Remote Monitoring and Management of Networks

Lecture weeks 32/33

Switch monitoring, port mirroring, SNMP

Outline

- Introduction
- Network monitoring
- Port mirroring
- Distributed monitoring
- Simple Network Management Protocol (SNMP)
- Remote Monitoring (RMON)

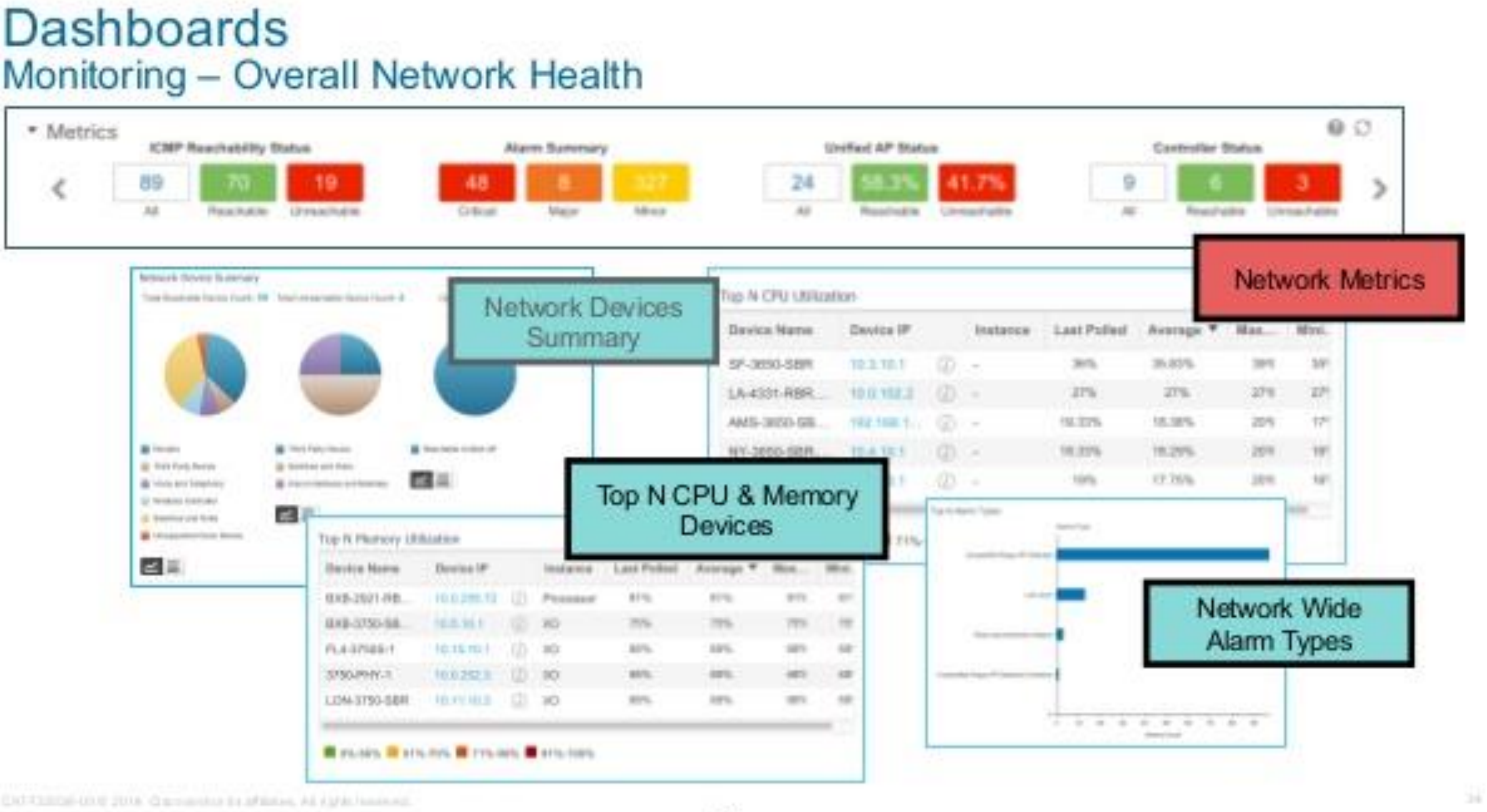
Learning Objectives

- Understanding of various network monitoring techniques.
- Understanding of SNMP and its implementation.
- Understanding of RMON and its implementation.

Introduction

- Monitoring large switched or routed networks can pose many administration problems.
- Some network analyzers tools are designed to overcome these problems and are mostly built into Business management suites such as Microsoft SCCM (System Center Configuration Manager), HP BTO (Business Technology Optimization), Cisco Prime, etc.
- In most cases the standard SNMP/RMON protocols are employed to capture and analyze the network traffic.
- Network faults or problems related to performance, uptime or availability of system components need to be analyzed.

Cisco Prime



Dashboards

Monitoring – Overall Network Health

Top N CPU Utilization

Device Name	Device IP		Instance	Last Polled	Average ▼	Max...	Mini...
SF-3850-SBR	10.3.10.1	ⓘ	-	36%	35.83%	38%	[illegible]
LA-4331-RBR...	10.0.102.2	ⓘ	-	27%	27%	27%	27
AMS-3850-GB...	192.168.1...	ⓘ	-	15.33%	15.38%	25%	17
NY-3850-SBR...	10.4.10.1	ⓘ	-	18.33%	18.29%	25%	18
[illegible]	[illegible]	ⓘ	-	19%	17.75%	25%	[illegible]

Top N Memory Utilization

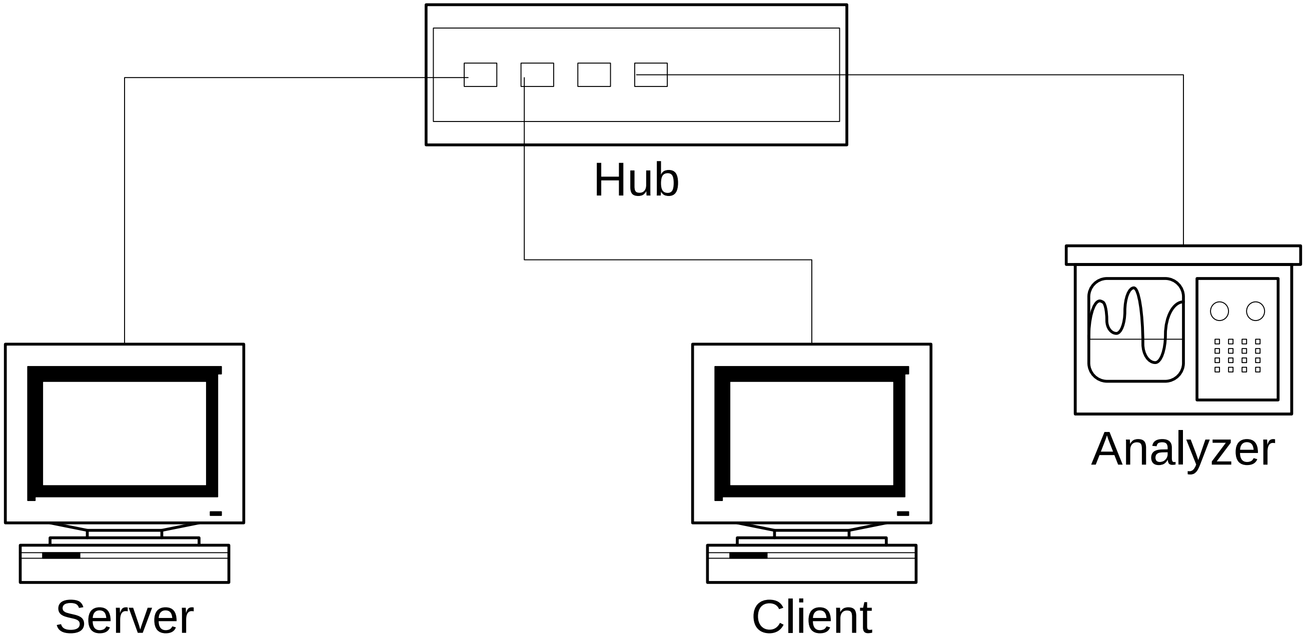
Device Name	Device IP		Instance	Last Polled	Average ▼	Max...	Mini...
BXB-2921-RB...	10.0.255.12	ⓘ	Processor	81%	81%	81%	[illegible]
BXB-3750-SB...	10.5.10.1	ⓘ	IO	75%	75%	75%	[illegible]
FL4-3750E8-1	10.15.10.1	ⓘ	IO	[illegible]	[illegible]	[illegible]	[illegible]
3750-PHY-1	10.0.252.3	ⓘ	IO	[illegible]	[illegible]	[illegible]	[illegible]
LON-3750-SBR	10.11.10.2	ⓘ	IO	[illegible]	[illegible]	[illegible]	[illegible]

🟩 [illegible] 🟨 [illegible] 🟧 [illegible] 🟥 [illegible]

Analyzer Types

- Network analyzers can be standalone or distributed.
- Stand-alone analyzers have no difficulty monitoring or capturing data on a simple shared LAN segments
- The analyzer is just plugged into a spare port on the hub to see all unicast and broadcast traffic on the segment (providing it can operate in promiscuous mode).
- May need special NIC/drivers to analyse errors

Shared LAN Analysis

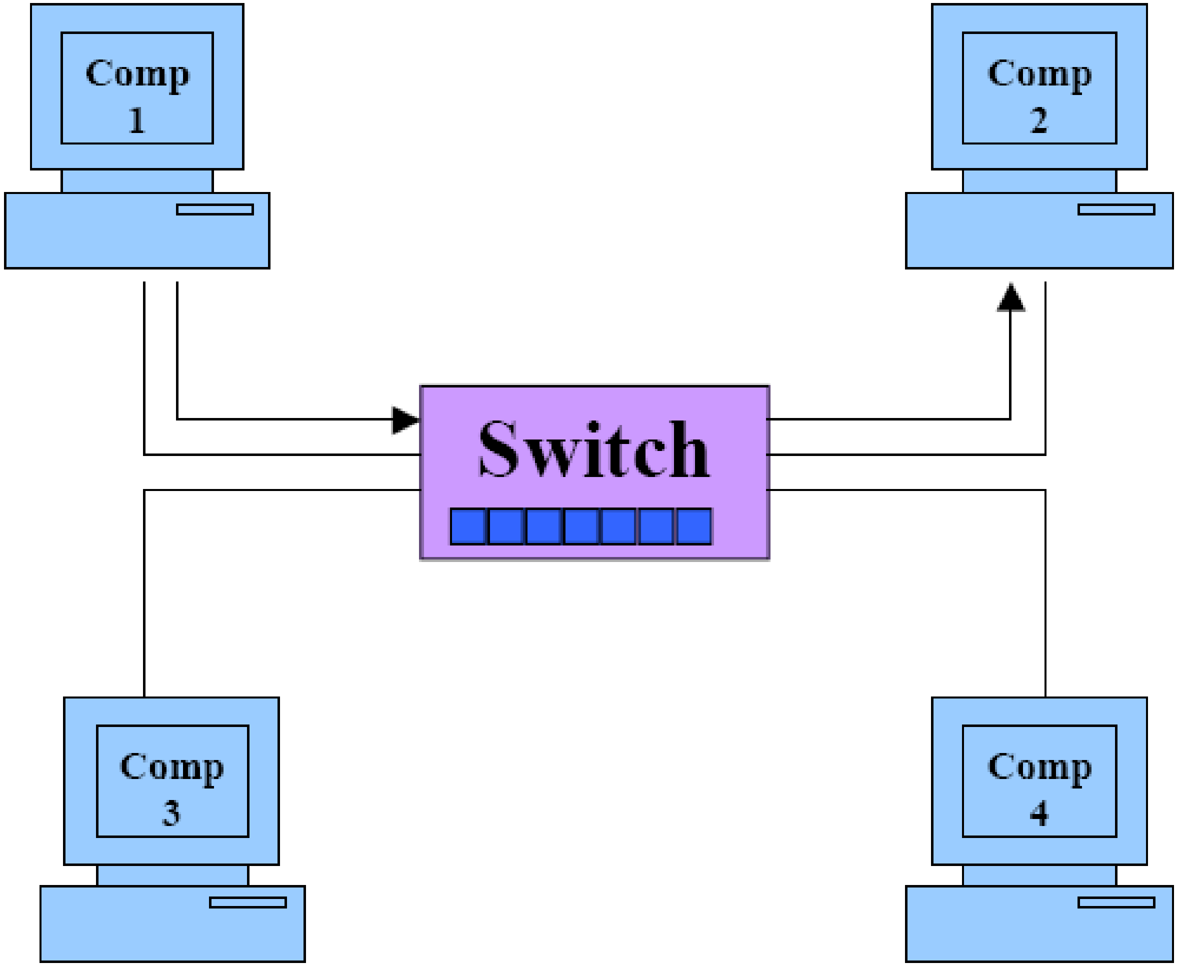


Multi-segment Problems

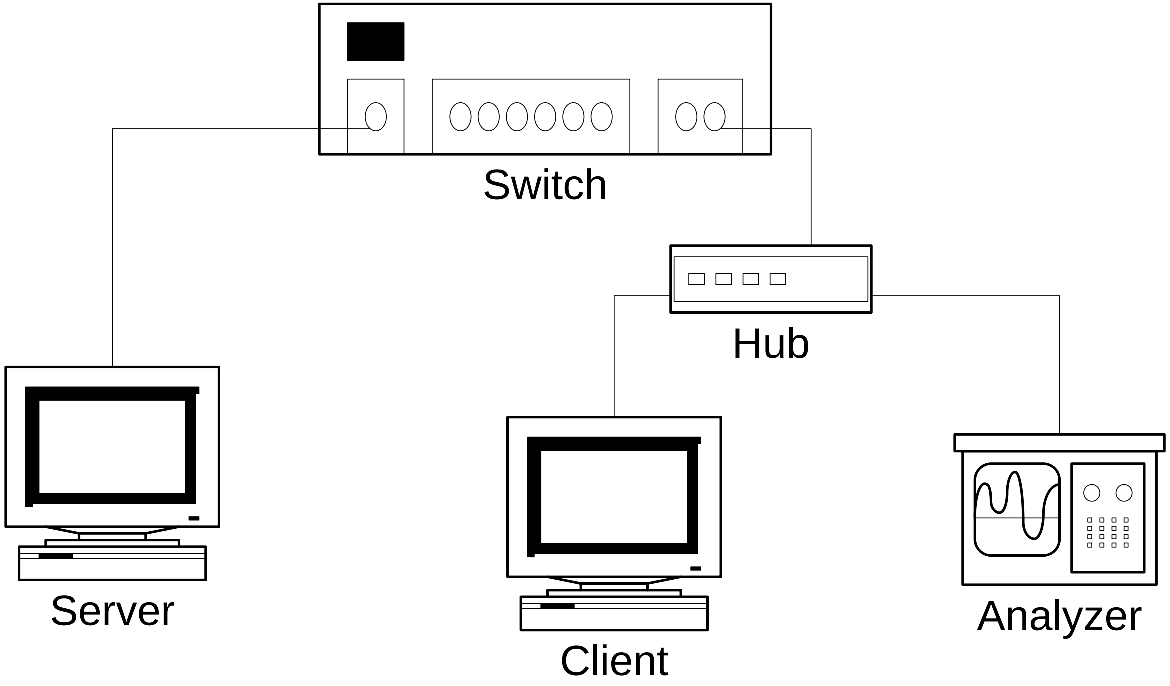
- Multi-segment networks containing switches pose problems because only broadcasts are detectable.

- You could use a portable mini hub to tap into the point to point connection:

Switched Network



Monitoring a switched Link with a hub



Here the communication between the client and server is being monitored by sharing the server connection with the analyzer.

