University of Colorado **Boulder**

Network Management and Automation
CSCI 5180

Simple Network Management Protocol (SNMP)

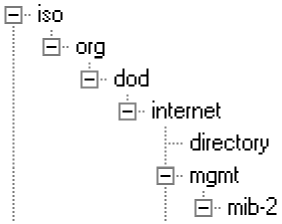
Levi Perigo, Ph.D.
University of Colorado Boulder
Department of Computer Science
Network Engineering

- **Syllabus**
- **Ungraded Labs**
- **Discussions**
  - NMS
    - ***Coding vs. Commercial***
  - SNMP
    - ***Legacy vs. Current***

SNMP Overview

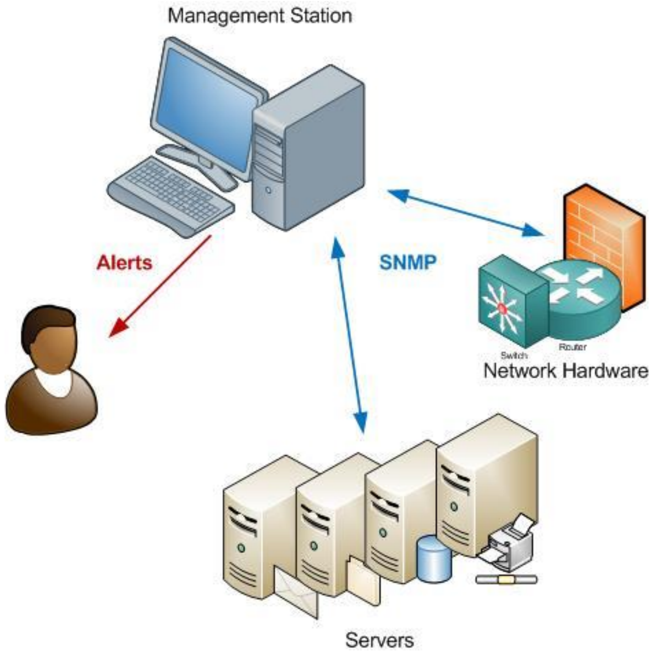
- **Vocabulary**
  - SNMP – Simple Network Management Protocol
  - NMS – Network Management System/station
    - ***Where is it located?***
  - MIB – Management Information Base
    - ***Definitions of the management data***
    - ***Tree structure***
    - ***Problems & Limitations of MIBs?***
  - OID – Object Identifier
    - ***Variables that can be read/set ("eth1 status")***
  - Trap – An asynchronous notification about conditions that the monitor should know
  - Agent

  - Coffee Example
    - ***Monitor water temp; warming/idle; how full it is; how long since last brew***
    - ***MIBs/OIDS***



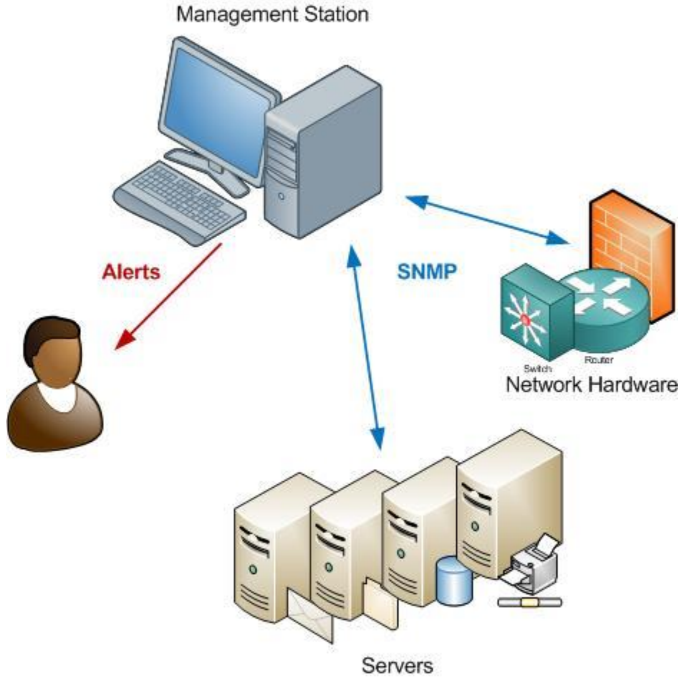
SNMP Overview

- **Three key parts:**
  1. Managed device (server, router, switch, etc.)
  2. Agent (software on device)
  3. NMS (software running on manager/server)



SNMP Diagram Example

- **Management Console (software)**
  - Polling (FROM NMS to Agent)
    - ***What must happen for this to work?***
- **Agent (software)**
- **Trap (alert – “rule has been broken”)**



