

# **Network Management:** **A Technical Look at Protocols,** **Tools, and Applications**

Presented by:  
Jeff Groman

# Definition:

The processes of managing, monitoring, and controlling a communications network. Modern Network Management systems also include the ability to re-configure network elements remotely.

- Found on <http://www.interoute.com/glossary.html>

# Agenda:

- Network Management Activities
- SNMP- Simple Network Management Protocol
- Tools
- Security
- Network Management Applications

# Activities:

- Baselineing
- Capacity Planning
- Prevention
- Recovery

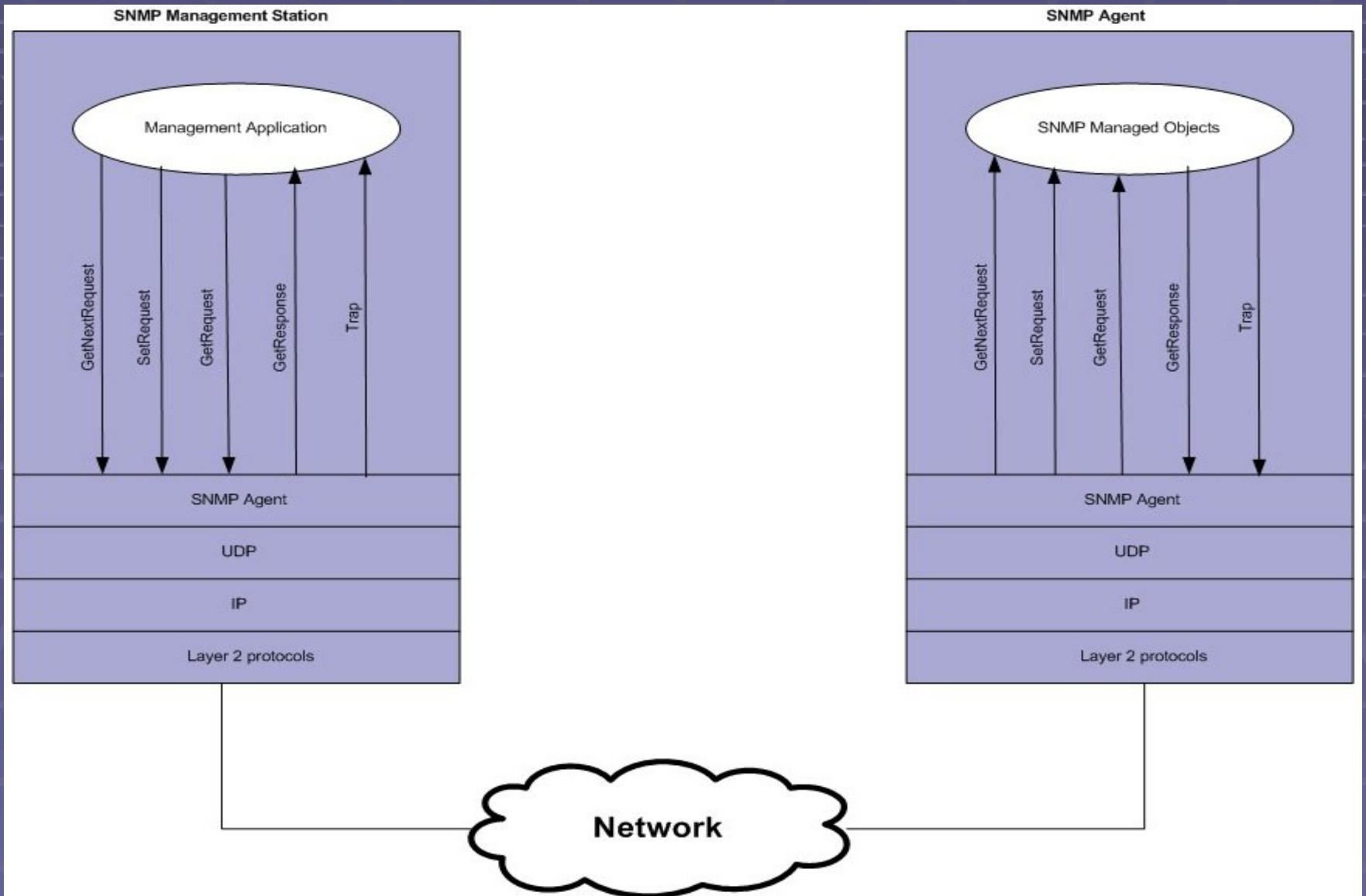
# SNMP

- Structure of Management Information (SMI)
- Management Information Base (MIB)
- Protocol
- Brief Introduction?