NB. Hubs are half-duplex (HDX) not suitable for full-duplex (FDX) links and you have to disconnect the link to insert the hub

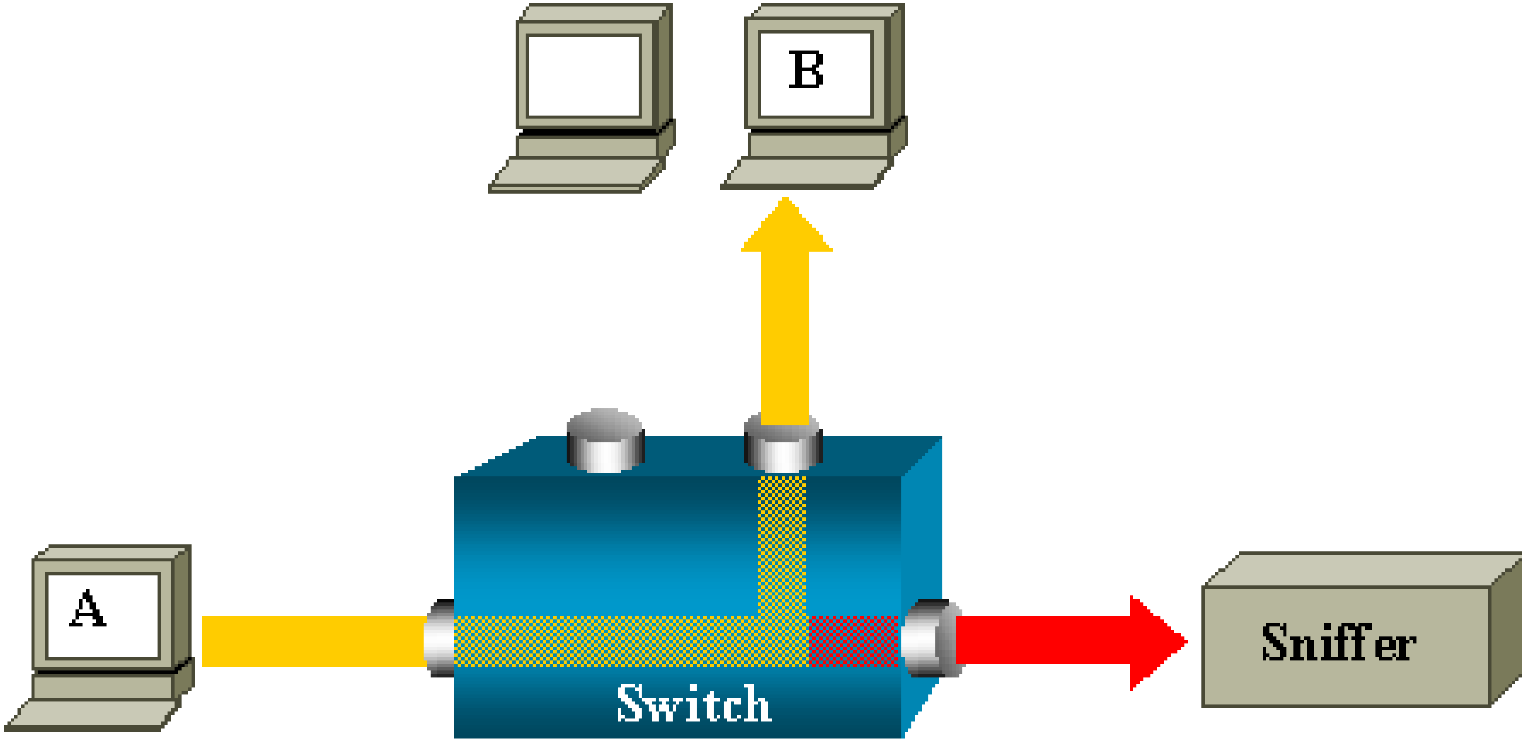
Monitoring a Switch port

- 3 ways for an analyser to gain access:
- Port mirror (or SPAN)
- Port aggregator
- TAP (test access port)

Port Mirroring

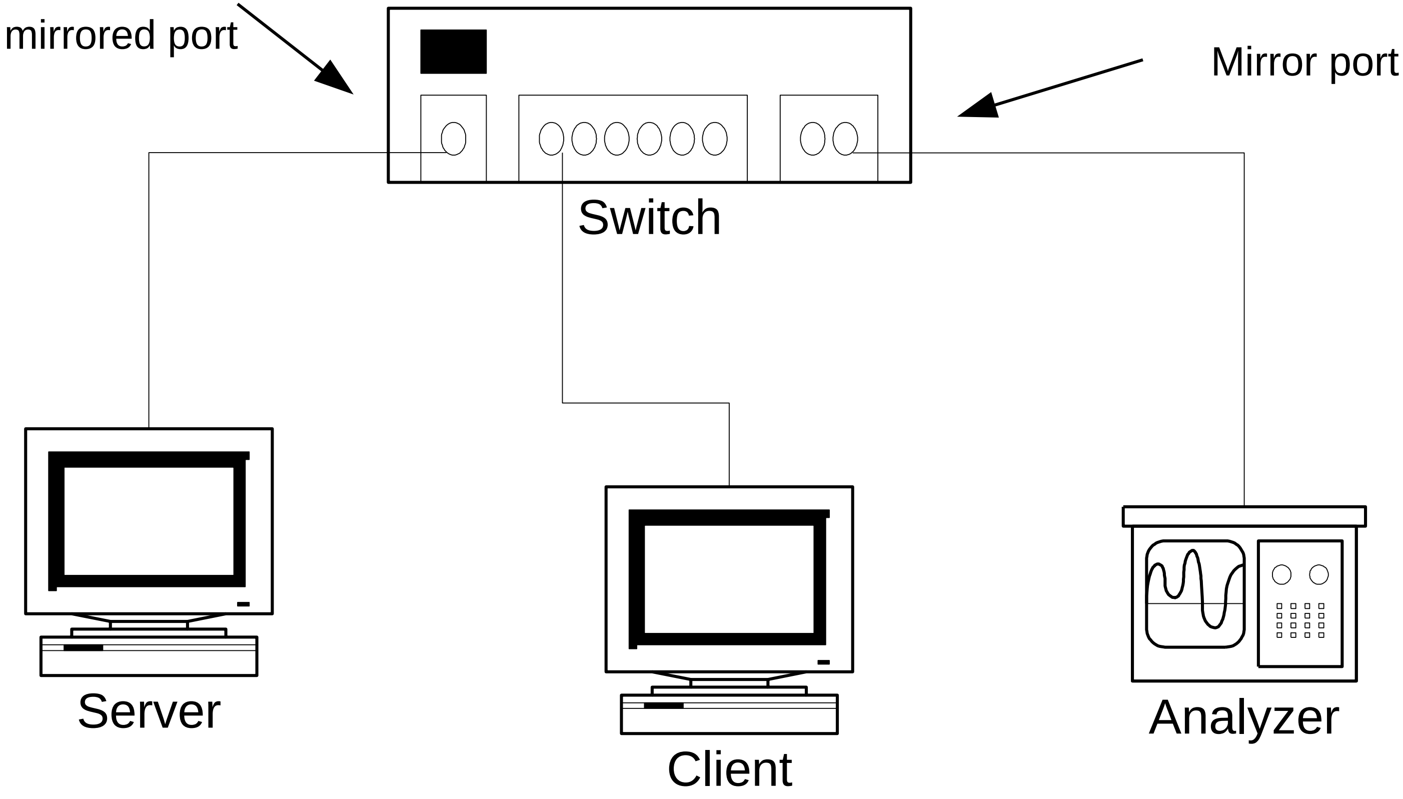
- Most managed switches have feature called port mirroring that enables a port to be specified for monitoring
- The hub is not required and it will see FDX
- You don't need to disconnect the link
- But, some traffic may not be seen by the mirror port - such as error frames and VLAN tags
- Only up to 50% utilisation on FDX

Port Mirroring

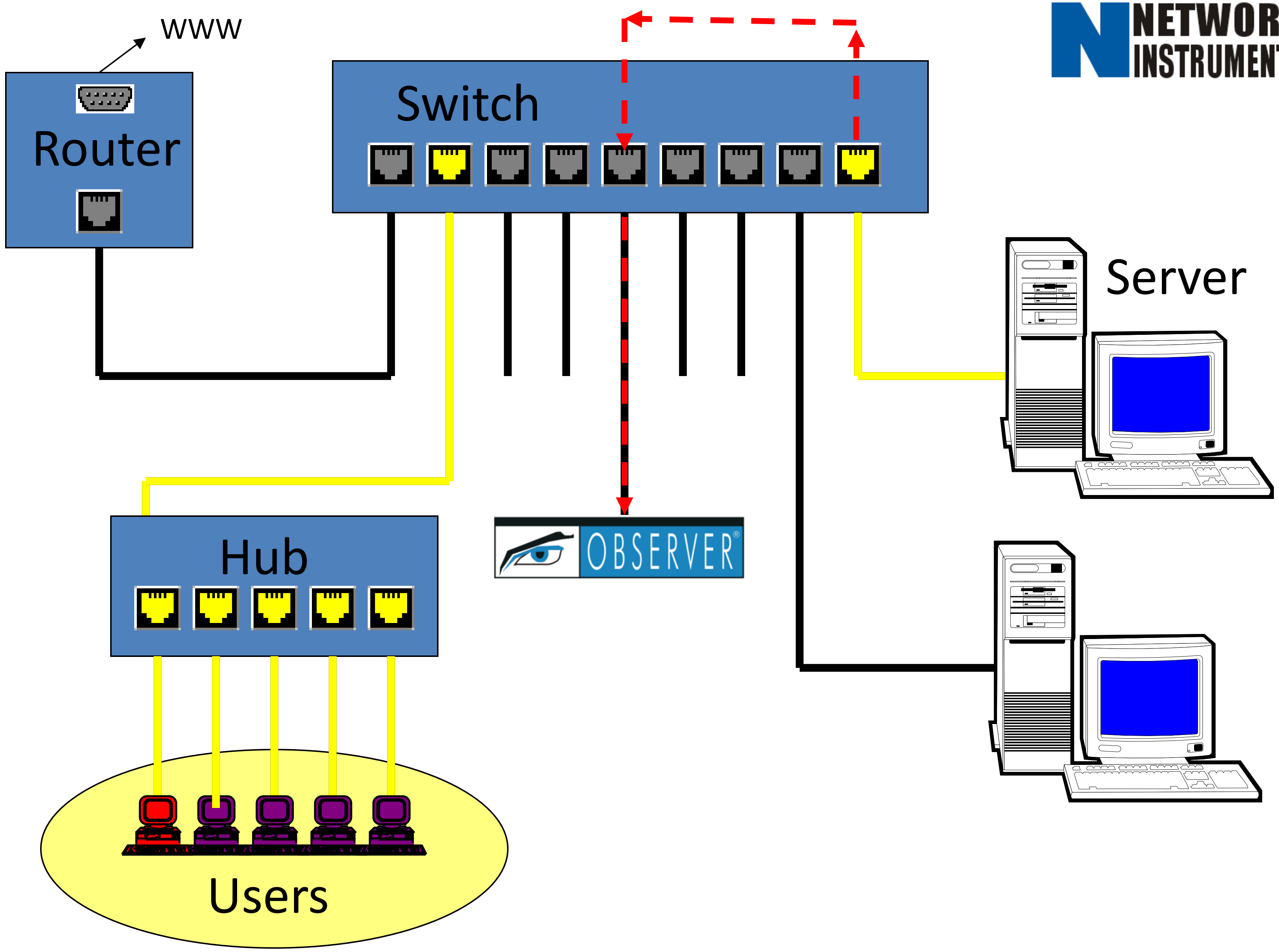


In this diagram, the sniffer is attached to a port that is configured to receive a copy of every packet that host A sends. This port is called a mirror or monitor port or a SPAN port by Cisco.

Monitoring a Switched Link with a Port Mirror



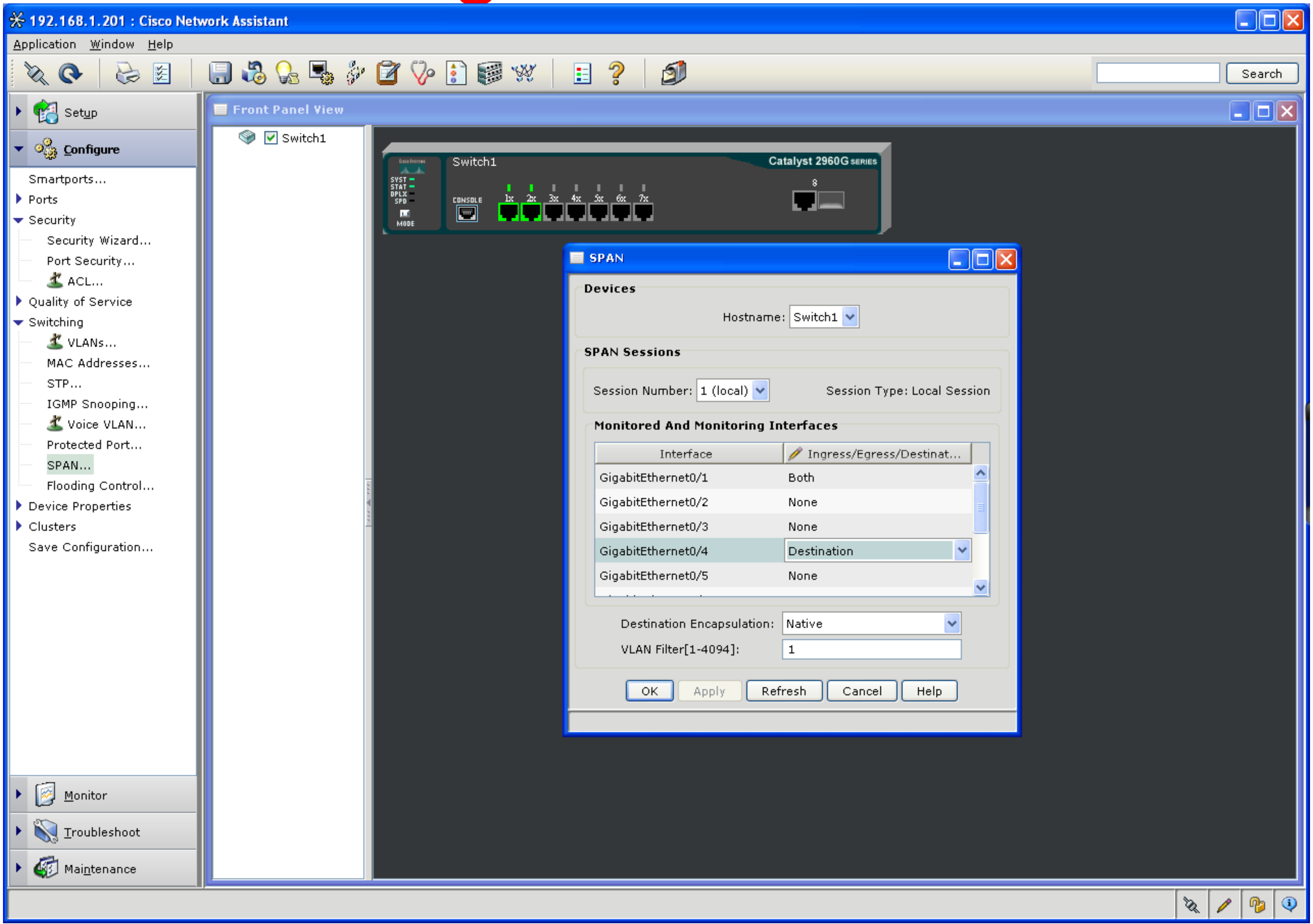
Server link is being monitored via the mirror port connected to the analyzer


WWW
Router
Switch
Server
Hub
OBSERVER
Users

Cisco SPAN

- The Switched Port ANalyzer (SPAN) feature is what Cisco called port mirroring
- It selects network traffic for analysis by a network analyzer for managed switches such as the 2960
- The following diagram shows how to configure a mirror (SPAN) port on a 2960 using the Cisco Network Assistant (CNA)

Configure a SPAN Port



Devices

Hostname: Switch1

SPAN Sessions

Session Number: 1 (local)

Session Type: Local Session

Monitored And Monitoring Interfaces

Interface	Ingress/Egress/Destinat...
GigabitEthernet0/1	Both
GigabitEthernet0/2	None
GigabitEthernet0/3	None
GigabitEthernet0/4	Destination
GigabitEthernet0/5	None

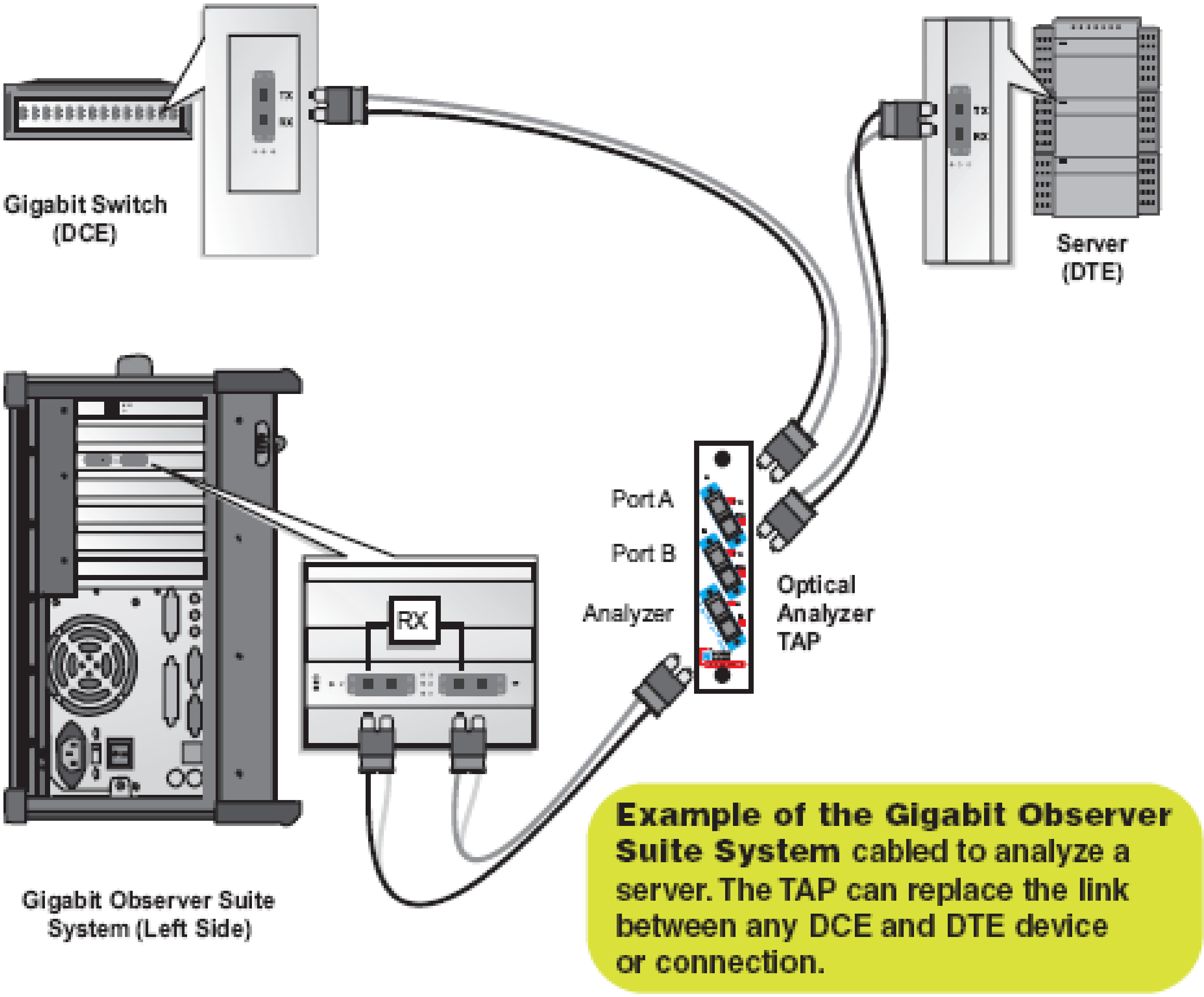
Destination Encapsulation: Native

VLAN Filter[1-4094]: 1

Port Taps

- Are special purpose copper or optical splitters for monitoring switch ports.
- They provide complete visibility of all traffic on the link being tapped (dual receivers to get both FDX channels at full utilization).
- Sit in-line with the link and are often left in place.
- The network tap has at least three ports -- an **A** port, a **B** port, and a **monitor** port.
- Tap passes through all traffic between A and B, but also copies the traffic between A and B to its monitor port, enabling a third party to listen.
- They are non-obtrusive, are not detectable on the network, can deal with full-duplex and non-shared networks, and will usually *pass-through* traffic even if the tap stops working or loses power.