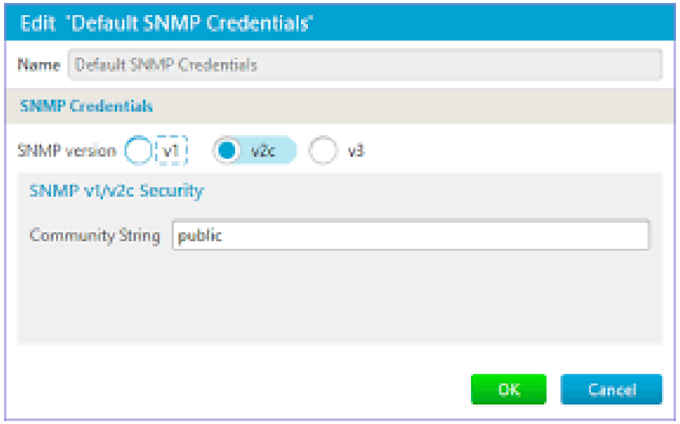
SNMP

- **Proactively monitor and communicate with devices**
- **Allows network admins to remotely manage their devices, network performance management, trend analysis**
- **Part of bigger SOFTWARE system**
- **Application Layer protocol (layer 7)**
- **Uses UDP as its transport layer protocol**
  - SNMP Requests = port 161
  - SNMP Traps/Informs = port 162
  - Connectionless
  - Efficient
  - Unreliable
    - ***Lost traps?***

SNMP

- **Community strings (*passwords/pre-shared key*)**
  - "public" (RO) and "private" (RW) - (default)
    - ***MUST CHANGE!***
  - DOD - #1 Security Attack
    - ***Security Denial of Service (DOS) - (LAN/WAN)***
      - Why is it a DOS?
      - How to prevent DOS?
        - » Out of Band management
        - » ACL "only NMS IP address & port"
        - » LAN DOS prevention
          - Different subnet (firewall rules)

- **What can be monitored?**
  - Alerts
  - Preventative maintenance
    - ***Server fan (example)***
  - Power outage?
  - WAN link down?



Edit 'Default SNMP Credentials'

Name: Default SNMP Credentials

SNMP Credentials

SNMP version ○ v1 ● v2c ○ v3

SNMP v1/v2c Security

Community String: public

SNMP

- **SNMP messages should be sent out of band (OoB)**
  - How/why?
    - ***Physical interfaces / VLANs***
    - ***Save bandwidth***
      - Not using company resources for management traffic
    - ***Backup link***

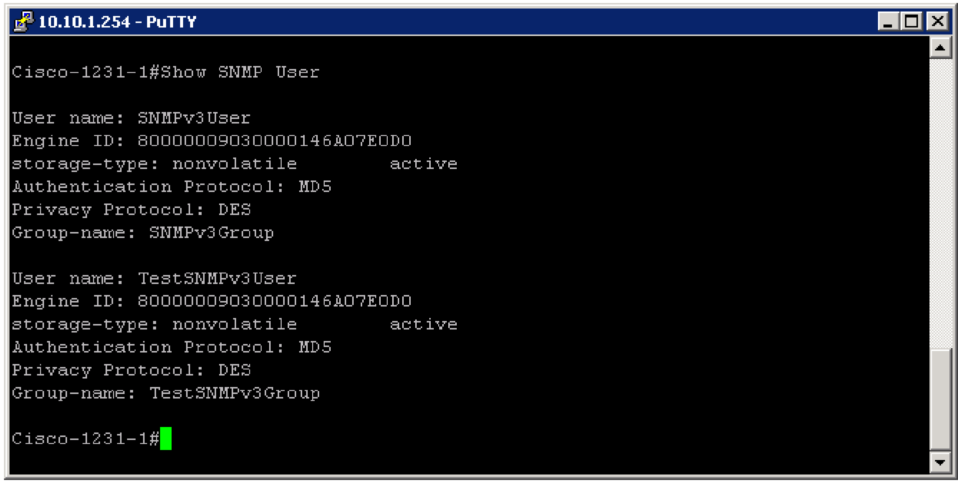
SNMP Versions

- **SNMP a.k.a. SNMPv1**
  - Works

- **SNMPv2 or SNMPv2c (community-based SNMP)**
  - “Feature pack upgrade” to v1
  - Improves performance, security (community), confidentiality
  - GetBulk (alt. GetNextRequest)
  - Standard (de facto) (most utilized)
  - Incompatible with v1 (without proxy)
  - Telnet vs SSH (still use management with Telnet)
  - SNMP = “Security Not My Problem”
  - Protocol analyzer can sniff community and contents!
    - ***Out of band network reduces this risk***