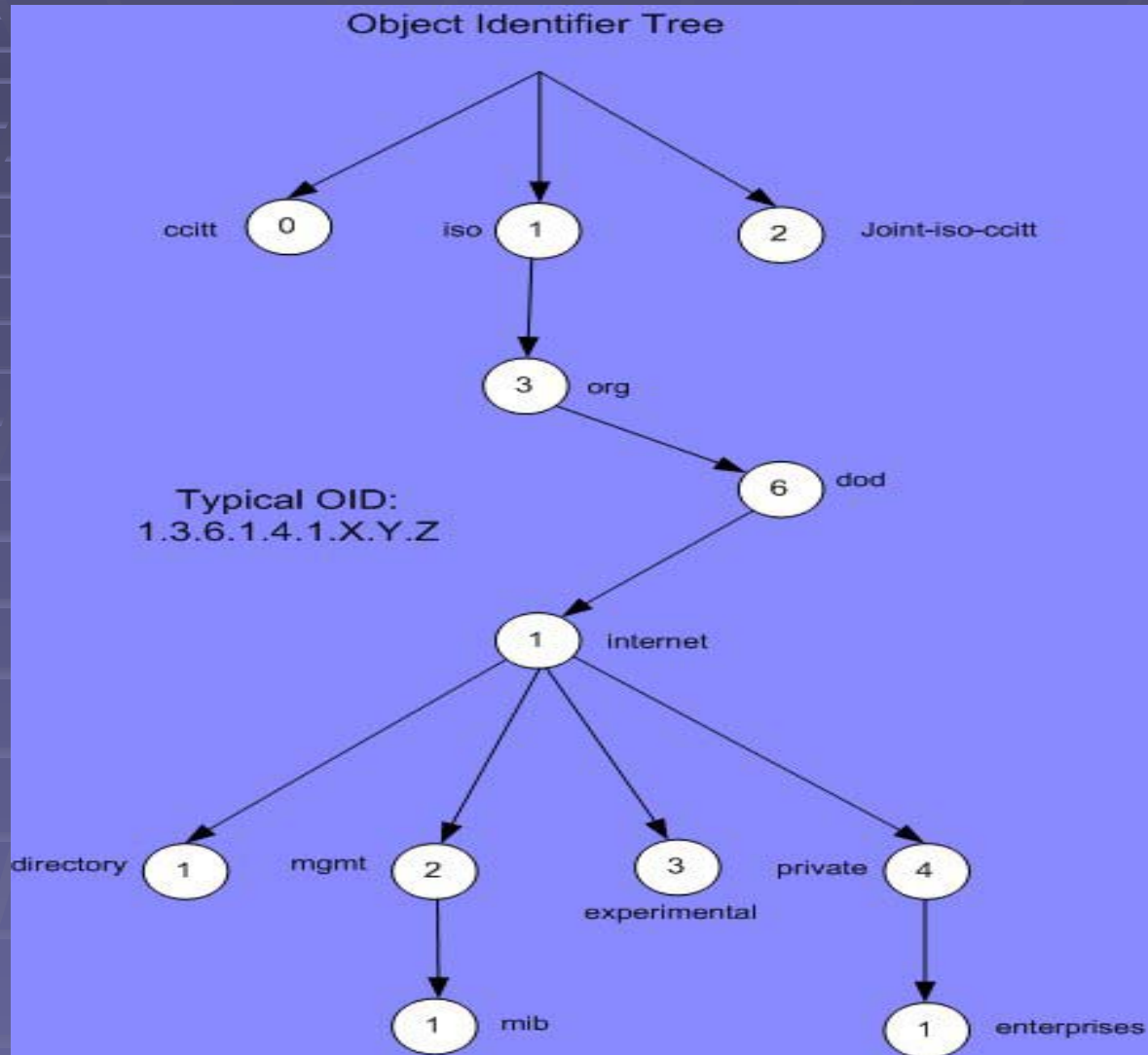
# SNMP Cont'd

- Monitor, Control
  - 3 basic functions: get, set, traps
- SNMPv1
  - Based on SGMP (~15 years old)
- SNMPv2
  - Party-based, SNMPv2, SNMPv2c, SNMPv2u ( a mess)
  - The draft standard SNMPv2 includes:
    - Counter64, GetBulk, Informs
- SNMPv3
  - Security features not included in v2

# SNMP Agent



# Object Identifiers



# SMI

- Structure of Management Information (RFC 1155) - Specifies how objects in a MIB are defined.
  - Uses ASN.1
    - Defines data types: scalars and arrays of scalars
    - Keep things simple
  - Extensible
  - Uses hierarchical tree structure

# MIBs

- Management Information Base (RFC 1212 and 1213) - Describes managed objects.
  - Using OIDs, characteristics of an object can be captured.
    - Object Identifiers and Object Descriptions are synonymous
  - Request enterprise OID at <http://www.isi.edu/cgi-bin/iana/enterprise.pl>
  - Find MIBs from most vendors at <http://www.mibdepot.com>

# Instrumentation

- Variables take forms including:
  - counters and gauges
    - icmpInEchoReps 1.3.6.1.2.1.5
  - octet strings
    - sysName 1.3.6.1.2.1.1
  - state variables
    - sPDUMasterState 1.3.6.1.4.1.318.1.1.4.2
- Can be combined into lists and table
  - ipRouteTable 1.3.6.1.2.1.4.21

# Standard MIBs

## RFC 1156, 1213

### 1.3.6.1.2.1

- system (1)
- interfaces (2)
- at (address translation) (3)
- ip (4)
- icmp (5)
- tcp (6)
- udp (7)
- egp (8)
- snmp (11)

# RMON

## 1.3.6.1.2.1.16

- statistics (1)
- history (2)
- alarm (3)
- host (4)
- hostTopN (5)
- matrix (6)
- filter (7)
- capture (8)
- event (9)
- tokenRing (10)
- protocolDir
- protocolDist
- addressMap
- n1Host
- n1Matrix
- a1Host
- a1Matrix
- usrHistory
- probeConfig

# Tools

- telnet, ping, traceroute
- ftp/tftp
- cdp
- netflow
- sFlow

# Tools Cont'd

- snmpwalk
- tcpdump (<http://www.tcpdump.org>)
- snort (<http://www.snort.org>)
- airtsnort (<http://airsnort.shmoo.com/>)
- ethereal (<http://www.ethereal.com>)
- Commercial Probes
  - NetScout
  - Agilent
  - Cisco NAM