Optical Splitter (in line tap)

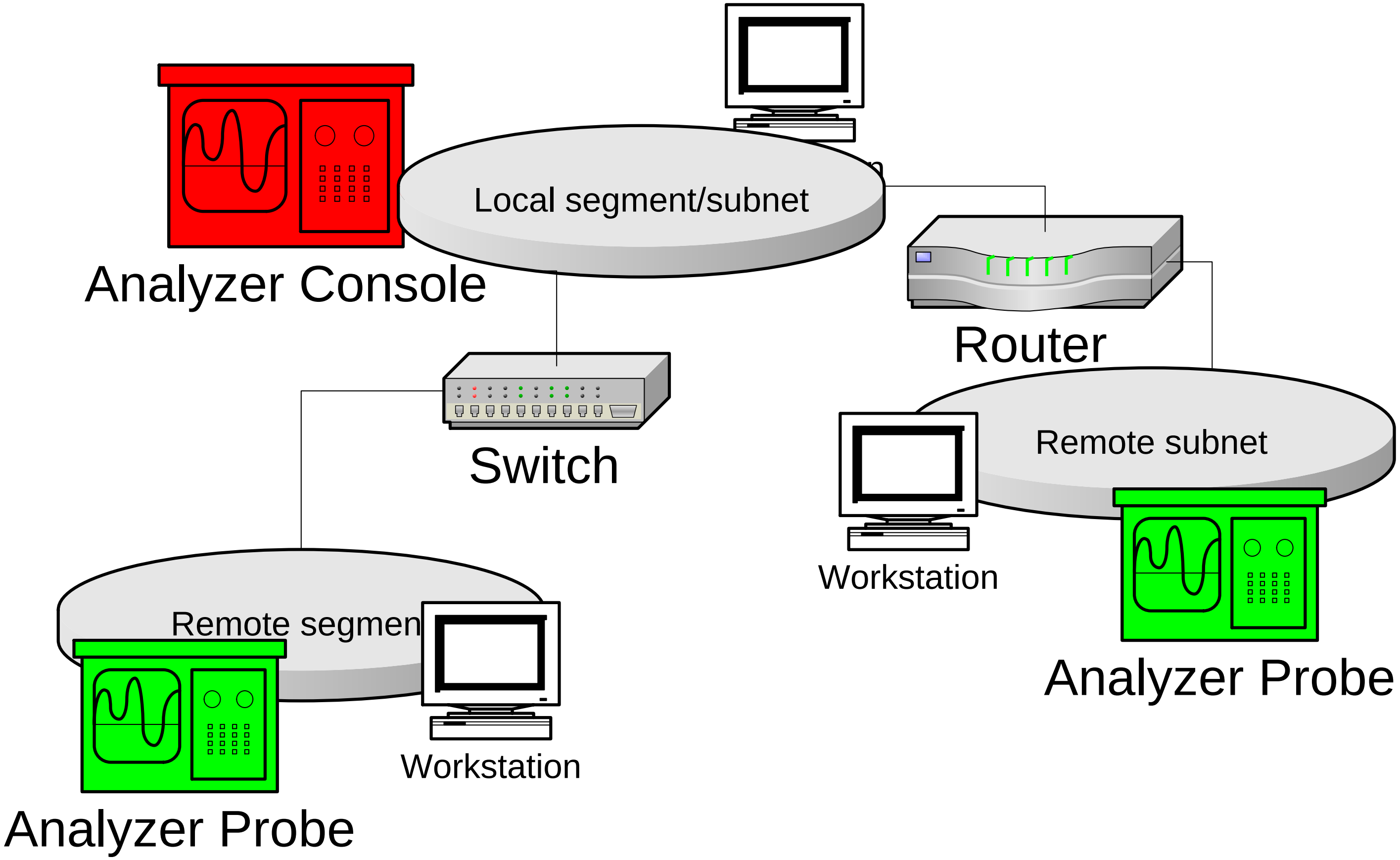


Example of the Gigabit Observer Suite System cabled to analyze a server. The TAP can replace the link between any DCE and DTE device or connection.

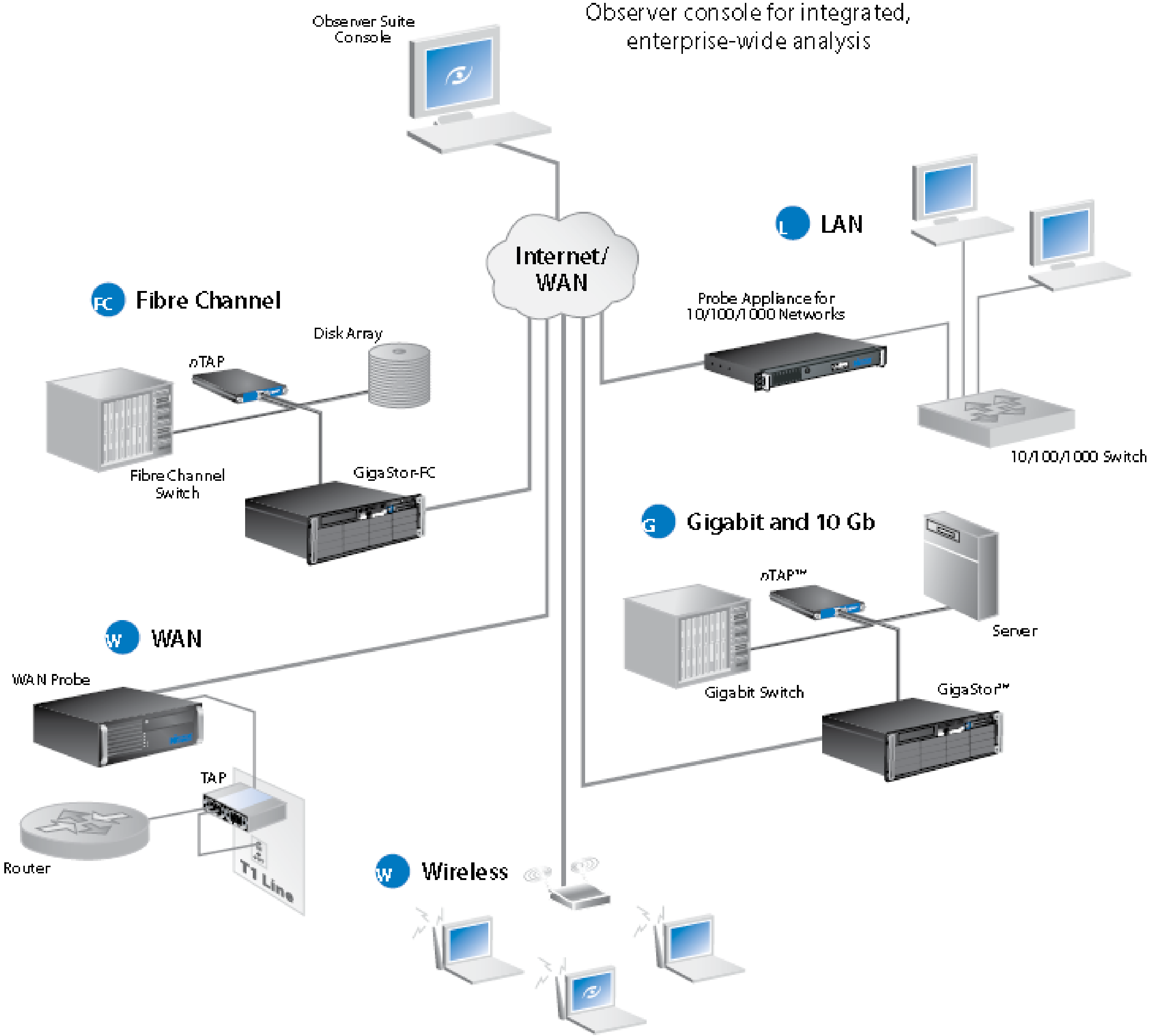
Distributed Analyzers

- Distributed Analyzers such as Observer or Sniffer actually contain two components:
  - An analyzer console to gather and analyze the captured data, and
  - A remote probes to send data from devices or PCs on other parts of the network.
- The combination shown overcomes the multi-segment analysis problem.

Multi-segment Analysis

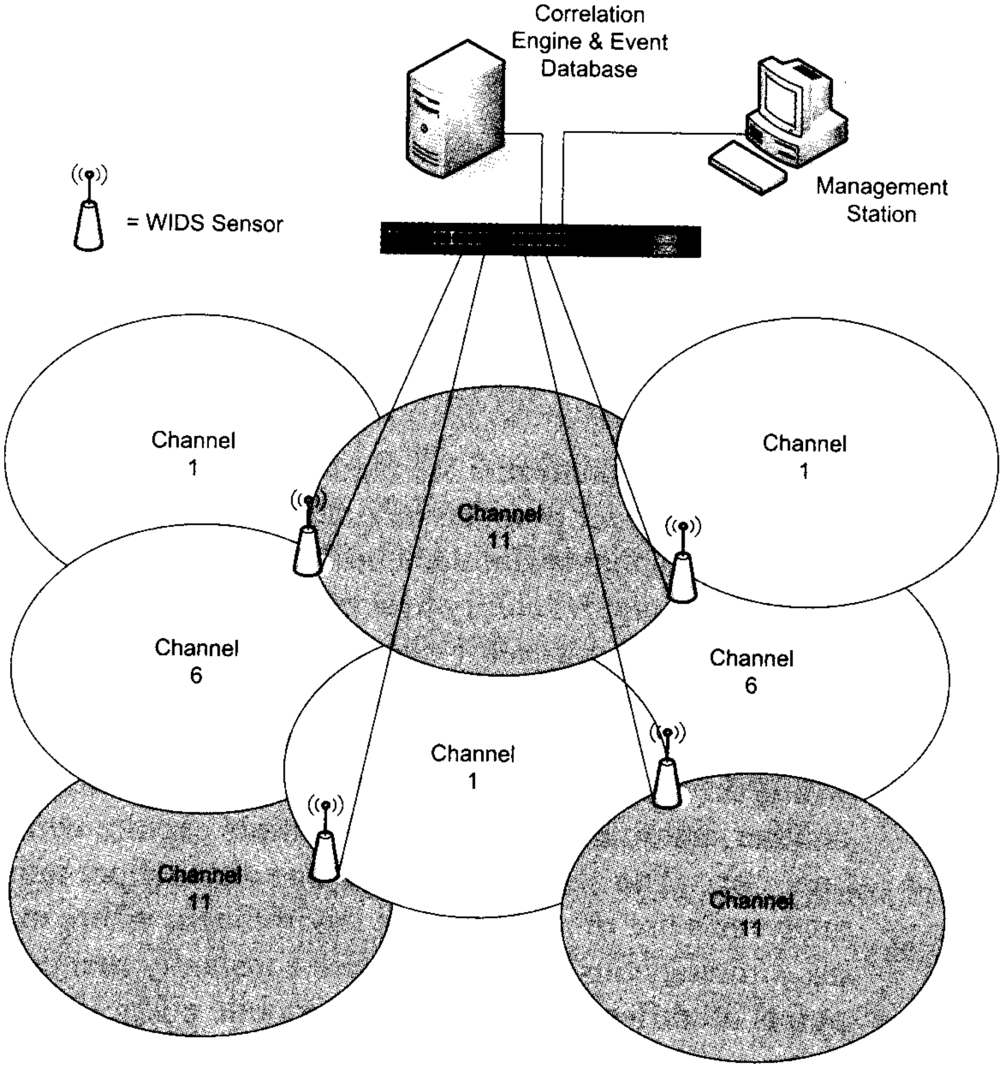


Distributed Observer Options



All probes report back to the Observer console for integrated, enterprise-wide analysis

Wireless Distributed Monitoring and Analysis



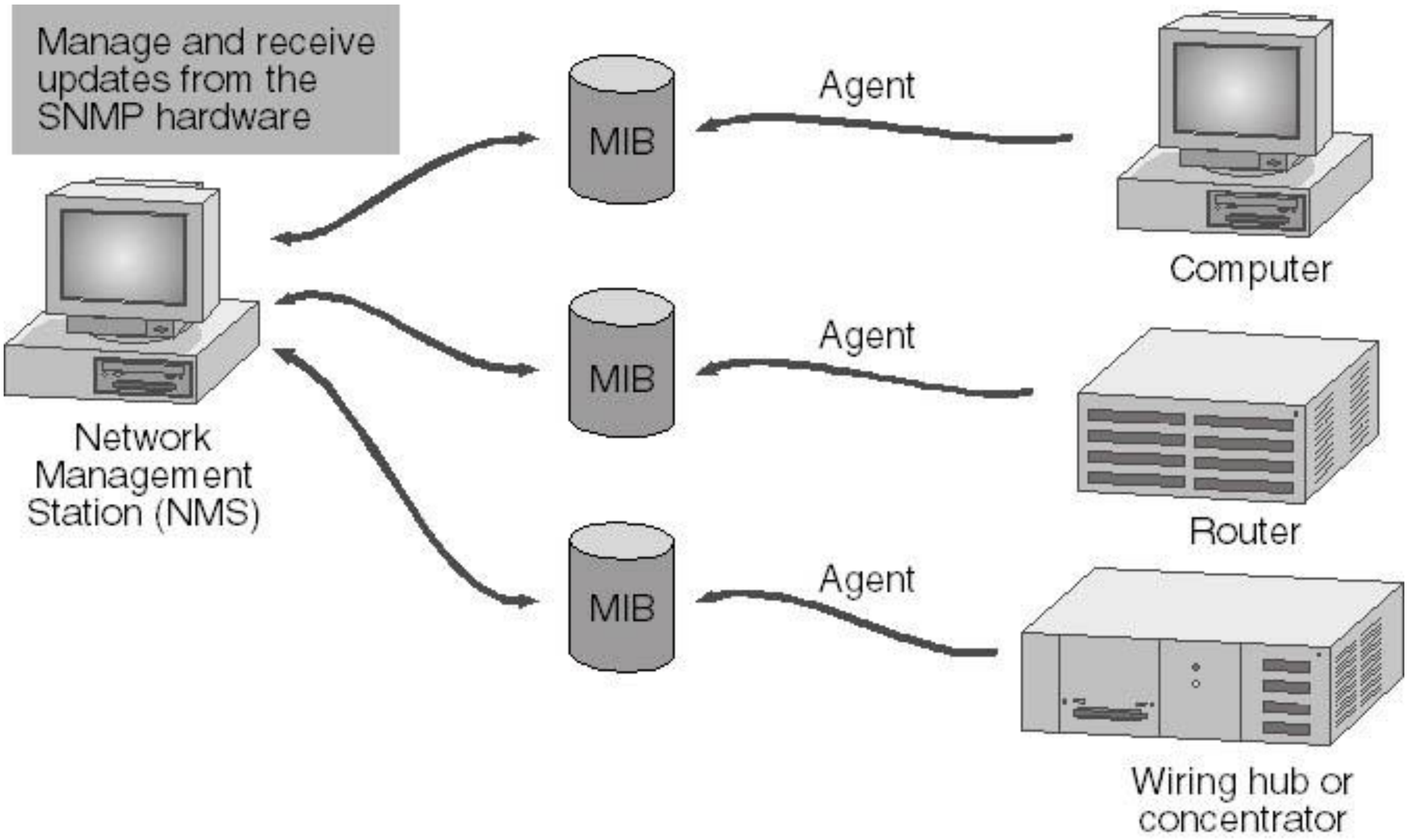
Need for Management

- As the size and complexity of networks increases so does the difficulty of monitoring.
- For large and enterprise networks sophisticated network management suites are used to monitor and track all aspects of network activity.
- These packages are based on the industry standard SNMP and RMON protocols.