SNMP Versions

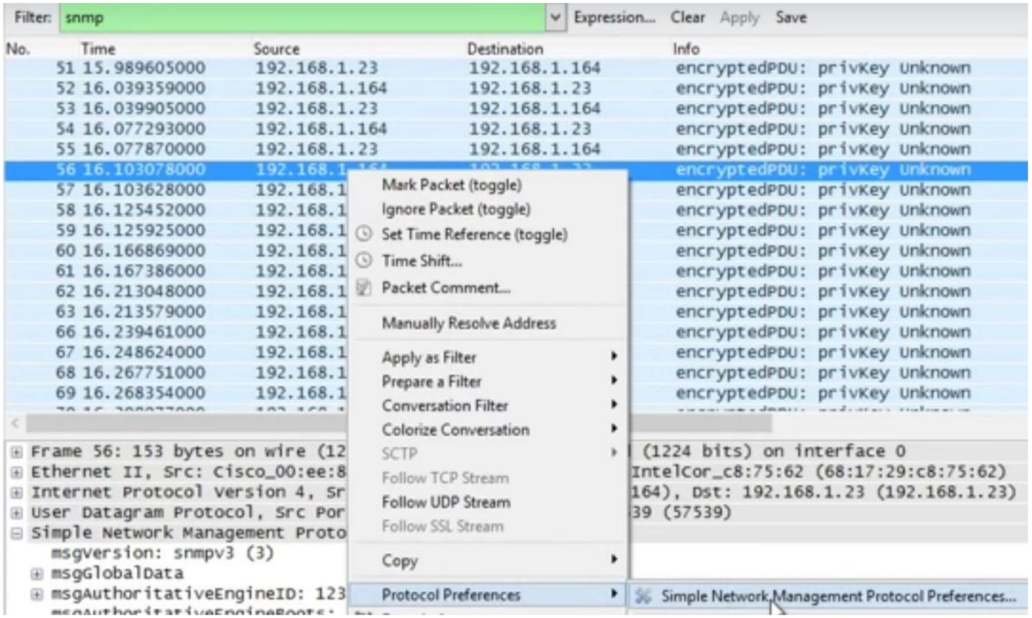
- **SMNPv3**
  - Security ("priv" - authentication and encryption)
    - ***Community string are not required***
    - ***Groups & Users & Auth/Encryption***
      - Can bypass this in Wireshark if UN/PW known
  - Mandatory in secure environments
  - Remote configuration
    - ***NETCONF!***
  - Each device has identifier
    - ***SNMPEngineID***
      - manually configured
        - » (better for documentation)
  - IOS – "show snmp user"



```
Cisco-1231-1#Show SNMP User

User name: SNMPv3User
Engine ID: 80000009030000146A07E0D0
storage-type: nonvolatile        active
Authentication Protocol: MD5
Privacy Protocol: DES
Group-name: SNMPv3Group

User name: TestSNMPv3User
Engine ID: 80000009030000146A07E0D0
storage-type: nonvolatile        active
Authentication Protocol: MD5
Privacy Protocol: DES
Group-name: TestSNMPv3Group

Cisco-1231-1#
```

- **SNMPv2 vs SNMPv3**
  - V3 = more secure and better
  - V2 = easier

- **Capture Community string, interface status, route table, etc.**
- **V3 - Decrypt in Wireshark**
  - – Find SNMP packet (SNMP)
  - – Right Click > Protocol Preferences > SNMP
  - – Edit Users Table = (UN/PW, etc.)


Filter: snmp

```
No.   Time          Source          Destination     Info
   51 15.989605000  192.168.1.23    192.168.1.164   encryptedPDU: privKey Unknown
   52 16.039359000  192.168.1.164   192.168.1.23    encryptedPDU: privKey Unknown
   53 16.039905000  192.168.1.23    192.168.1.164   encryptedPDU: privKey Unknown
   54 16.077293000  192.168.1.164   192.168.1.23    encryptedPDU: privKey Unknown
   55 16.077870000  192.168.1.23    192.168.1.164   encryptedPDU: privKey Unknown
   56 16.103078000  192.168.1.164   192.168.1.23    encryptedPDU: privKey Unknown
   57 16.103628000  192.168.1                       encryptedPDU: privKey Unknown
   58 16.125452000  192.168.1                       encryptedPDU: privKey Unknown
   59 16.125925000  192.168.1                       encryptedPDU: privKey Unknown
   60 16.166869000  192.168.1                       encryptedPDU: privKey Unknown
   61 16.167386000  192.168.1                       encryptedPDU: privKey Unknown
   62 16.213048000  192.168.1                       encryptedPDU: privKey Unknown
   63 16.213579000  192.168.1                       encryptedPDU: privKey Unknown
   66 16.239461000  192.168.1                       encryptedPDU: privKey Unknown
   67 16.248624000  192.168.1                       encryptedPDU: privKey Unknown
   68 16.267751000  192.168.1                       encryptedPDU: privKey Unknown
   69 16.268354000  192.168.1                       encryptedPDU: privKey Unknown
```

```
⊞ Frame 56: 153 bytes on wire (12                (1224 bits) on interface 0
⊞ Ethernet II, Src: Cisco_00:ee:8                IntelCor_c8:75:62 (68:17:29:c8:75:62)
⊞ Internet Protocol Version 4, Sr                164), Dst: 192.168.1.23 (192.168.1.23)
⊞ User Datagram Protocol, Src Por                39 (57539)
⊟ Simple Network Management Proto
    msgVersion: snmpv3 (3)
  ⊞ msgGlobalData
  ⊞ msgAuthoritativeEngineID: 123
```