# Security

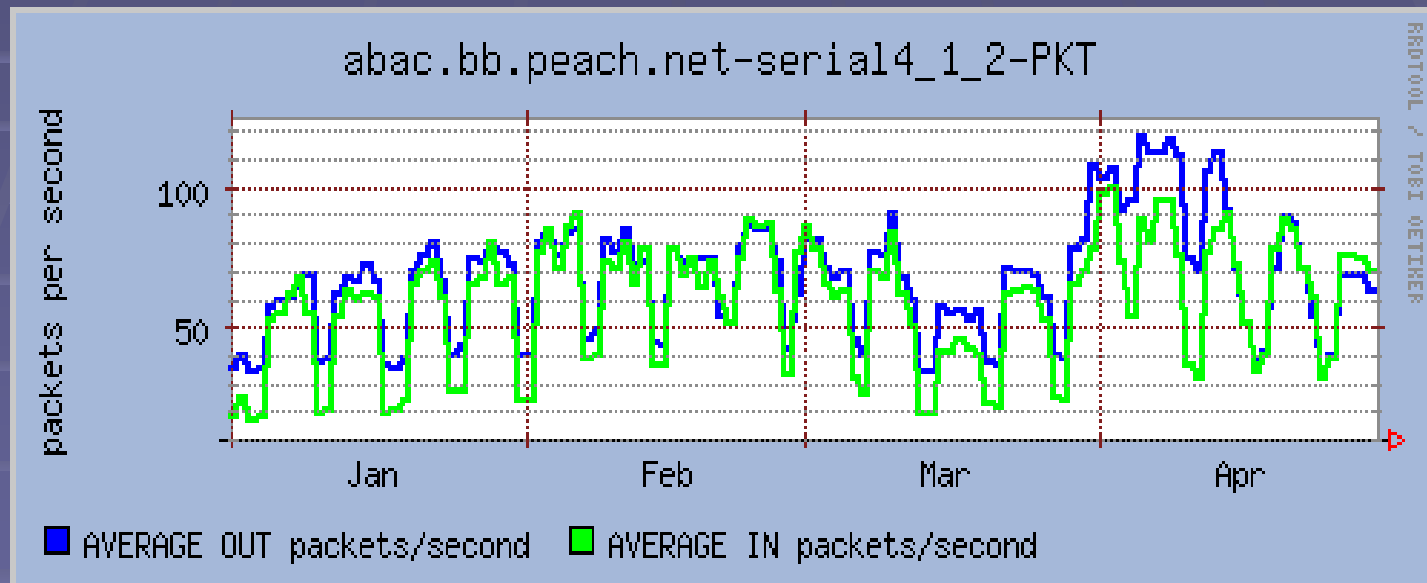
- SNMPv1, SNMPv2
  - Community strings - shared secret (shared or secret?)
  - ACLs
- SNMPv3
  - User-based
    - Authentication, Privacy, key mgt, others
    - Does not use MIBs
  - View-based
    - Access Control
    - Uses MIBs
- SSH instead of telnet
- SFTP

# Configuring SNMPv3

- IOS:
  - **snmp-server group** [groupname {v1 | v2c | v3{auth | noauth | priv}}] [read readview] [write writeview] [notify notifyview] [access access-list]
  - **snmp-server user** username [groupname remote ip-address [udp-port port] {v1 | v2c | v3 [encrypted] [auth {md5 | sha} auth-password [priv des56 priv password]]] [access access-list]
  - **snmp-server host** [host [traps | informs]] [version {1 | 2c | 3 [{auth | noauth | priv}]] community-string [udp-port port] [notification-type]

# Applications

- MRTG/Cricket (<http://cricket.sourceforge.net>)
  - Written in Perl, based on RRDTool (<http://www.rrdtool.org>)



# Applications Cont'd

- CiscoWorks
  - Campus Manager (Map)
  - CiscoView (Element Manager)
  - Device Fault Manager (Alarms)
  - Resource Manager Essentials (Remote Device Manager)
- InMon
  - netflow
  - sFlow

# Applications Cont'd

- OpenView
  - Maps
    - New support for HSRP, layer 2, and vendor icons
  - Alarms, Correlation
  - Collections/Thresholds
- Probe Software
  - Baselining (HP, NetScout)
  - Database (Agilent, NetScout)

# Conclusion

- SNMP protocol is flexible and secure for network management
- Network Management needs to be comprehensive
- Downsides:
  - These applications are expensive to own
  - Take time to configure for your environment
- Upside: Once they are in place, maintenance is minimal