Simple Network Management Protocol

- SNMP is a large-scale tool for measuring and monitoring networks.
- SNMP1, 2 and 3(secured) versions
- SNMP uses two network devices:
  - An agent that runs on client computers or other networking components such as hubs, routers, switches etc. to monitor their status, and
  - A manager which polls clients and summarizes data.
- Alerts can be set to inform the administrator of any problems.

SNMP Components


Manage and receive updates from the SNMP hardware
MIB
MIB
MIB
Agent
Agent
Agent
Computer
Router
Wiring hub or concentrator
Network Management Station (NMS)

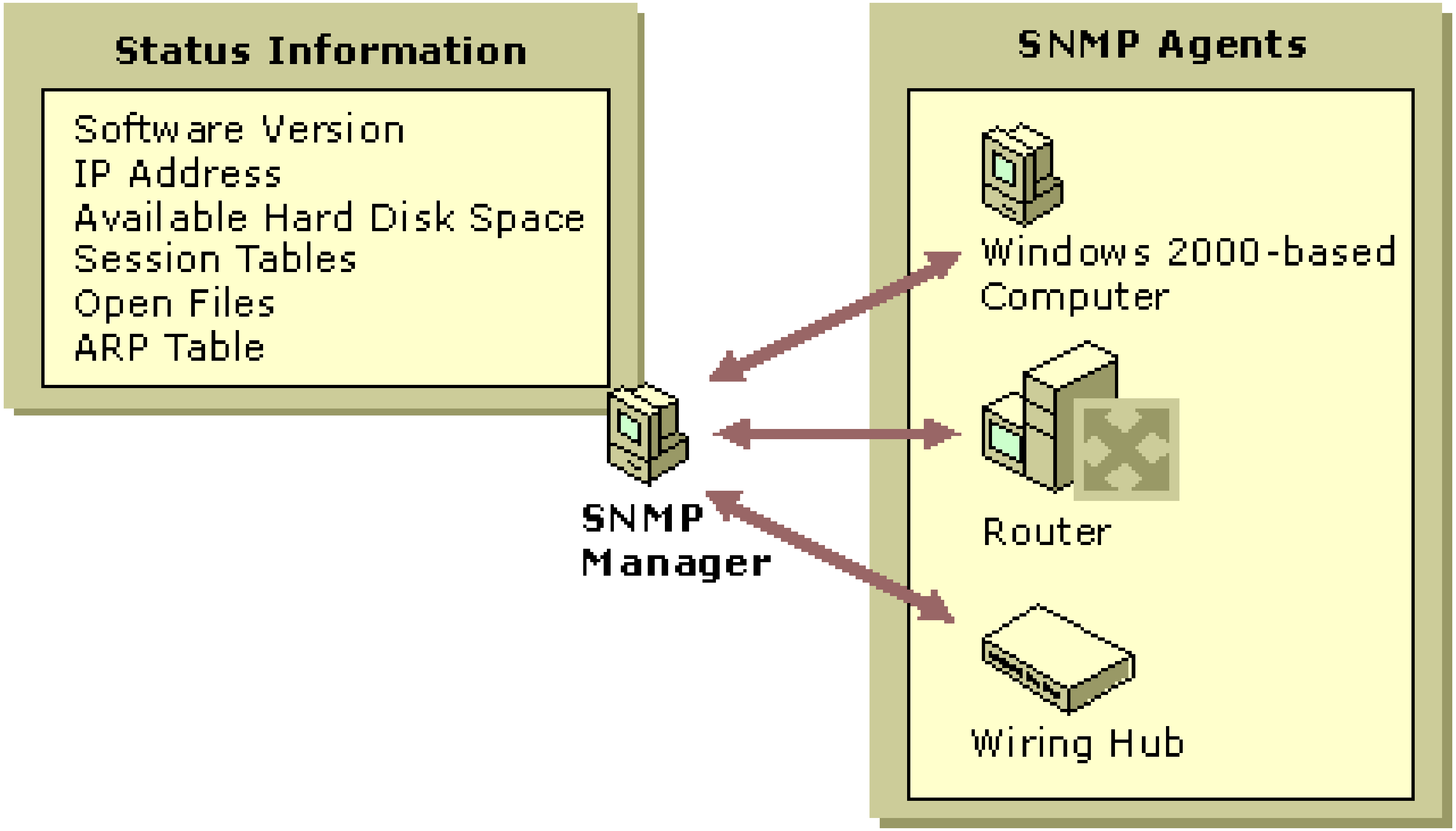
SNMP Managers

- The network management station (NMS) does not have to run on the same computer as the SNMP agents.
- The NMS can request the information from SNMP agents using SNMP request messages.

SNMP Information

- Network protocol identification and statistics
- Hardware and software configuration data
- Device performance and usage statistics
- Device error and event messages
- Program and application usage statistics
- The management system can also send a configuration request to the agent that requests the agent to change a local parameter.

Status Info



Status Information

Software Version
IP Address
Available Hard Disk Space
Session Tables
Open Files
ARP Table

SNMP Manager

SNMP Agents

Windows 2000-based Computer

Router

Wiring Hub

SNMP Agents

- SNMP agents supply information about activities that occur at network layer and respond to management system requests for information.
- The agent service can be configured to determine what statistics are to be tracked and what management systems are authorized to request information.
- In general, agents do not originate messages; they only respond to messages.

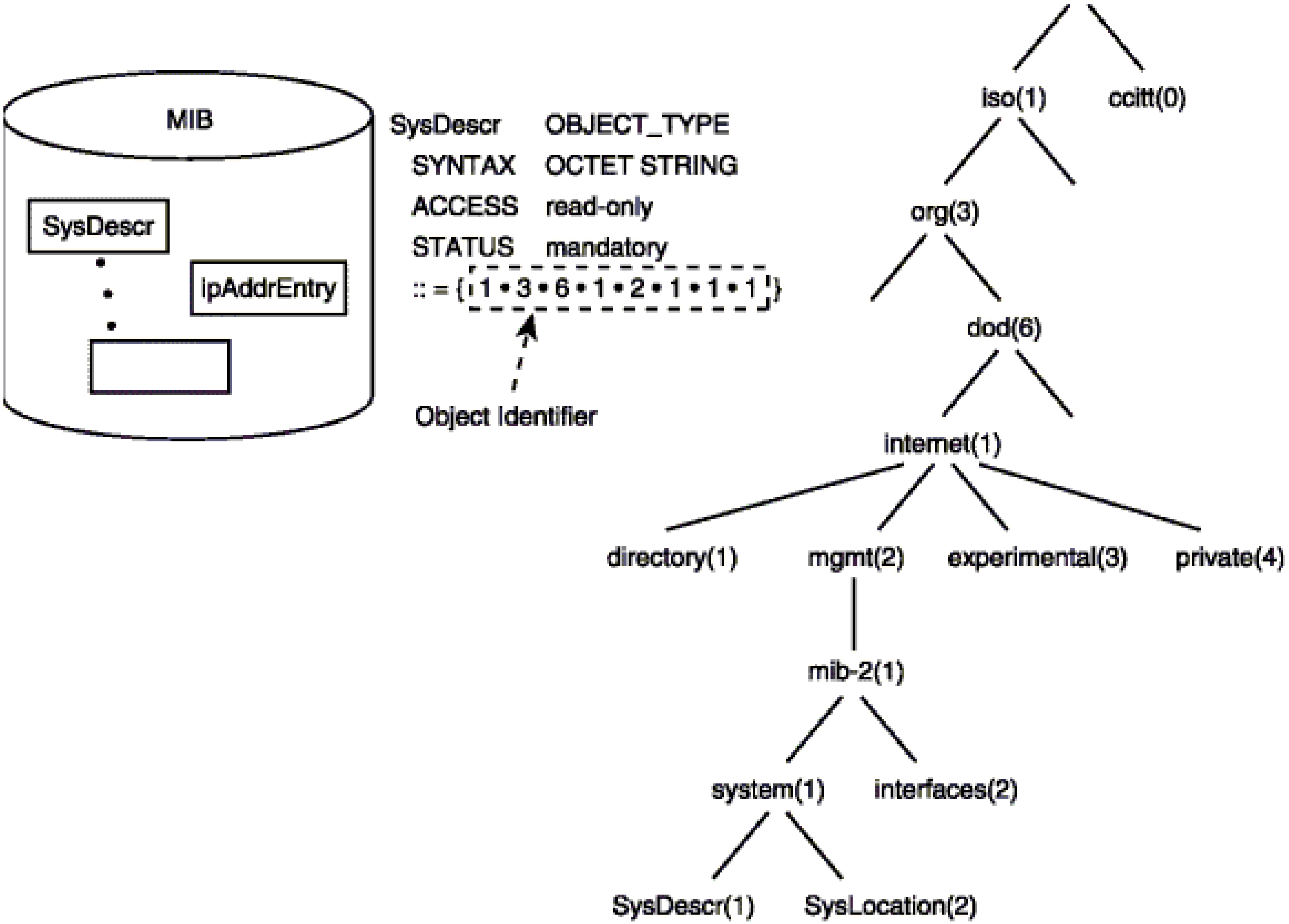
Traps

- The exception is an alarm message or alert triggered by a specific event.
- An alarm message is known as a *trap message*.
- A *trap* is an event such as a system reboot or illegal device access.
- Traps and trap messages provide a rudimentary form of security by notifying the management system whenever such an event occurs.

Management Information Base

- *MIB* is a container of objects which represents a particular type of information required by a management system.
- E.g. one MIB object can represent the number of active sessions on an agent; another can represent the amount of available hard drive space on the agent.
- The information requested from an agent is stored in various MIBs and defines values for each object depending on device type.

MIB Example



```
SysDescr    OBJECT_TYPE
  SYNTAX    OCTET STRING
  ACCESS    read-only
  STATUS    mandatory
  :: = { 1 • 3 • 6 • 1 • 2 • 1 • 1 • 1 }
```

MIB Contents

The MIB may contain :

- numbers,
- text,
- addresses,
- object ids
- more complex data such as routing tables.

MIB Identifiers

- Type (counter, string, or address)
- Access level (read, read/write or none)
- Size restriction
- Range information

Abstract Syntax Notation

Each object has a name, syntax, access rights, status and description as specified by the ASN.1.

- **Name** identifies the object (e.g. SysDesc is the object descriptor and 1.3.6.1.2.1.1.1 is the object identifier)
- **Syntax** defines object’s structure (e.g. octet string, integer)
- **Access** - Objects are Read-only, Read-Write or not accessible
- **Status** – Mandatory or optional for the particular agent.
- **Description** – this is a textual description of the object

Basic Encoding Rules

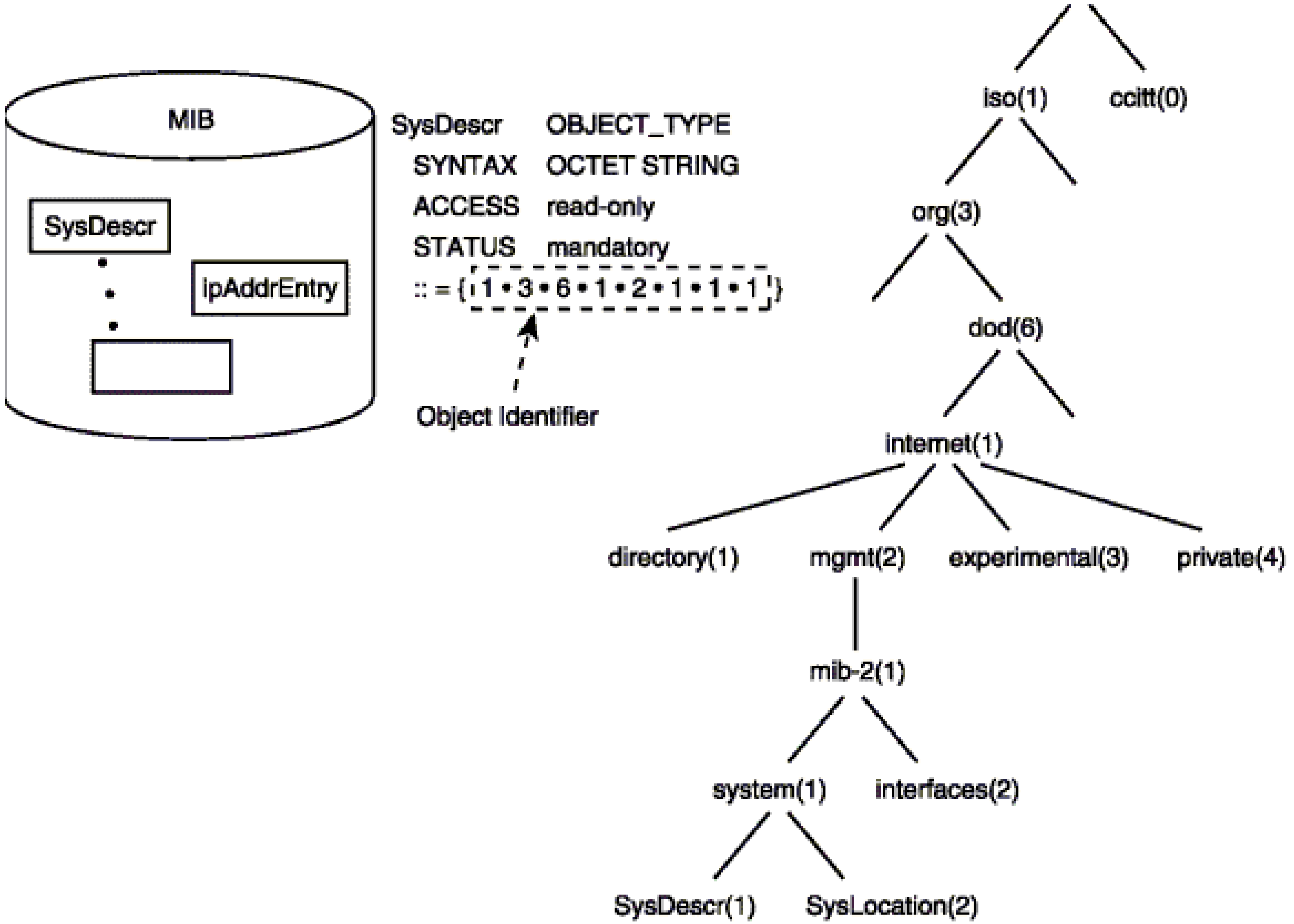
- BER describes how to convert the values of MIB objects into a format that allows them to be transferred through a network.
- ASN.1 objects are expressed in binary format including type, length and data fields.
- The consistent format allows multiple objects to be placed in a single frame on the transmitting side and decoded on the receiving side.

Object Identifiers (OIDs)

- Object Identifiers (OIDs) are represented by a tree hierarchy.
- Each object has a unique address based on its position in the tree.
- The Internet standard management MIB is
  1.3.6.1.2.1. - in numeric form or
  iso.org.dod.internet.management.mib - in text form.
- The root is the ISO trunk value is 1.
- Each branch below further identifies the various branches of the sub-tree.
- All SNMP objects are members of the sub-tree identified by *iso.org.dod.internet* or 1.3.6.1.
- Each additional component further defines the exact location of the object-
- e.g. SysDescr is identified by the OID 1.3.6.1.2.1.1.1.0

N.B. A zero at the end indicates that this is a singular (as opposed to columnar object such as an address table) and has only one instance in the MIB.