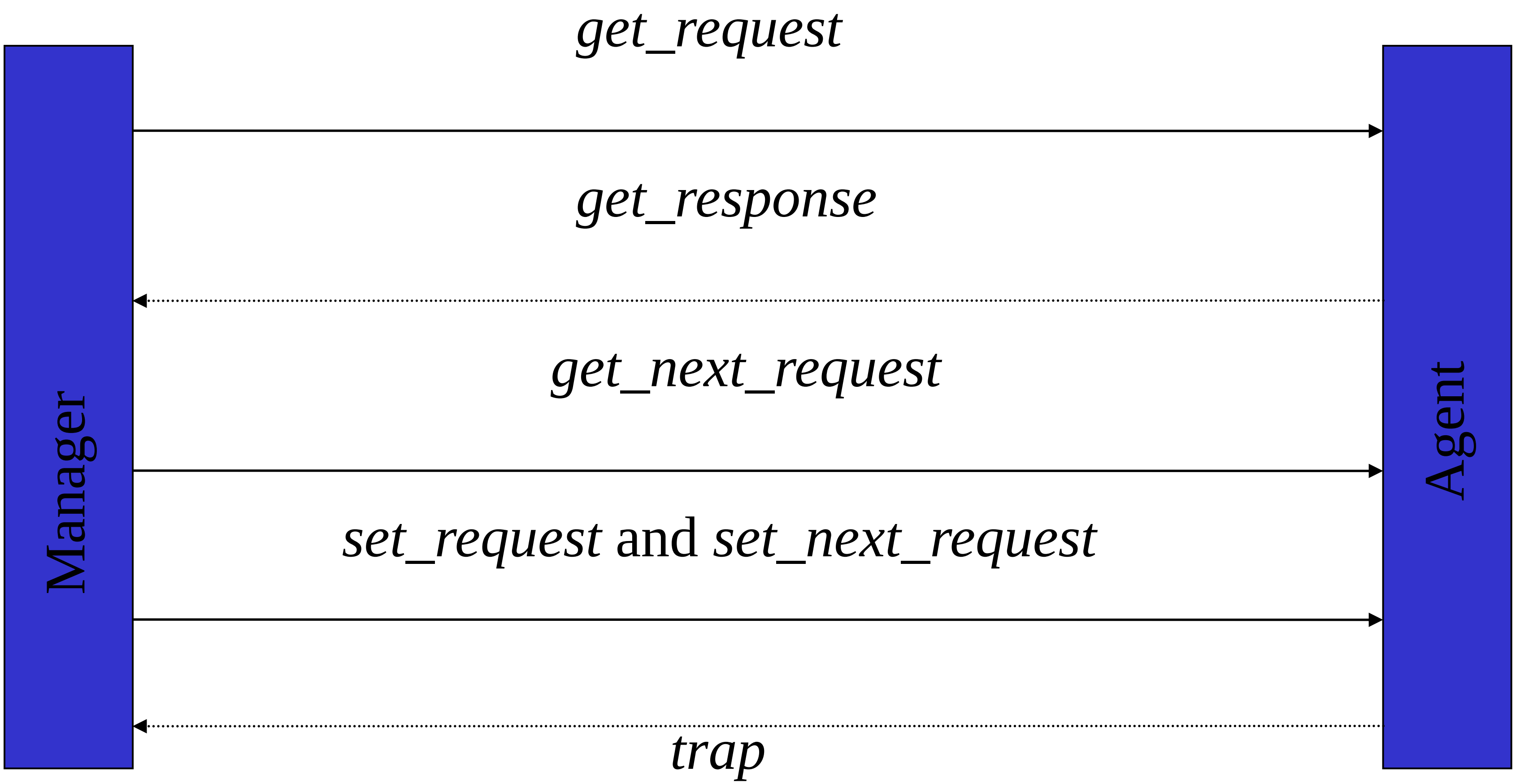
Community Strings

- Gives access to an SNMP Agent (the device we want to look at)
  - ***Essentially passwords or pre-shared key***
- Clear text (security problem but addressed in SNMPv3)
  - ***Users & Groups***
- Default for Read-Only: public
- Default for Read/Write: private
- Top 10 Most Critical Internet Security Threat
- Caution on “extreme” Community strings
  - ***Reserved characters (@ = VLAN)***
  - ***Length of string***

SNMPv1 Messages

- **5 Messages**
  - GetRequest
    - ***Used to retrieve information from an agent***
  - GetNextRequest
    - ***Used in conjunction w/ a get request to get a table of data (routing table)***
  - SetRequest
    - ***Allows remote configuration (change IP address)***
  - GetResponse
    - ***Agent's response to a get-request***
  - Trap
    - ***Unsolicited message from an agent to a manager***

