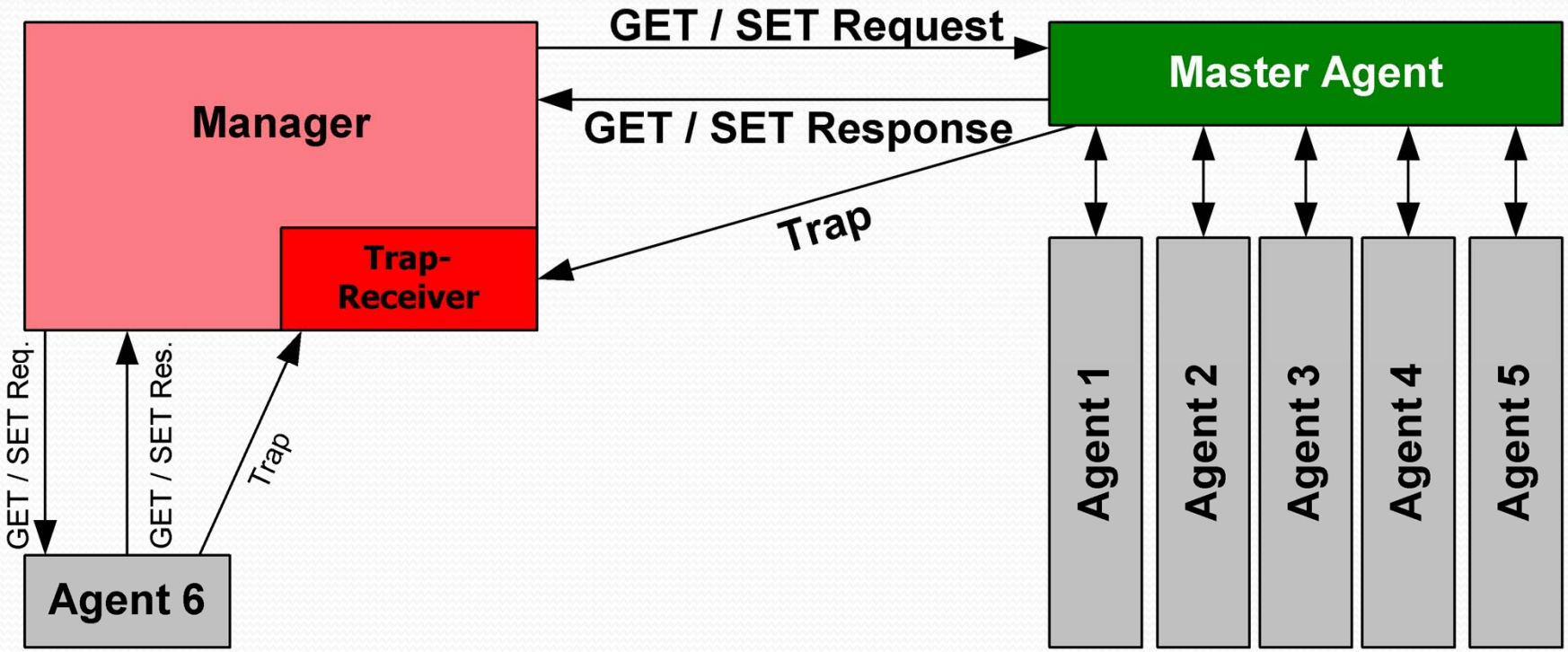
- ASN.1 example for incoming octets for an interface:

```
ifInOctets OBJECT-TYPE
    SYNTAX Counter
    ACCESS read-only
    STATUS mandatory
    DESCRIPTION
        "The total number of octets received on the interface,
        including framing characters.

        Discontinuities in the value of this counter can occur at
        re-initialization of the management system, and at other
        times as indicated by the value of
        ifCounterDiscontinuityTime."
    ::= { ifEntry 10 }
```

From ftp://ftp.cisco.com/pub/mibs/v1/IF-MIB-V1SMI.my - describing the Interface MIB

How this all works



Basic net-snmp Commands

- Net SNMP is a free open source SNMP implementation available for Unix and Linux
- It supports the following shell commands to query agents:
  - snmpget, snmpgetnext – one snmp request at a time
  - snmpwalk, snmptable, snmpdelta – multiple requests for a block of information
  - snmpset – manage a device
  - And more
  - See http://www.net-snmp.org/