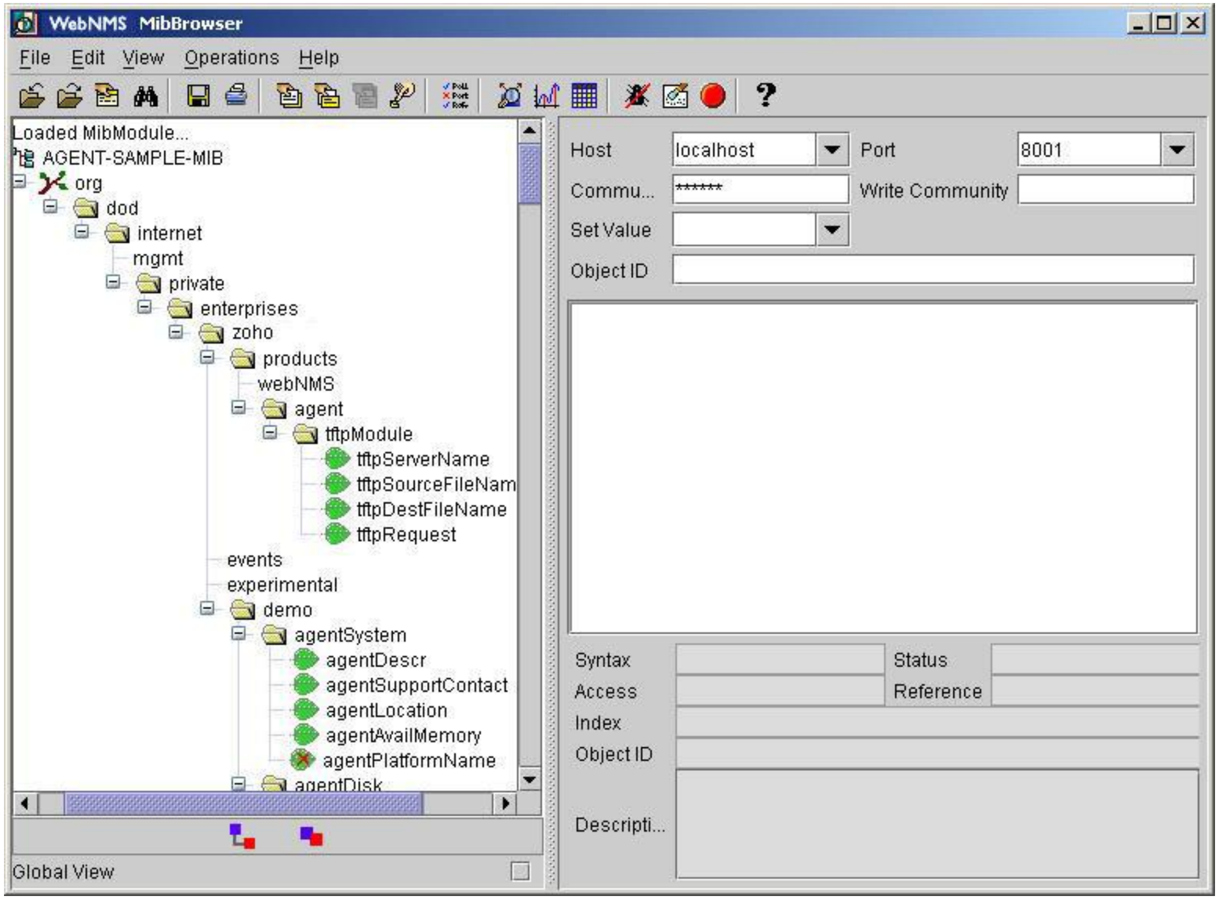
MIB Tree Structure



```
SysDescr   OBJECT_TYPE
  SYNTAX   OCTET STRING
  ACCESS   read-only
  STATUS   mandatory
  ::= {1•3•6•1•2•1•1•1}
```

Walking the MIB Tree

- *You can 'walk' through the name tree with an SNMP console utility or using a stand alone MIB browser to view the contents of each supported variable in the MIB tree.*



Loaded MibModule...

- AGENT-SAMPLE-MIB
- org
  - dod
    - internet
      - mgmt
      - private
        - enterprises
          - zoho
            - products
              - webNMS
              - agent
                - tftpModule
                  - tftpServerName
                  - tftpSourceFileNam
                  - tftpDestFileName
                  - tftpRequest
            - events
            - experimental
            - demo
              - agentSystem
                - agentDescr
                - agentSupportContact
                - agentLocation
                - agentAvailMemory
                - agentPlatformName
              - agentDisk

Host: localhost

Port: 8001

Commu...: ******

Write Community:

Set Value:

Object ID:

Syntax:

Status:

Access:

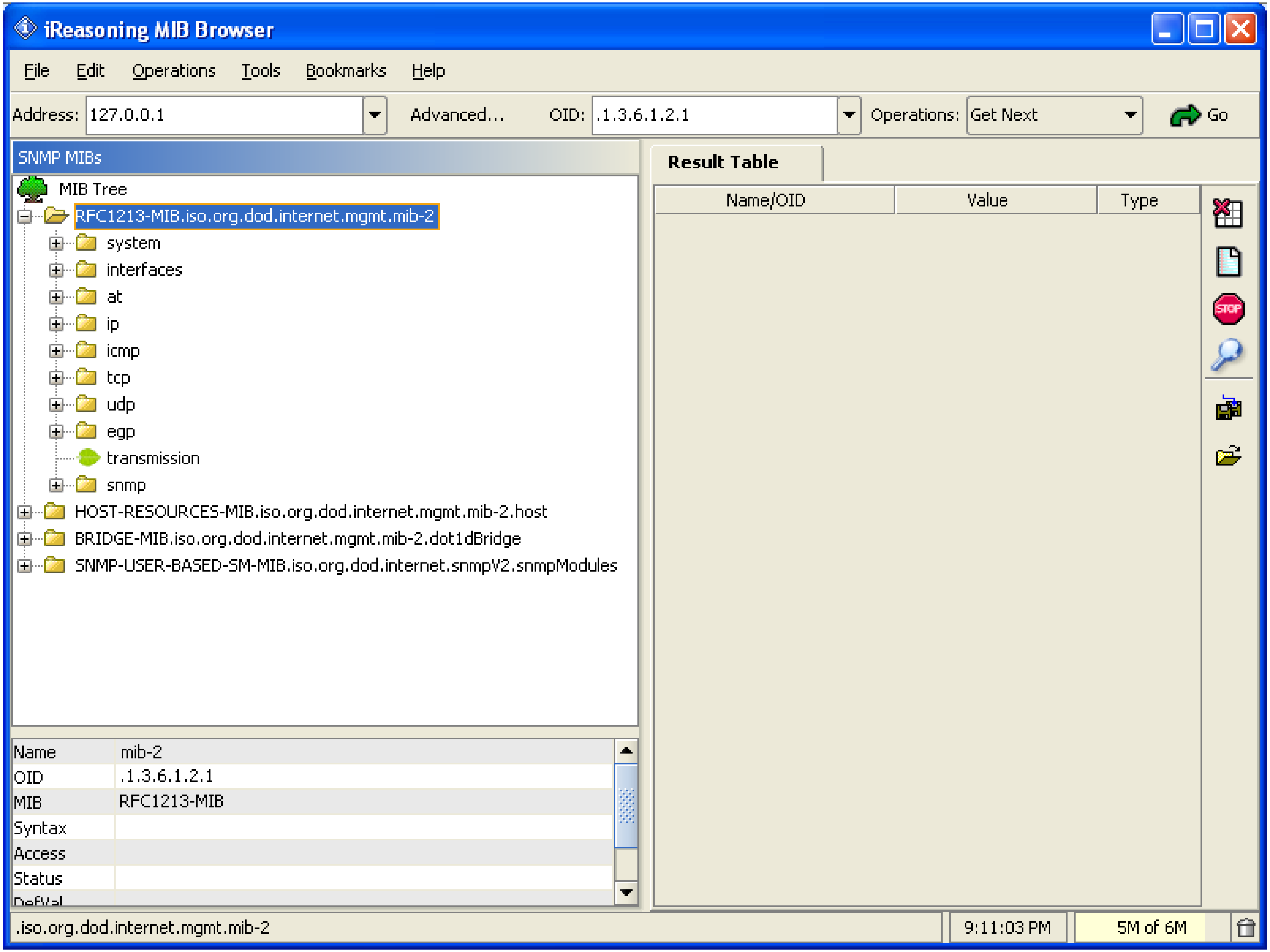
Reference:

Index:

Object ID:

Descripti...:

MIB Browser Used in LAB3



Address: 127.0.0.1

OID: .1.3.6.1.2.1

Operations: Get Next

```
MIB Tree
  RFC1213-MIB.iso.org.dod.internet.mgmt.mib-2
    system
    interfaces
    at
    ip
    icmp
    tcp
    udp
    egp
    transmission
    snmp
  HOST-RESOURCES-MIB.iso.org.dod.internet.mgmt.mib-2.host
  BRIDGE-MIB.iso.org.dod.internet.mgmt.mib-2.dot1dBridge
  SNMP-USER-BASED-SM-MIB.iso.org.dod.internet.snmpV2.snmpModules
```

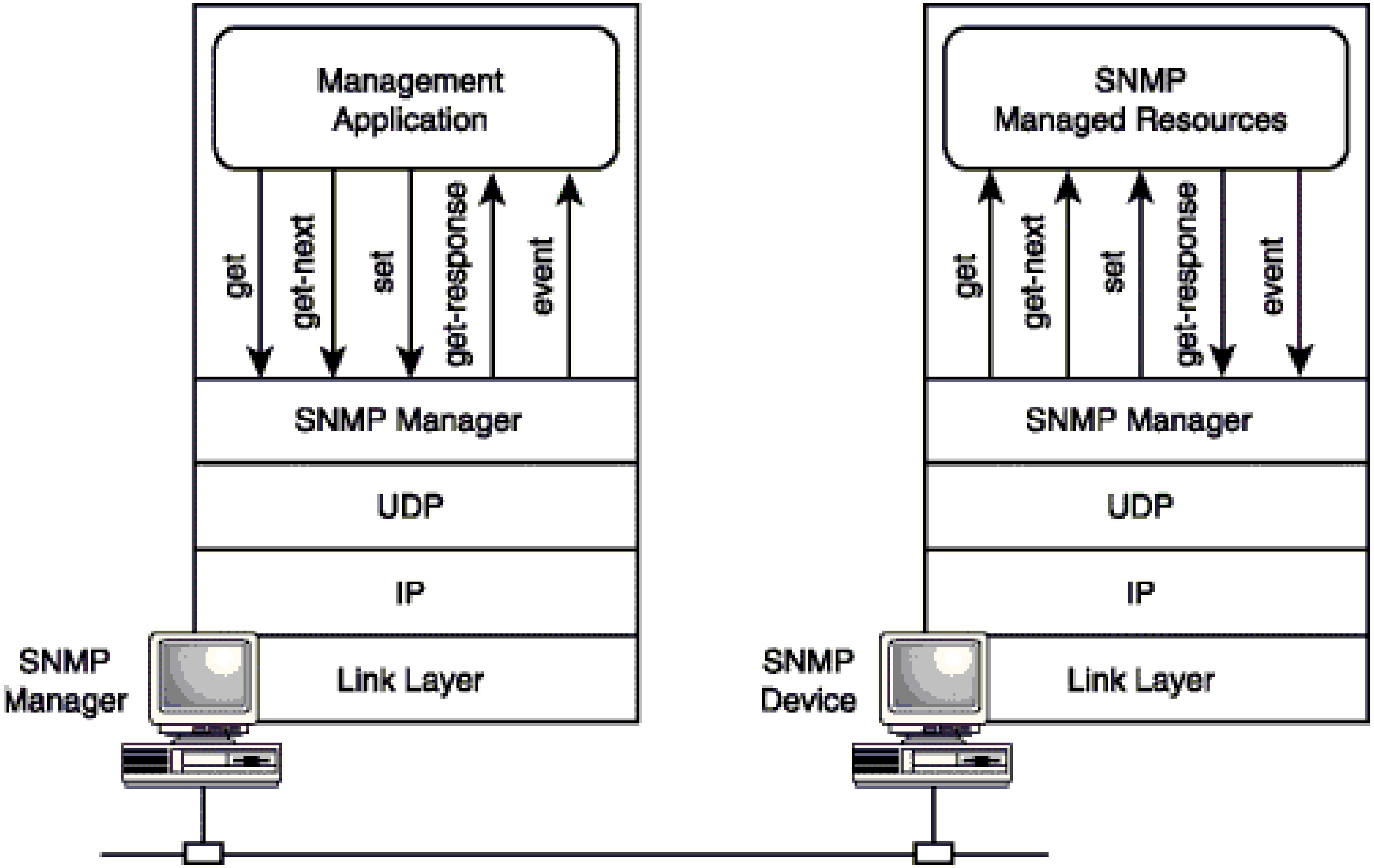
Name	mib-2
OID	.1.3.6.1.2.1
MIB	RFC1213-MIB
Syntax	
Access	
Status	
DefVal	

.iso.org.dod.internet.mgmt.mib-2 | 9:11:03 PM | 5M of 6M

SNMP Communications

- Both agents and management systems use SNMP messages to inspect and communicate information about managed objects.
- SNMP message are sent across the network in standard format (specified in relevant RFCs).
- SNMP messages are sent via the User Datagram Protocol (UDP).
- UDP port 161 is used to listen for SNMP messages and port 162 is used to listen for SNMP traps.

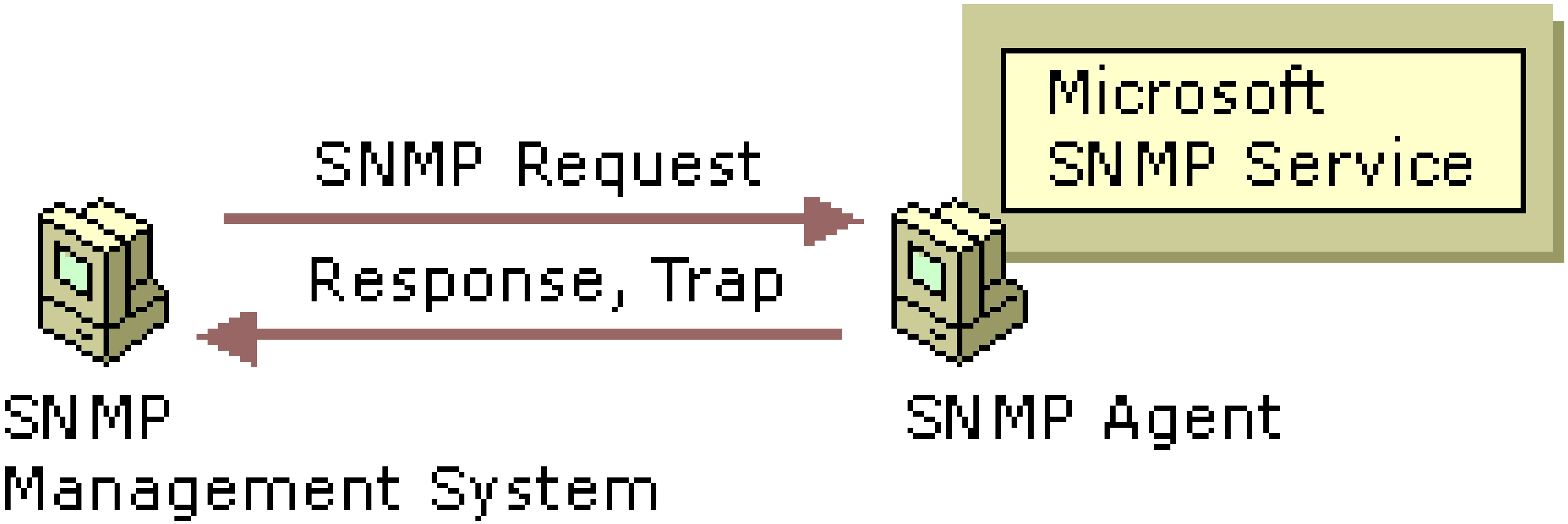
SNMP Model


Management Application
get
get-next
set
get-response
event
SNMP Manager
UDP
IP
Link Layer
SNMP Manager
SNMP Managed Resources
get
get-next
set
get-response
event
SNMP Manager
UDP
IP
Link Layer
SNMP Device

SNMP Interaction

- When an NMS sends requests to a network device, the agent on the device retrieves the requested information from the MIBs and sends the requested information back to the initiating NMS.
- An SNMP agent also sends information when a trap event occurs.