SNMP Messages



SNMP Messages - Architecture

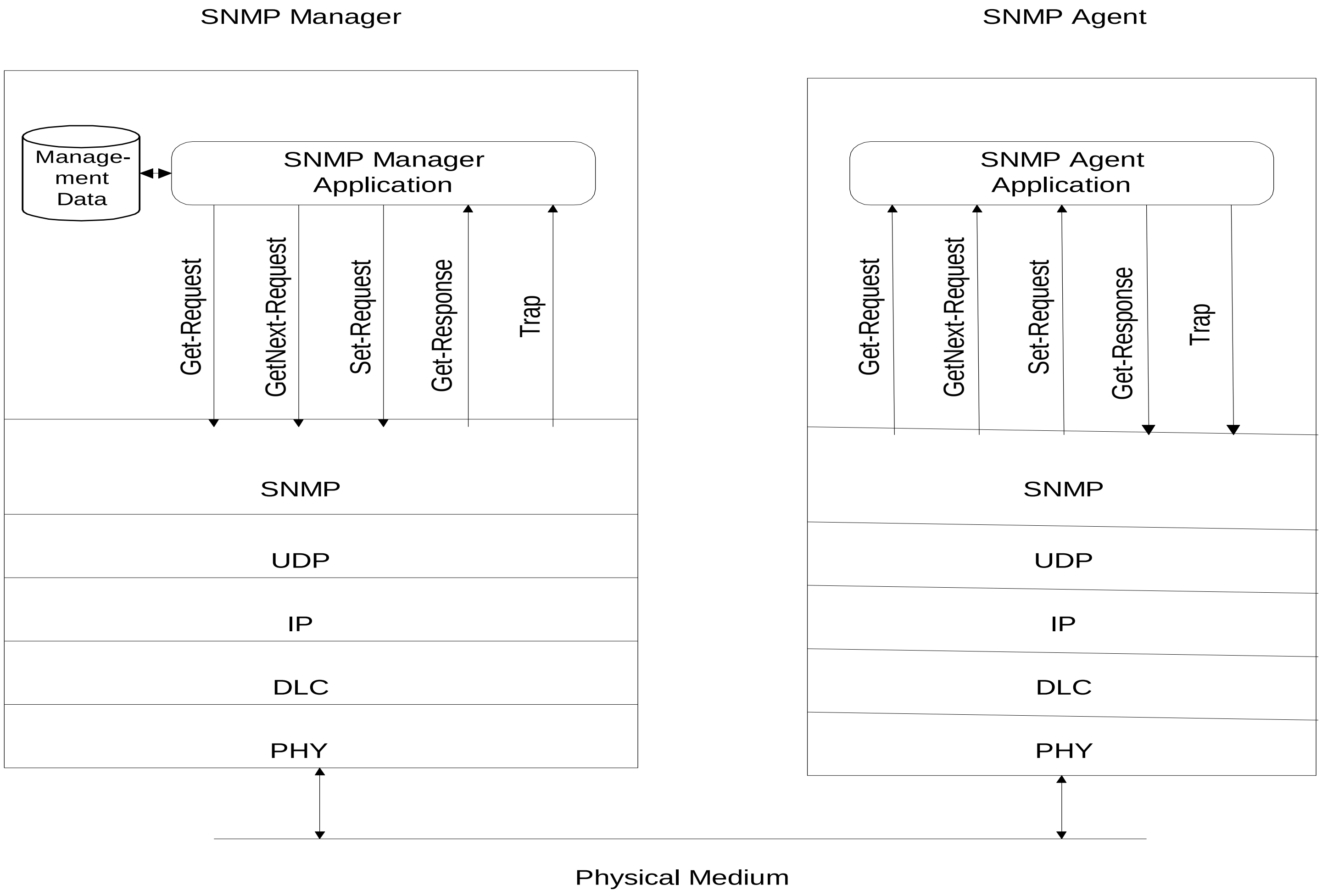


Figure 4.9 SNMP Network Management Architecture

SNMPv2 Messages

- **7 Messages**
  - GetRequest
    - ***Used to retrieve information from an agent***
  - GetNextRequest
    - ***Used in conjunction w/ a get request to get a table of data (routing table)***
  - *GetBulkRequest
  - SetRequest
    - ***Allows remote configuration (change IP address)***
  - *InformRequest
    - ***Similar to a Trap, but sent continuously until an ACK is received***
  - Response
    - ***Agent’s response to a GetRequest, SetRequest, GetNextRequest, GetBulkRequest, and InformRequest***
  - Trap
    - ***Unsolicited message from an agent to a manager***

SNMPv3 Messages

- **8 Messages**
  - GetRequest
    - ***Used to retrieve information from an agent***
  - GetNextRequest
    - ***Used in conjunction w/ a get request to get a table of data (routing table)***
  - SetRequest
    - ***Allows remote configuration (change address)***
  - GetBulkRequest
  - Response
    - ***Agent's response to a get-request, SetRequest, GetNextRequest, GetBulkRequest, and InformRequest***
  - Trap
    - ***Unsolicited message from an agent to a manager***
  - InformRequest
    - ***Similar to a Trap, but sent continuously until an ACK is received***
  - *Report PDU
    - ***Make encrypted messages more secure***

GET

```
Frame 126 (203 bytes on wire, 203 bytes captured)
Ethernet II, Src: DellEsgP_67:5f:03 (00:0b:db:67:5f:03), Dst: All-HSRP-routers_1c (00:00:0c:07:ac:1c)
Internet Protocol, Src: 172.22.67.204 (172.22.67.204), Dst: 10.19.251.224 (10.19.251.224)
User Datagram Protocol, Src Port: 1587 (1587), Dst Port: snmp (161)
Simple Network Management Protocol
    Version: 1 (0)
    Community: public
    PDU type: GET (0)
    Request Id: 0x0000267b
    Error Status: NO ERROR (0)
    Error Index: 0
    Object identifier 1: 1.3.6.1.2.1.1.1.0 (SNMPv2-MIB::sysDescr.0)
    Value: NULL
    Object identifier 2: 1.3.6.1.2.1.1.2.0 (SNMPv2-MIB::sysObjectID.0)
    Value: NULL
```