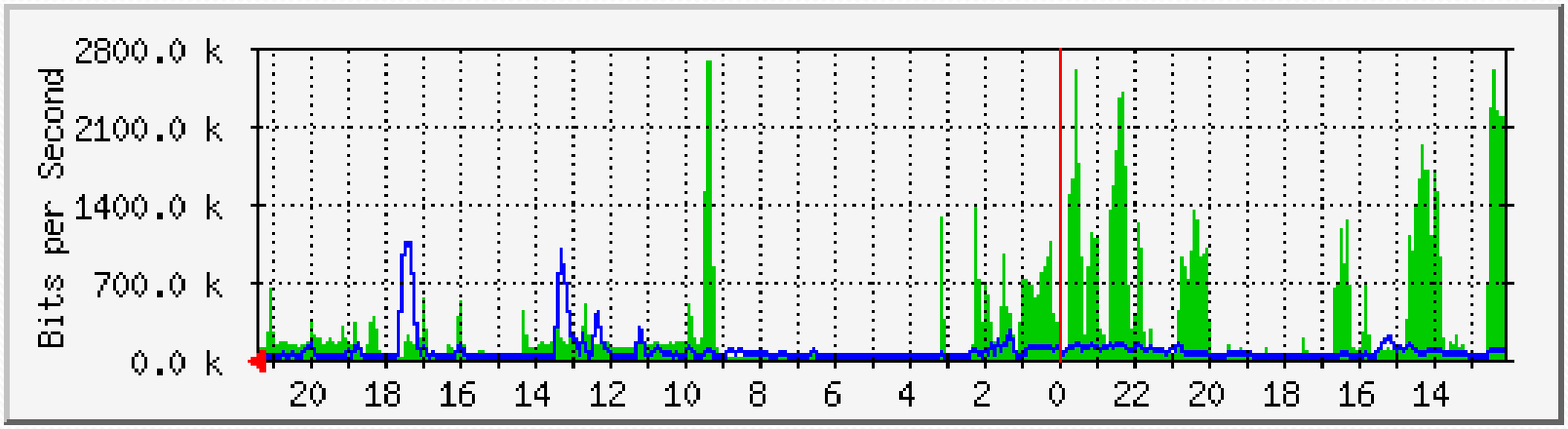
SNMPv2 and SNMPv3

- SNMPv2 added:
  - GetBulkRequest, to eliminate iterative GetnextRequests
  - Inform option, typically one manager may message another manager using inform.
  - Different message formats and protocol operations.
- SNMPv3 added:
  - Authentication – community string replaced with defined snmp users
  - Authorization
  - Optional encryption