SNMP Messages



SNMP Message Types

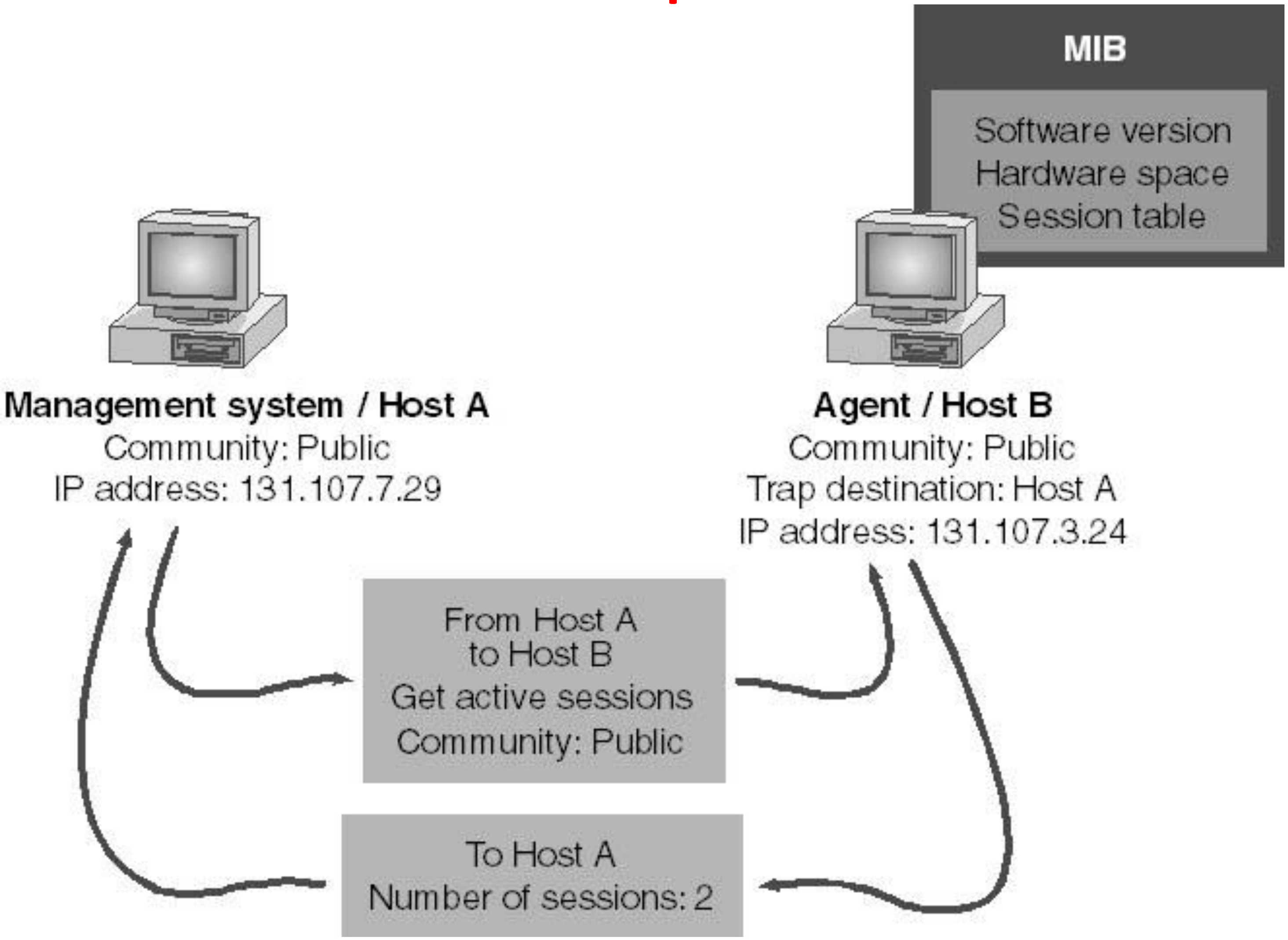
- **GET** The basic SNMP request message. Sent by an NMS, it requests information about a single MIB entry on an agent—for example, the amount of free disk space.
- **GET-NEXT** An extended type of request message that can be used to browse the entire hierarchy of management objects - the agent returns the identity and value of the object that logically follows the previous information that was sent - useful mostly for dynamic tables, such as an internal IP route table.

More Message Types

- **SET** A message that can be used to send and assign an updated MIB value to the agent when write access is permitted.
- **TRAP (or NOTIFY)** An unsolicited message sent by an agent to a management system when the agent detects a certain type of event. E.g. a trap message might be sent when a system restart occurs. The NMS that receives the trap message is referred to as the trap destination.

N.B. SMNP v.2 introduced GET-BULK – a request that the data transferred by the agent be as large as possible within the given restraints of message size. This minimizes the number of protocol exchanges required to retrieve a large amount of management information.

Manager and Agent Interaction example



Example Process

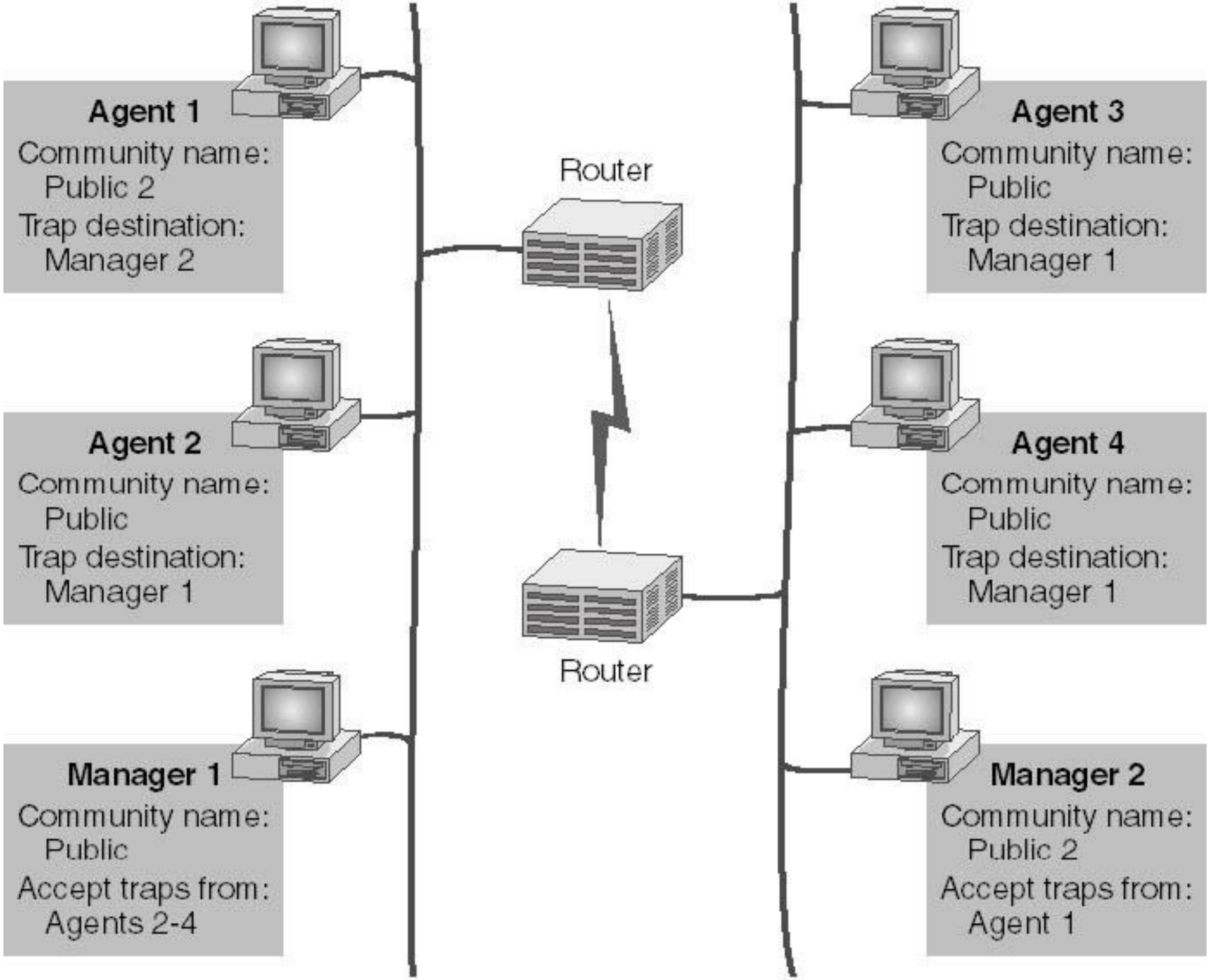
1. NMS forms an SNMP message that contains an information request (GET), the name of the community to which the management system belongs, and the destination of the message—the agent's IP address (131.107.3.24).
2. The SNMP message is sent to the agent.
3. The agent receives the packet and decodes it. The community name (Public) is verified as acceptable.
4. The SNMP service calls the appropriate subagent to retrieve the session information requested from the MIB.
5. The SNMP takes the session information from the subagent and forms a return SNMP message that contains the number of active sessions and the destination—the management system's IP address (131.107.7.29).
6. The SNMP message is sent to the management system.

SNMP Communities

- Each SNMP management host and agent belongs to an SNMP community - a collection of hosts grouped together for administrative purposes. Communities are identified by the names you assign to them.
- A community name can be thought of as a password shared by SNMP management consoles and managed computers.

- *N.B. By default public communities are read only, private communities are read/write.*

Example Communities



Agent 1
Community name:
Public 2
Trap destination:
Manager 2

Agent 2
Community name:
Public
Trap destination:
Manager 1

Manager 1
Community name:
Public
Accept traps from:
Agents 2-4

Agent 3
Community name:
Public
Trap destination:
Manager 1

Agent 4
Community name:
Public
Trap destination:
Manager 1

Manager 2
Community name:
Public 2
Accept traps from:
Agent 1

Community Restrictions

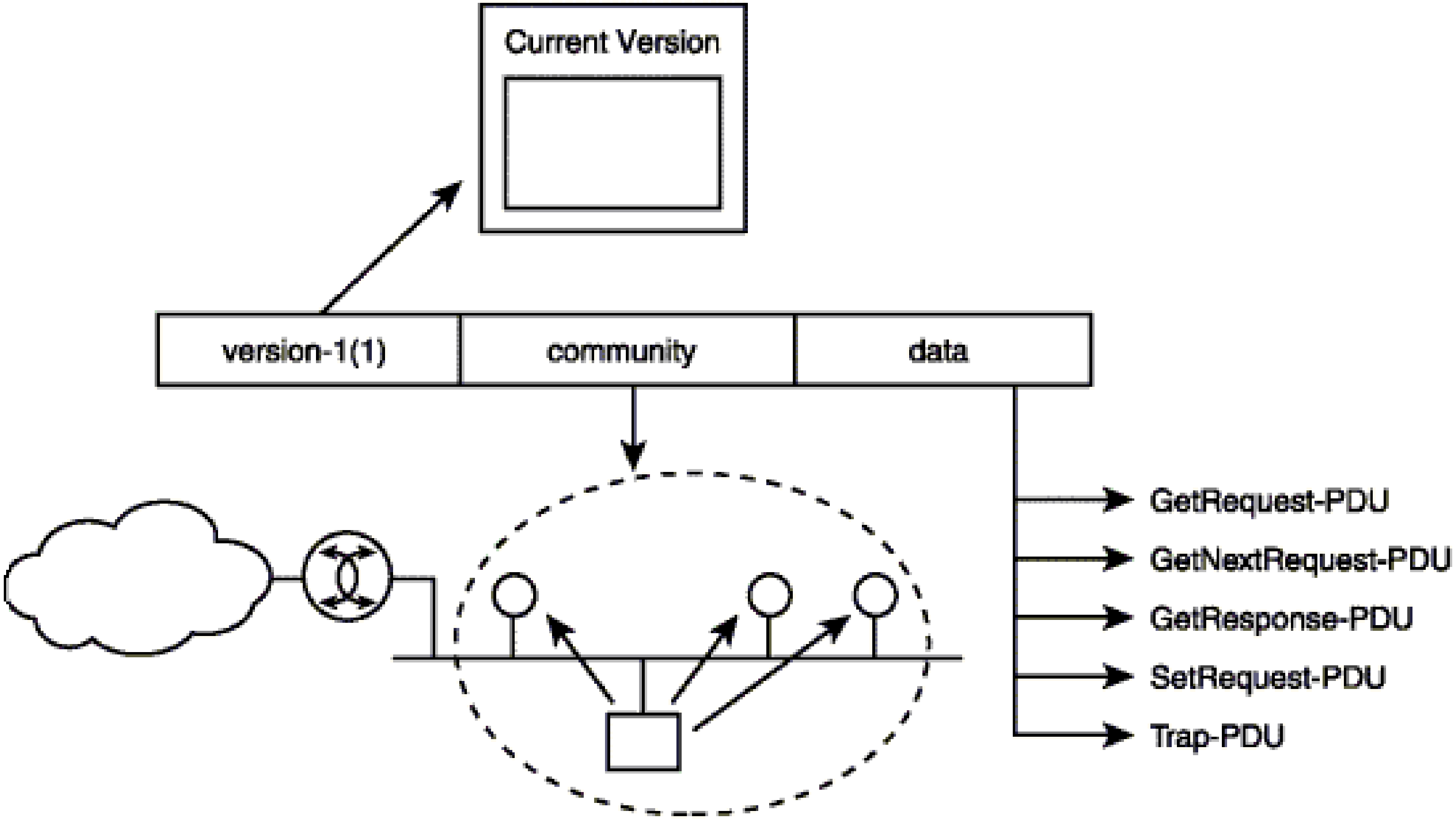
- In the previous example there are two communities — Public and Public 2.
- Agent 1 can respond to SNMP requests from and can send traps to Manager 2 because they are both members of the Public 2 community.
- Agent 2, Agent 3, and Agent 4 can respond to SNMP requests from and can send traps to Manager 1 because they are all members of the (default) Public community.

Note on community names

- *There is no relationship between community names and domain or workgroup names. Community names represent a shared password for groups of network hosts, and they should be selected and changed as you would change any password. Deciding which hosts belong to the same community is generally determined by physical proximity.*

SNMP Message Format

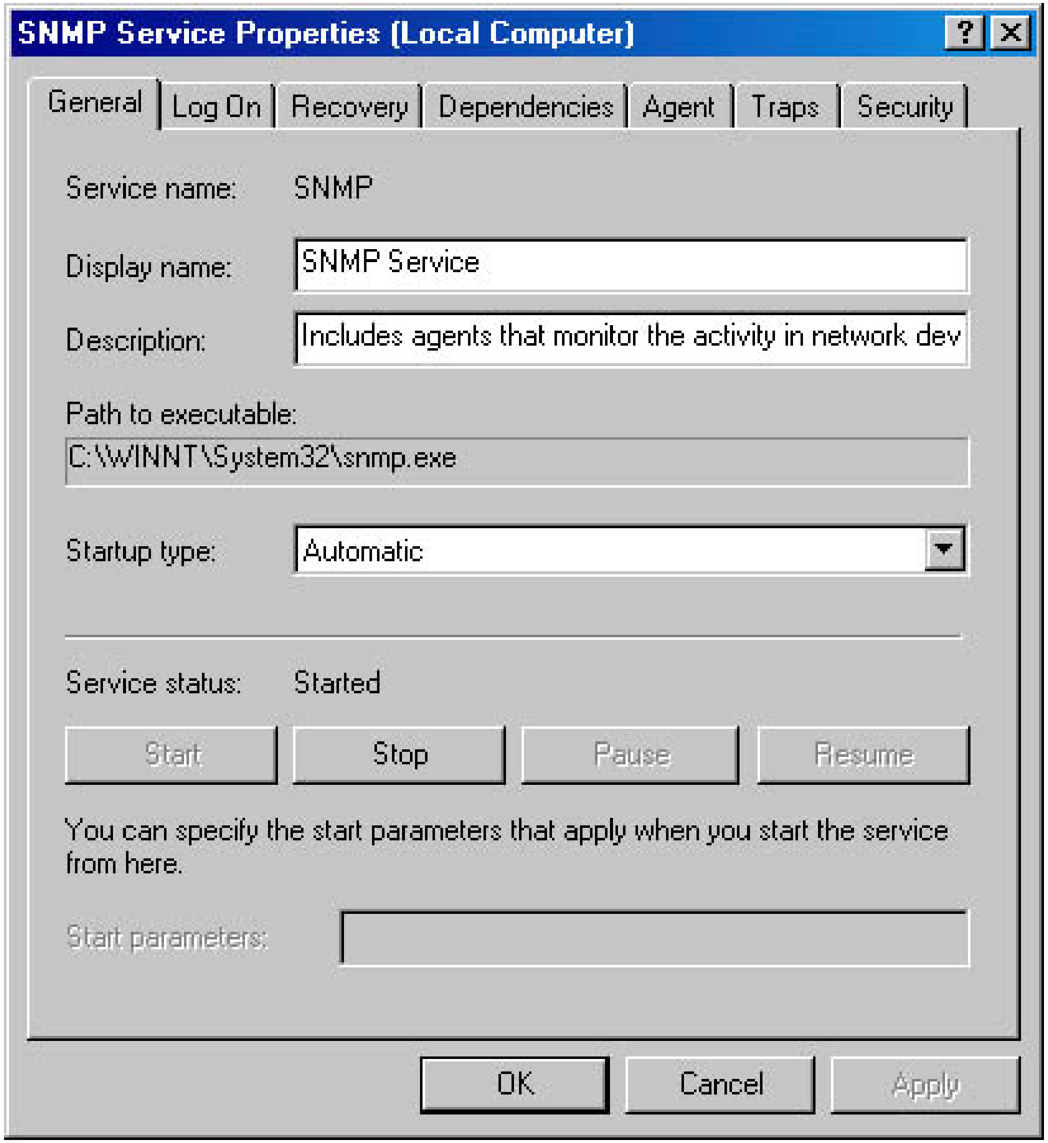
```
SNMP-Message ::=  SEQUENCE {
                  VERSION INTEGER {version-1(1)},
                  community OCTET STRING,
                  data ANY}
```



Windows SNMP agent

- The Windows 7/2012 OS provides a SNMP agent installed from the Control Panel Add/Remove Windows Programs application under Management and Monitoring Tools.
- This contains the Simple Network Management Protocol, which is the SNMP agent which is listed as SNMP Service after it is installed.
- Once the SNMP service is installed, you can configure the SNMP services through Administrative Tools.
- In the Services node you select SNMP Service from the details panel, and then select Properties from the Action menu.