GET RESPONSE

```
Frame 127 (291 bytes on wire, 291 bytes captured)
Ethernet II, Src: 172.22.71.251 (00:30:b6:34:ca:40), Dst: DellEsgP_67:5f:03 (00:0b:db:67:5f:03)
Internet Protocol, Src: 10.19.251.224 (10.19.251.224), Dst: 172.22.67.204 (172.22.67.204)
User Datagram Protocol, Src Port: snmp (161), Dst Port: 1587 (1587)
Simple Network Management Protocol
    Version: 1 (0)
    Community: public
    PDU type: RESPONSE (2)
    Request Id: 0x0000267b
    Error Status: NO ERROR (0)
    Error Index: 0
    Object identifier 1: 1.3.6.1.2.1.1.1.0 (SNMPv2-MIB::sysDescr.0)
    Value: STRING: NetVanta 4430, Version: R11.4.3.E, Date: Thu Nov 24 16:20:50 2014
    Object identifier 2: 1.3.6.1.2.1.1.2.0 (SNMPv2-MIB::sysObjectID.0)
    Value: OID: SNMPv2-SMI::enterprises.664.1.583
```

GET-NEXT

```
Frame 43 (88 bytes on wire, 88 bytes captured)
Ethernet II, Src: DellEsgP_67:5f:03 (00:0b:db:67:5f:03), Dst: All-HSRP-routers_1c (00:00:0c:07:ac:1c)
Internet Protocol, Src: 172.22.67.204 (172.22.67.204), Dst: 10.19.251.224 (10.19.251.224)
User Datagram Protocol, Src Port: 1616 (1616), Dst Port: snmp (161)
Simple Network Management Protocol
    Version: 1 (0)
    Community: public
    PDU type: GET-NEXT (1)
    Request Id: 0x00002ea5
    Error Status: NO ERROR (0)
    Error Index: 0
    Object identifier 1: 1.3.6.1.2.1 (SNMPv2-SMI::mib-2)
    Value: NULL
```

GET-NEXT RESPONSE

```
Frame 44 (152 bytes on wire, 152 bytes captured)
Ethernet II, Src: 172.22.71.251 (00:30:b6:34:ca:40), Dst: DellEsgP_67:5f:03 (00:0b:db:67:5f:03)
Internet Protocol, Src: 10.19.251.224 (10.19.251.224), Dst: 172.22.67.204 (172.22.67.204)
User Datagram Protocol, Src Port: snmp (161), Dst Port: 1616 (1616)
Simple Network Management Protocol
    Version: 1 (0)
    Community: public
    PDU type: RESPONSE (2)
    Request Id: 0x00002ea5
    Error Status: NO ERROR (0)
    Error Index: 0
    Object identifier 1: 1.3.6.1.2.1.1.1.0 (SNMPv2-MIB::sysDescr.0)
    Value: STRING: NetVanta 6355, Version: R11.05.00.E, Date: Thu Nov 24 16:20:50 2010
```

SET

```
Frame 52 (88 bytes on wire, 88 bytes captured)
Ethernet II, Src: DellEsgP_67:5f:03 (00:0b:db:67:5f:03), Dst: All-HSRP-routers_1c (00:00:0c:07:ac:1c)
Internet Protocol, Src: 172.22.67.204 (172.22.67.204), Dst: 10.19.251.224 (10.19.251.224)
User Datagram Protocol, Src Port: 1803 (1803), Dst Port: snmp (161)
Simple Network Management Protocol
    Version: 1 (0)
    Community: private
    PDU type: SET (3)
    Request Id: 0x00000206
    Error Status: NO ERROR (0)
    Error Index: 0
    Object identifier 1: 1.3.6.1.2.1.1.4.0 (SNMPv2-MIB::sysContact.0)
    Value: STRING: LEVI
```

SET RESPONSE

```
Frame 53 (88 bytes on wire, 88 bytes captured)
Ethernet II, Src: 172.22.71.251 (00:30:b6:34:ca:40), Dst: DellEsgP_67:5f:03 (00:0b:db:67:5f:03)
Internet Protocol, Src: 10.19.251.224 (10.19.251.224), Dst: 172.22.67.204 (172.22.67.204)
User Datagram Protocol, Src Port: snmp (161), Dst Port: 1803 (1803)
Simple Network Management Protocol
    Version: 1 (0)
    Community: private
    PDU type: RESPONSE (2)
    Request Id: 0x00000206
    Error Status: NO ERROR (0)
    Error Index: 0
    Object identifier 1: 1.3.6.1.2.1.1.4.0 (SNMPv2-MIB::sysContact.0)
    Value: STRING: LEVI
```

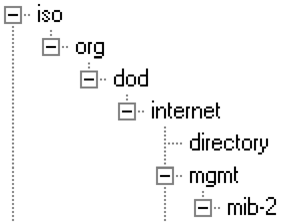
RESPONSE ERROR

```
Frame 44 (92 bytes on wire, 92 bytes captured)
Ethernet II, Src: 172.22.71.251 (00:30:b6:34:ca:40), Dst: DellEsgP_67:5f:03 (00:0b:db:67:5f:03)
Internet Protocol, Src: 10.19.251.224 (10.19.251.224), Dst: 172.22.67.204 (172.22.67.204)
User Datagram Protocol, Src Port: snmp (161), Dst Port: 1632 (1632)
Simple Network Management Protocol
    Version: 1 (0)
    Community: private
    PDU type: RESPONSE (2)
    Request Id: 0x00002ec9
    Error Status: NO SUCH NAME (2)
    Error Index: 1
    Object identifier 1: 1.3.6.1.2.1.1.4 (SNMPv2-MIB::sysContact)
    Value: STRING: Levi Test
```