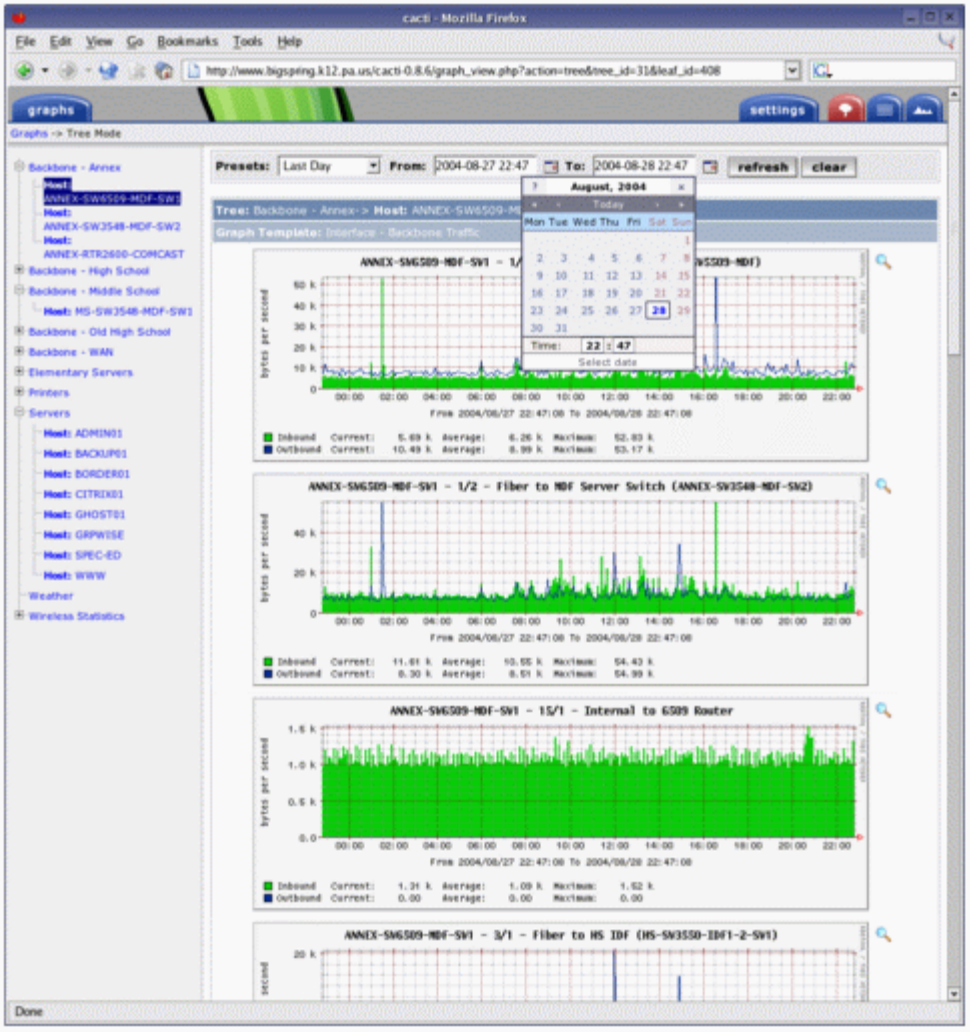
SNMP Open Source Applications

- MRTG
- Cacti
- NetDisco

MRTG


Bits per Second
2800.0 k
2100.0 k
1400.0 k
700.0 k
0.0 k
20 18 16 14 12 10 8 6 4 2 0 22 20 18 16 14

Cacti


cacti - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
graphs
settings
Presets: Last Day From: 2004-08-27 22:47 To: 2004-08-28 22:47 refresh clear
Backbone - Annex
Backbone - High School
Backbone - Middle School
Backbone - Old High School
Backbone - WAN
Elementary Servers
Printers
Servers
Weather
Wireless Statistics
ANNEX-SW6509-MDF-SW1 - 1/2 - Fiber to MDF Server Switch (ANNEX-SW3548-MDF-SW2)
ANNEX-SW6509-MDF-SW1 - 15/1 - Internal to 6509 Router
Done

NetDisco


Netdisco
[Network Map]
[Device Search]
[Device Inventory]
[Node Search]
[Port Report]
[Duplex Mismatch Finder]
[Node Inventory]
[Backend Log]
[Documentation]
[About]
User more [Logout]
[Change Password]
Search Results
MAC Vendor Match Device or Node First Seen Last Seen
00:01:80:5f:c1:9b AOpen, Inc. IP -> MAC 193.92.216.235 (dhcp-235.med) Jun 18 14:31 2007 Sep 7 17:30 2007
Switch Port 193.92.217.6 [FastEthernet0/16] (building2.med) Jun 18 14:15 2007 Sep 7 10:02 2007
Switch Port 193.92.217.2 [Port 2 on Unit 1] (swopt-prokl.med) Sep 5 20:02 2007 Sep 6 08:01 2007
* - Denotes archived data.
Matched 1 nodes.
Node Search
MAC, Hostname, IP, NetBIOS: dhcp-235.med.duth.gr
* and ? are wildcards.
Time Stamps: On Off
Archived Data:
Show Vendor : On Off
Search [Clear]
Advanced Node Search
[+] Search on Vendor or OUI
Specific Searches
Search for possible Wireless Access Points (APs)
These aren't guranteed to be wireless access points, they just have MACs that fall into the right range. Also remember people can hide them under fake MAC addresses as well.
Search for nodes with multiple active IP addresses
* Advanced Searches can be slow to load.
Netdisco 0.95