General Properties



Service name: SNMP

Display name: SNMP Service

Description: Includes agents that monitor the activity in network dev

Path to executable:
C:\WINNT\System32\snmp.exe

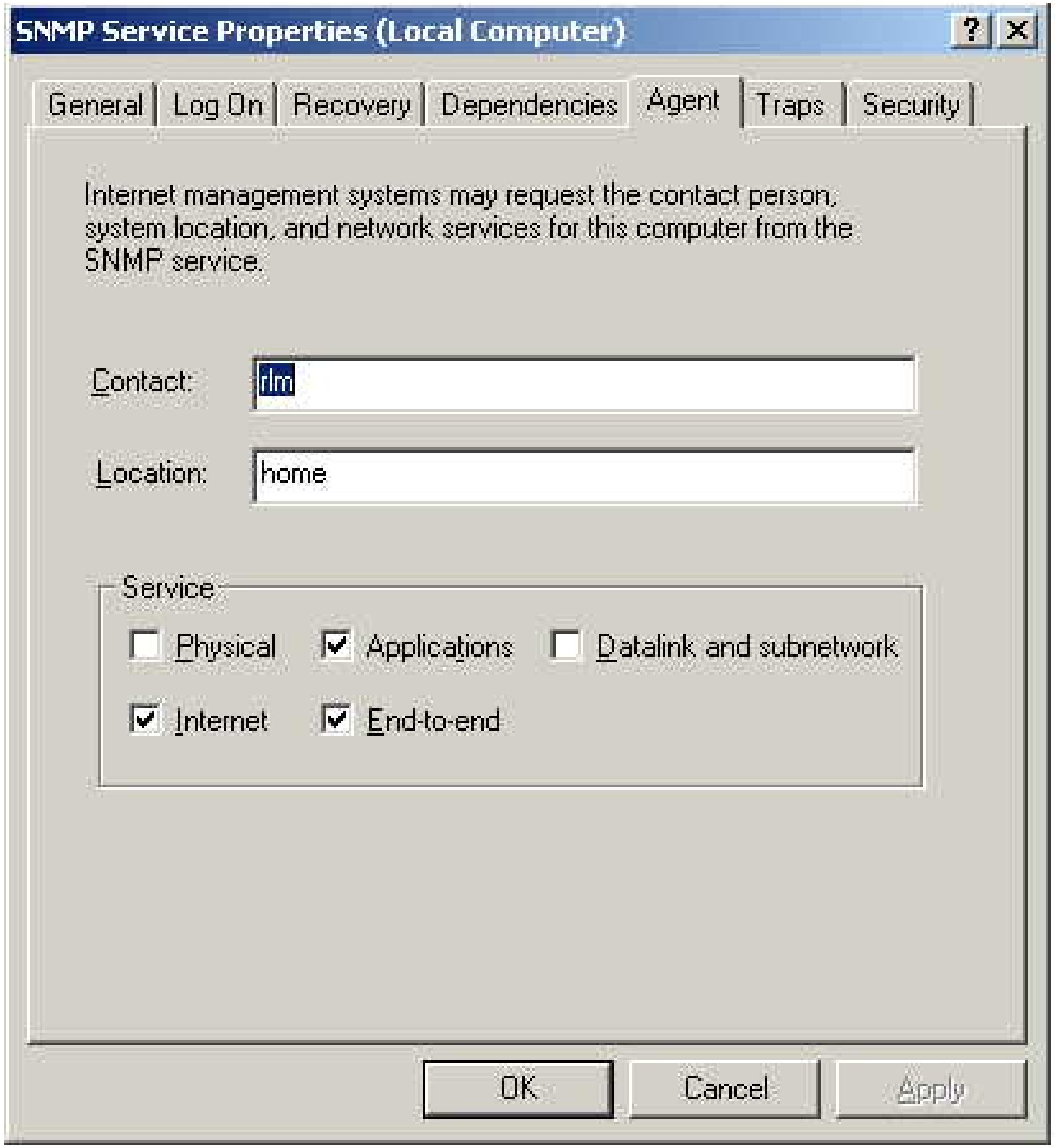
Startup type: Automatic

Service status: Started

You can specify the start parameters that apply when you start the service from here.

Start parameters:

Agent Properties



Internet management systems may request the contact person, system location, and network services for this computer from the SNMP service.

Contact: rlm

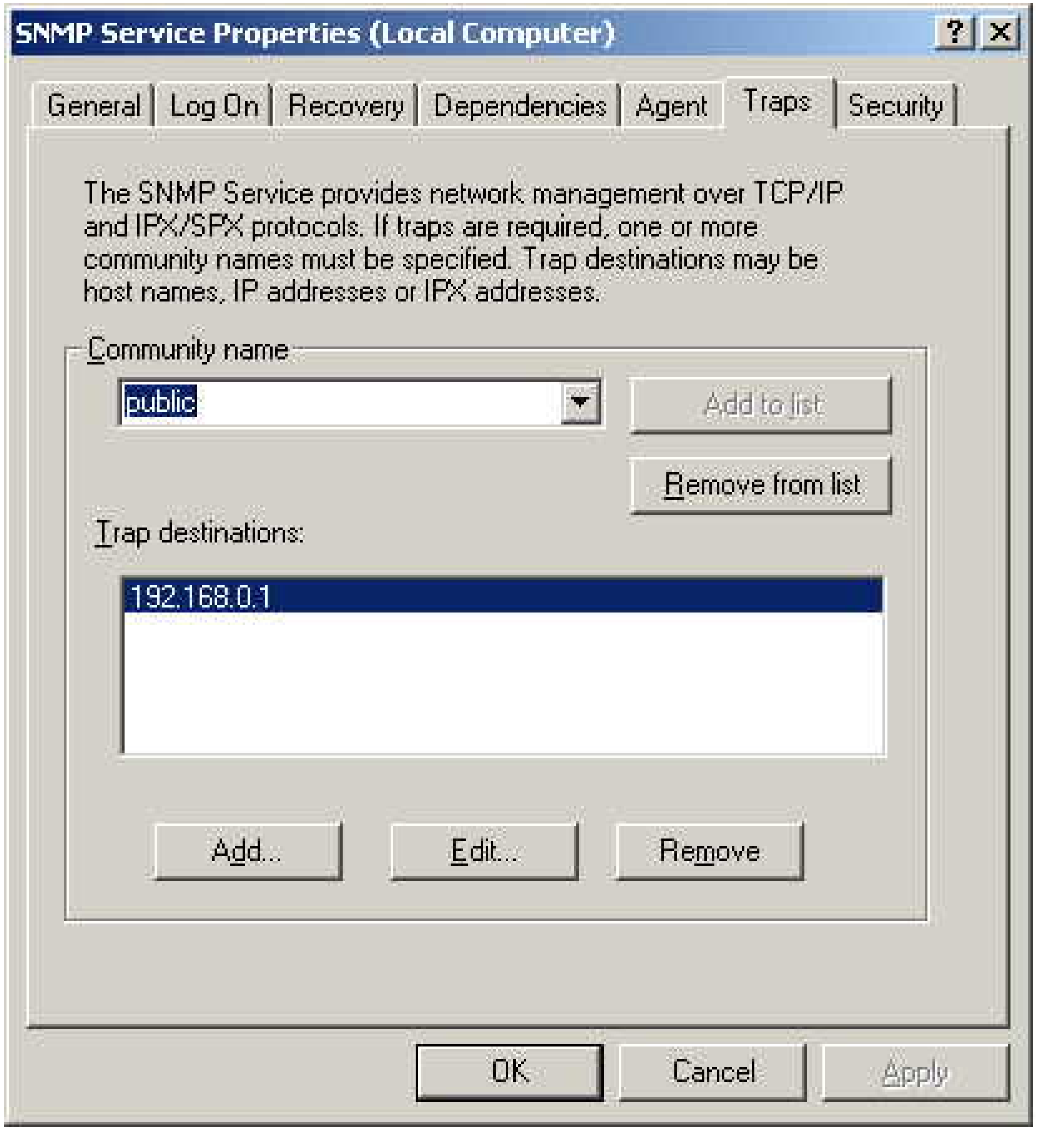
Location: home

Service

□ Physical ☑ Applications □ Datalink and subnetwork

☑ Internet ☑ End-to-end

Trap Properties



SNMP Service Properties (Local Computer)

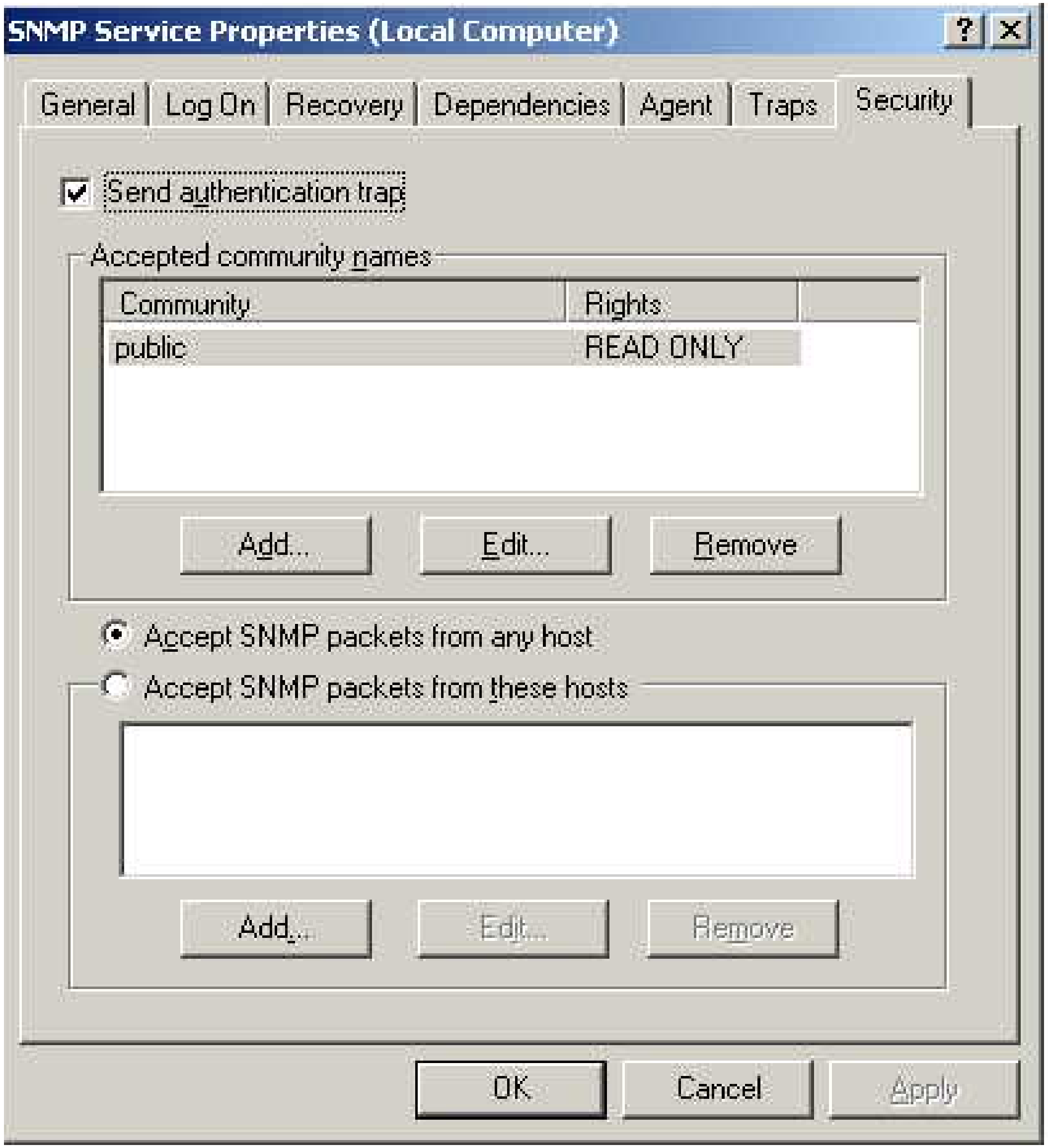
The SNMP Service provides network management over TCP/IP and IPX/SPX protocols. If traps are required, one or more community names must be specified. Trap destinations may be host names, IP addresses or IPX addresses.

Community name: public

Trap destinations:

192.168.0.1

Security Properties



SNMP Service Properties (Local Computer)

☑ Send authentication trap

Accepted community names

Community	Rights
public	READ ONLY

● Accept SNMP packets from any host

○ Accept SNMP packets from these hosts

Network Device Agents

- SNMP managed switches, routers and other network equipment are initially configured using:

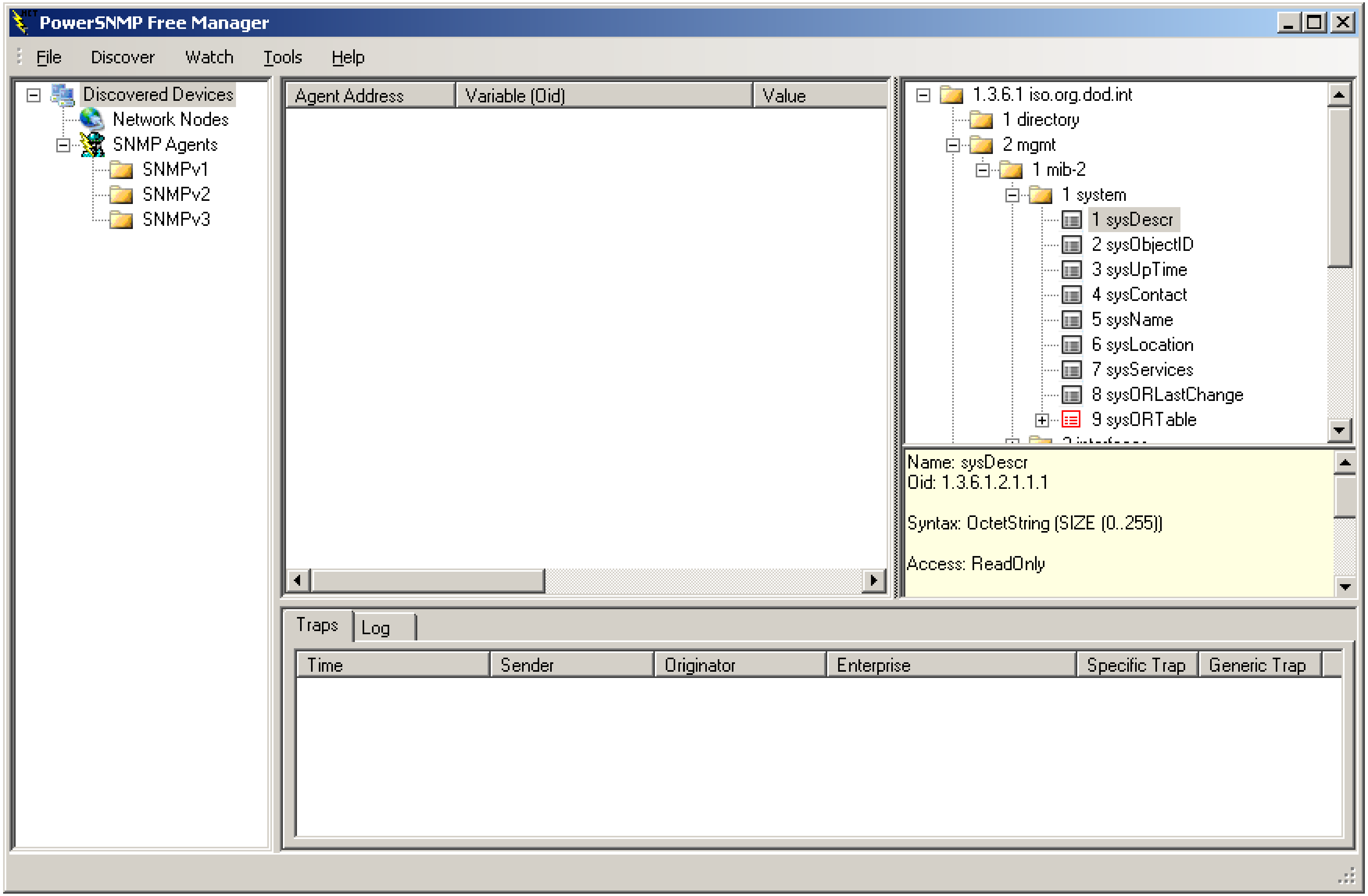
- A serial port connected to a VT-100 terminal (out of band) or

- Via a Telnet or HTTP session (in band).