MIBs

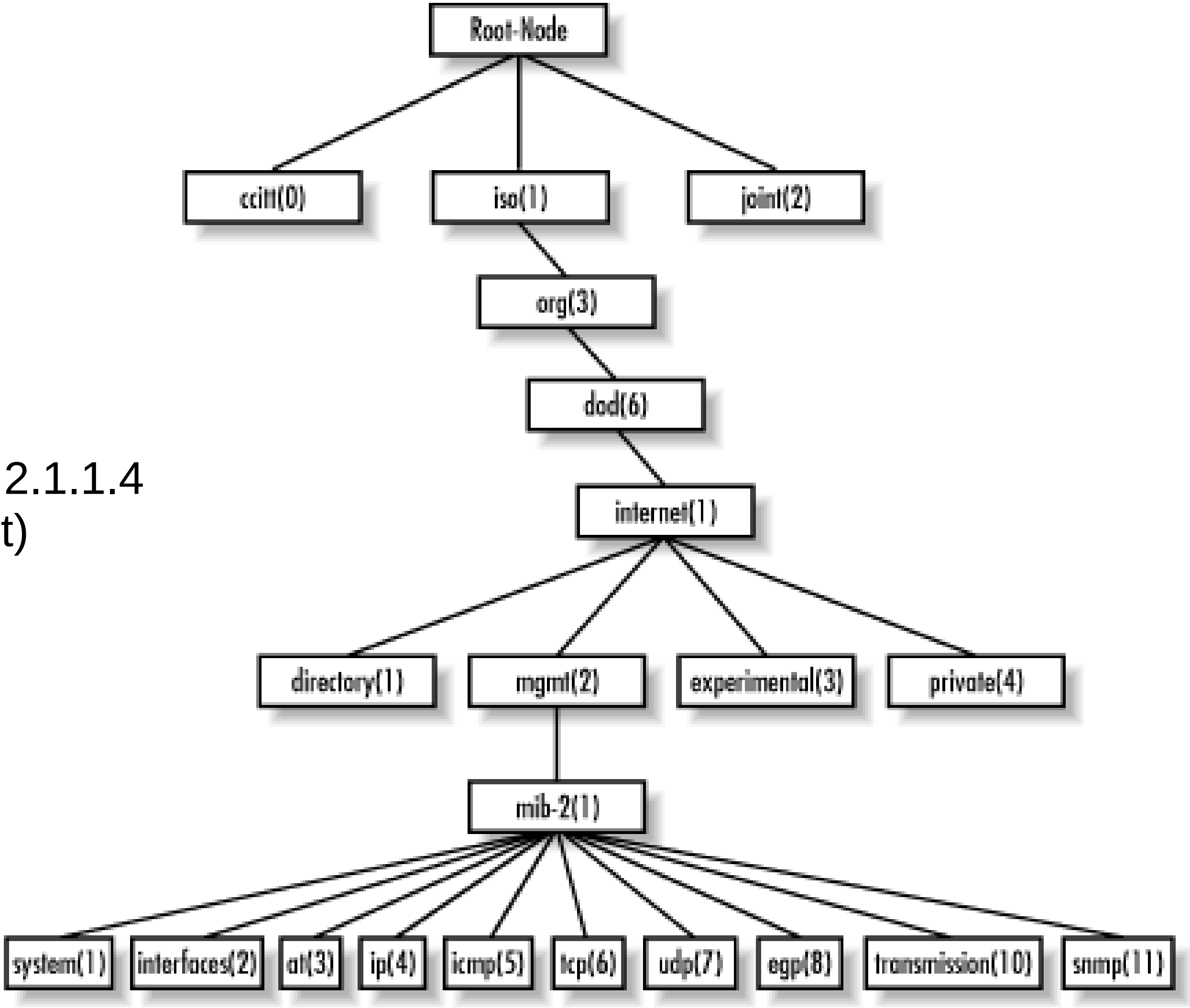
- **Provided by “<u>manufacturer</u>” and loaded/installed on NMS (server) and extracted**
- **Define managed objects and their behavior**
- **A database of objects and agent tracks**
  - i.e. what devices are connected to ports of my switch
- **Written in ASN.1 and are clear text**
- **Must be compiled by the NMS before use (each NMS has its own way of compiling)**

SNMP MIB



```
⊟ iso
   ⊟ org
      ⊟ dod
         ⊟ internet
            directory
            ⊟ mgmt
               ⊟ mib-2
```

Object identifier 1: 1.3.6.1.2.1.1.4
(SNMPv2-MIB::sysContact)



Traps

- A message (alert) sent from an SNMP agent to a NMS (SNMP Monitor) because a certain (<u>triggered</u>) event occurred

- This allows the device to send a message to a monitor saying
  - “Hey I’m OK” or “Hey I’m Having Problems” without the monitor always polling the device

- User/Admin defined
  - “What do I want to be alerted about?”

Traps

- Events are defined in the MIB for the device

- Configured on each Agent

- Concept / Network Design - Proactive vs. Reactive Traps
  - Link down vs. Fan failure

Troubleshooting

- **Troubleshooting - Bottom Up vs Top Down**
  - CCNP TSHOOT

- **Can you ping the device from the NMS?**
  - No route to NMS

- **Can the device ping the NMS?**
  - Why could you ping agent, but agent couldn’t ping NMS?

- **You can browse the MIB on the device (from the NMS) but don’t receive traps**
  - Traps enabled?
  - SNMP server IP address configured? Configured correctly?
  - Firewall?
  - Source IP address or Loopback

Troubleshooting

- **Are the community strings set?**
  - Do they match? Case sensitive?

- **Do you need to specify a *source interface* on the agent?**
  - Draw

- **Note: SNMP walk of all the entries in the MIB, can crash the device (or the network)**

Troubleshooting

- **Cisco SNMP commands reference: http://www.cisco.com/c/en/us/td/docs/ios/12_2/configfun/command/reference/ffun_r/frf014.html**

```
Router# show snmp
Chassis: 01506199
37 SNMP packets input
0 Bad SNMP version errors
4 Unknown community name
0 Illegal operation for community name supplied
0 Encoding errors
24 Number of requested variables
0 Number of altered variables
0 Get-request PDUs
28 Get-next PDUs
0 Set-request PDUs
78 SNMP packets output
0 Too big errors (Maximum packet size 1500)
0 No such name errors
0 Bad values errors
0 General errors
24 Response PDUs
   13 Trap PDUs
```

SNMP and NMS Software

- **Nagios**
  - Open Source; Free
  - CLI based
    - ***GUI Display/Reporting***
- **SolarWinds**
  - Popular in industry (expensive)
  - Arguably best all-around solution
- **Cacti**
  - Network Graphing solution

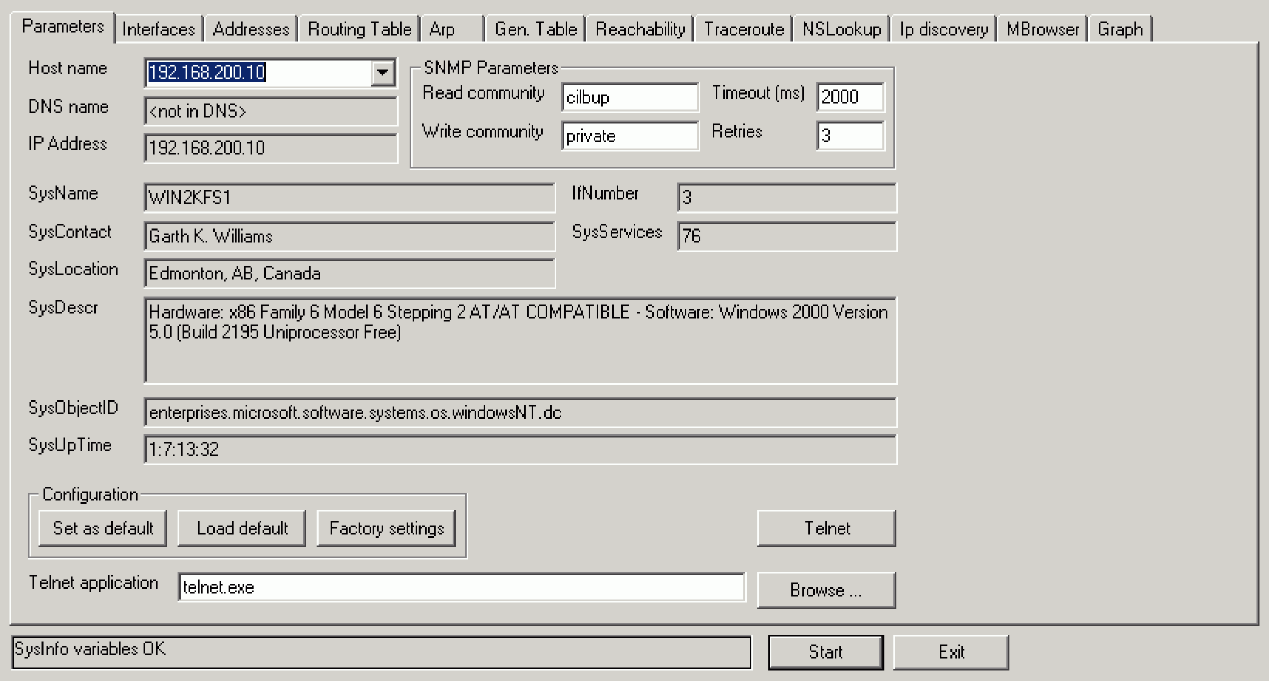
Continued…

- **WhatsUPGold**
  - Popular in industry (expensive)

- **Network Management Information System (NMIS)**
  - FOSS
  - GUI based

SNMP and NMS Software

- **Free/basic SNMP Software**
  - – Getif (MIB browser)
  - – Net-snmp



Host name: 192.168.200.10

DNS name: <not in DNS>

IP Address: 192.168.200.10

SNMP Parameters

Read community: cilbup

Write community: private

Timeout (ms): 2000

Retries: 3

SysName: WIN2KFS1

SysContact: Garth K. Williams

SysLocation: Edmonton, AB, Canada

IfNumber: 3

SysServices: 76

SysDescr: Hardware: x86 Family 6 Model 6 Stepping 2 AT/AT COMPATIBLE - Software: Windows 2000 Version 5.0 (Build 2195 Uniprocessor Free)

SysObjectID: enterprises.microsoft.software.systems.os.windowsNT.dc

SysUpTime: 1:7:13:32

Configuration

Telnet application: telnet.exe

SysInfo variables OK

SNMP - Python

Questions?