Vendor SNMP Tools

- Network equipment vendors also offer management tools to help with agent administration
- Tools can be stand-alone or integrated into management suites such as HP OpenView.
- e.g. ATView or SNMPc management software for Allied Telesyn devices,
- Observer suite…

PowerSNMP



Name: sysDescr
Oid: 1.3.6.1.2.1.1.1

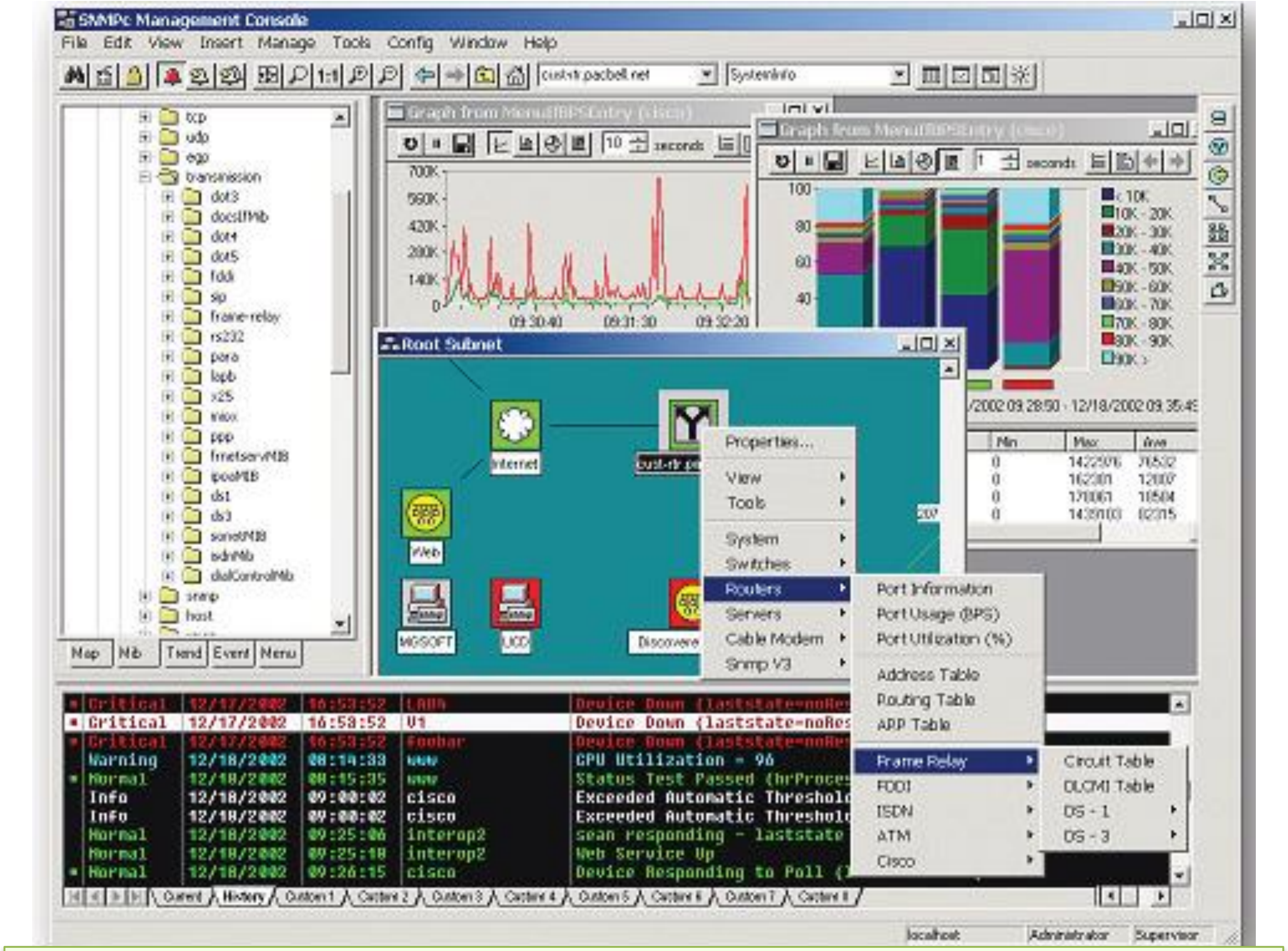
Syntax: OctetString (SIZE (0..255))

Access: ReadOnly

Device Discovery and Mapping

- Management systems have visual interface features to help with management
- E.g. SNMPc or Network View can automatically discover all SNMP devices connected and draw an active multilevel network map of the network.
- Clicking on a device icon allows device specific information to be easily obtained.
- Non SNMP devices can also be found using ICMP discovery
- Proprietary protocols such as Cisco's CDP may be used or Microsoft'S LLTD are also employed.

SNMPc

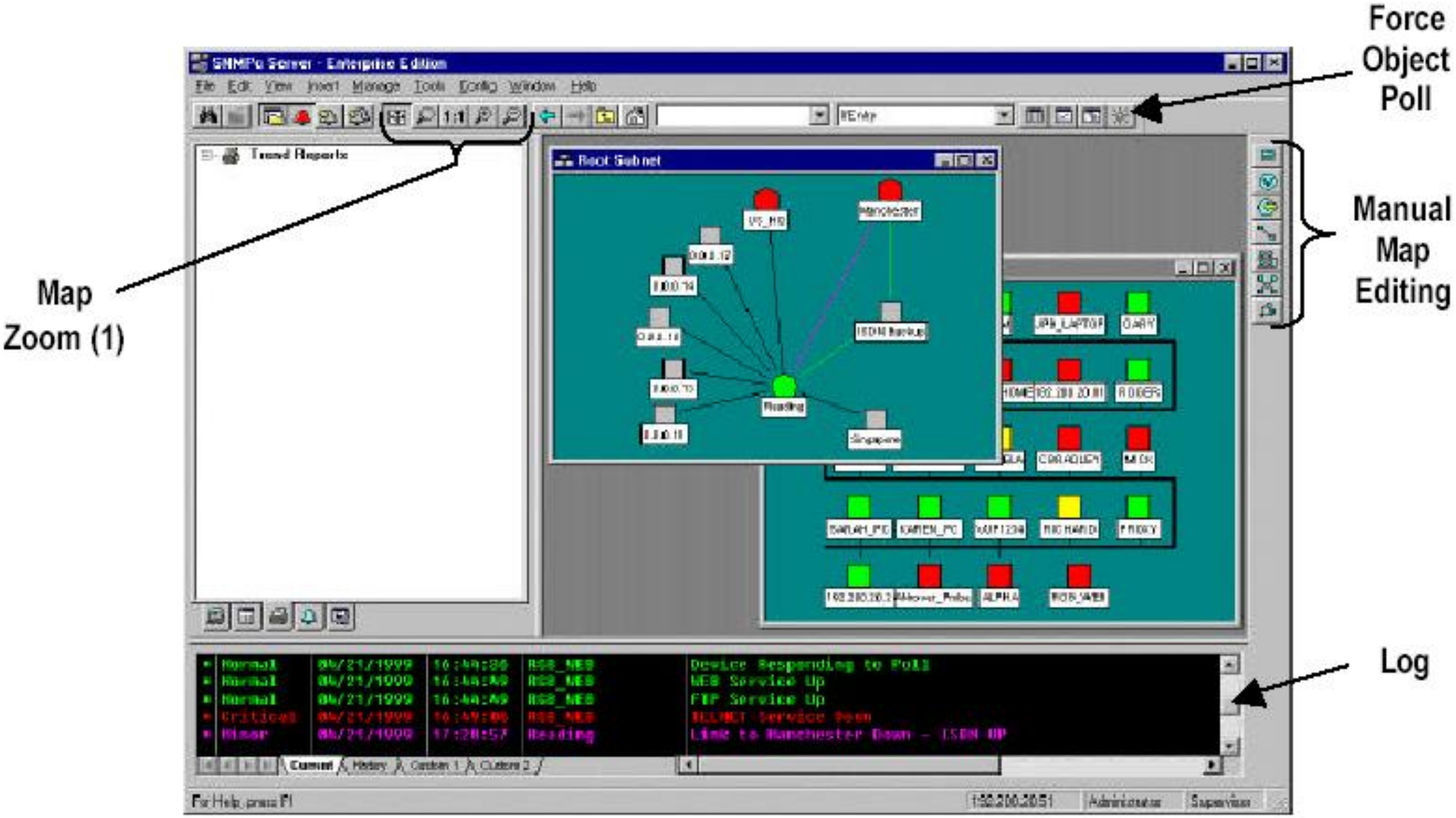


Min	Max	Ave
0	1422976	76532
0	162301	12007
0	170061	10504
0	1430103	82315

```
Critical  12/17/2002  16:53:52  LABA       Device Down (laststate=noRes
Critical  12/17/2002  16:53:52  V1         Device Down (laststate=noRes
Critical  12/17/2002  16:53:52  Foobar     Device Down (laststate=noRes
Warning   12/18/2002  08:14:33  www        CPU Utilization = 96
Normal    12/18/2002  08:15:35  www        Status Test Passed (hrProces
Info      12/18/2002  09:00:02  cisco      Exceeded Automatic Threshold
Info      12/18/2002  09:00:02  cisco      Exceeded Automatic Threshold
Normal    12/18/2002  09:25:06  interop2   sean responding - laststate
Normal    12/18/2002  09:25:10  interop2   Web Service Up
Normal    12/18/2002  09:26:15  cisco      Device Responding to Poll (
```

SNMPc is a full featured SNMP management system with could discovery and mapping features as shown

SNMPc Visual Interface



Force Object Poll

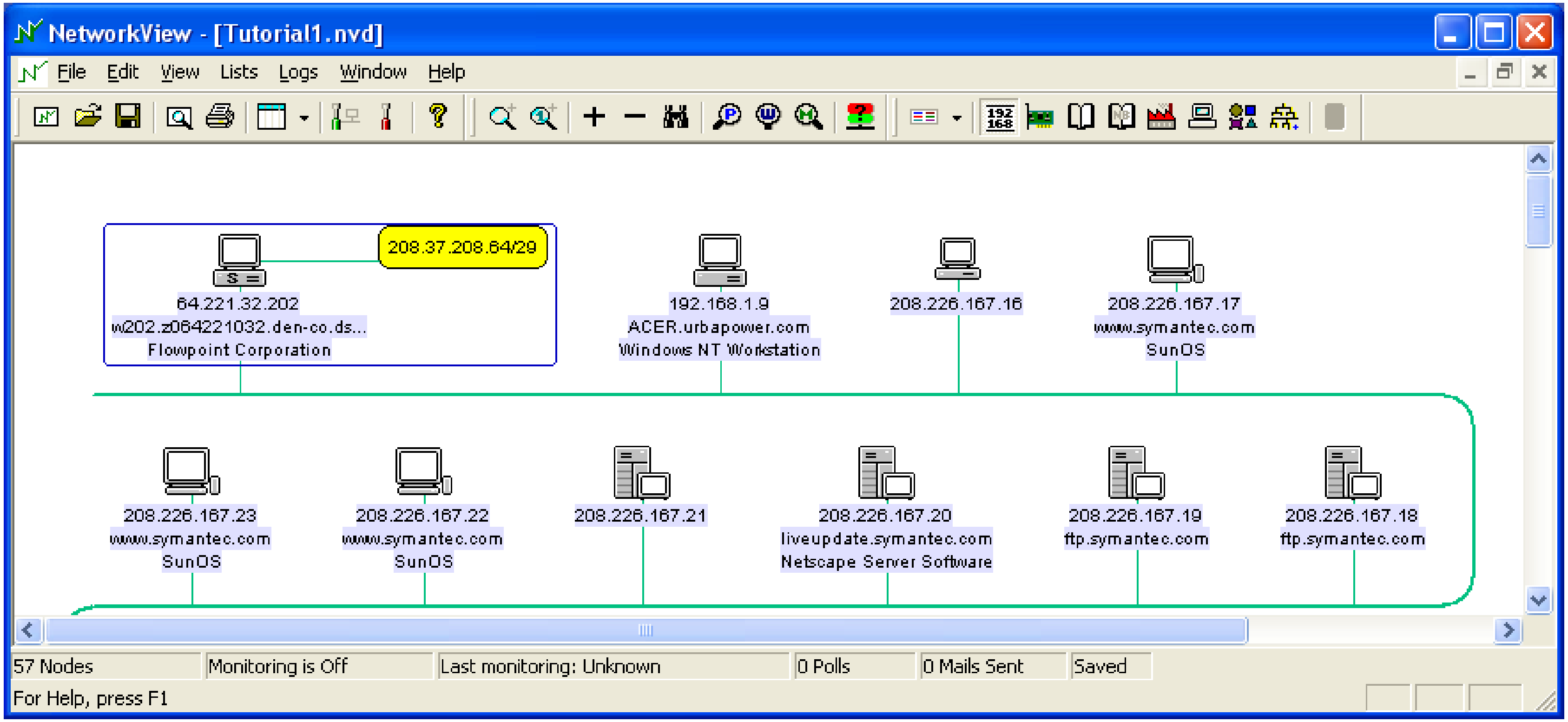
Manual Map Editing

Map Zoom (1)

Log

```
Normal    04/21/1999  16:44:38  RSB_WEB    Device Responding to Poll
Normal    04/21/1999  16:44:49  RSB_WEB    WEB Service Up
Normal    04/21/1999  16:44:49  RSB_WEB    FTP Service Up
Critical  04/21/1999  16:49:06  RSB_WEB    TELNET Service Down
Minor     04/21/1999  17:20:57  Reading    Link to Manchester Down - ISDN UP
```

Network View



57 Nodes | Monitoring is Off | Last monitoring: Unknown | 0 Polls | 0 Mails Sent | Saved

For Help, press F1

Cisco Discovery Protocol

- **CDP** is a proprietary Data Link Layer network protocol developed by Cisco Systems.
- Is implemented in most Cisco networking equipment and is used to share information about other directly connected Cisco equipment, such as the operating system version and IP address via multicast frames.
- Routing information can be used in CDP announcements so that dynamic routing protocols do not need to be used in simple networks.

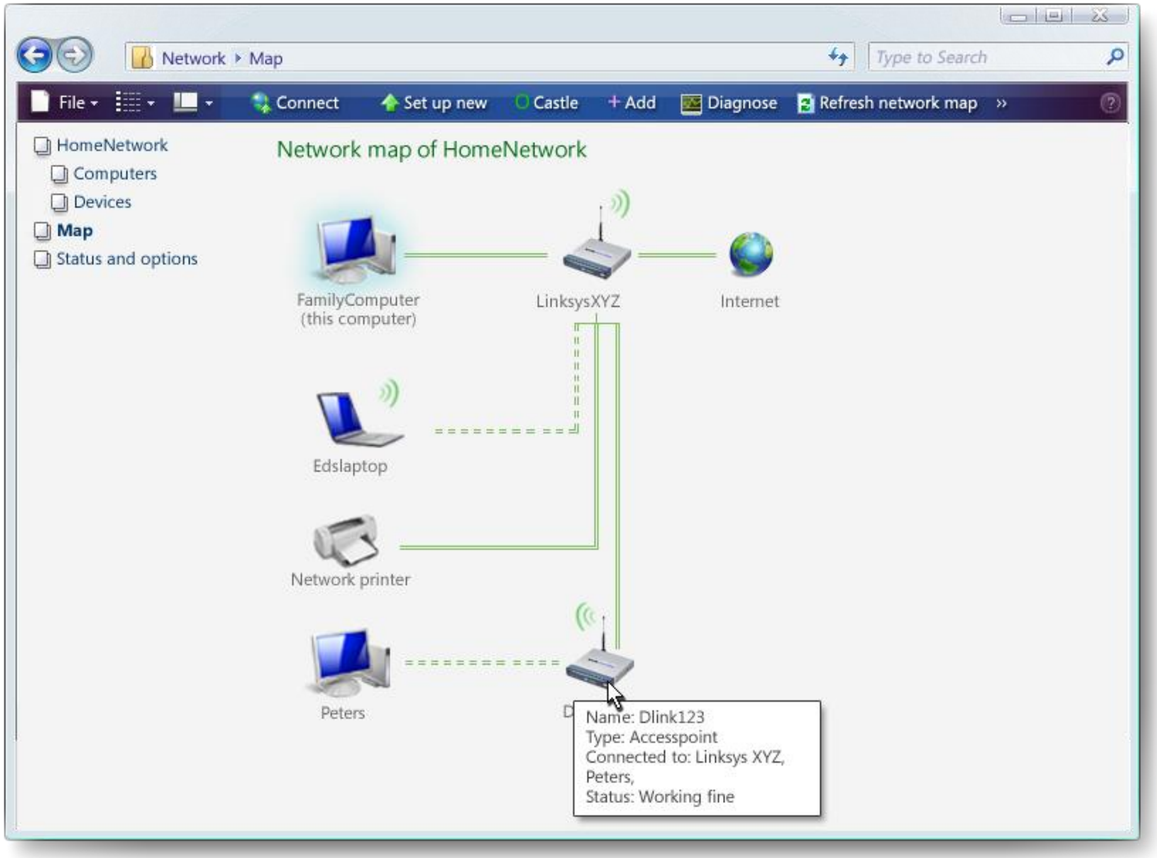
Link Layer Topology Discovery

- **LLTD** is a Microsoft proprietary Data Link Layer protocol for network topology discovery and quality of service diagnostics.
- The LLTD protocol operates over both IEEE 802.3 Ethernet and IEEE 802.11 wireless networks.
- LLTD is included in Windows 7.
- It is used by the *Network Map* feature to display a graphical representation of the LAN, to which the computer is connected.
- LLTD operates strictly on a given local network segment.
- It cannot discover devices across routers.
- LLTD responder needed fo XP PCs

LLTD Features

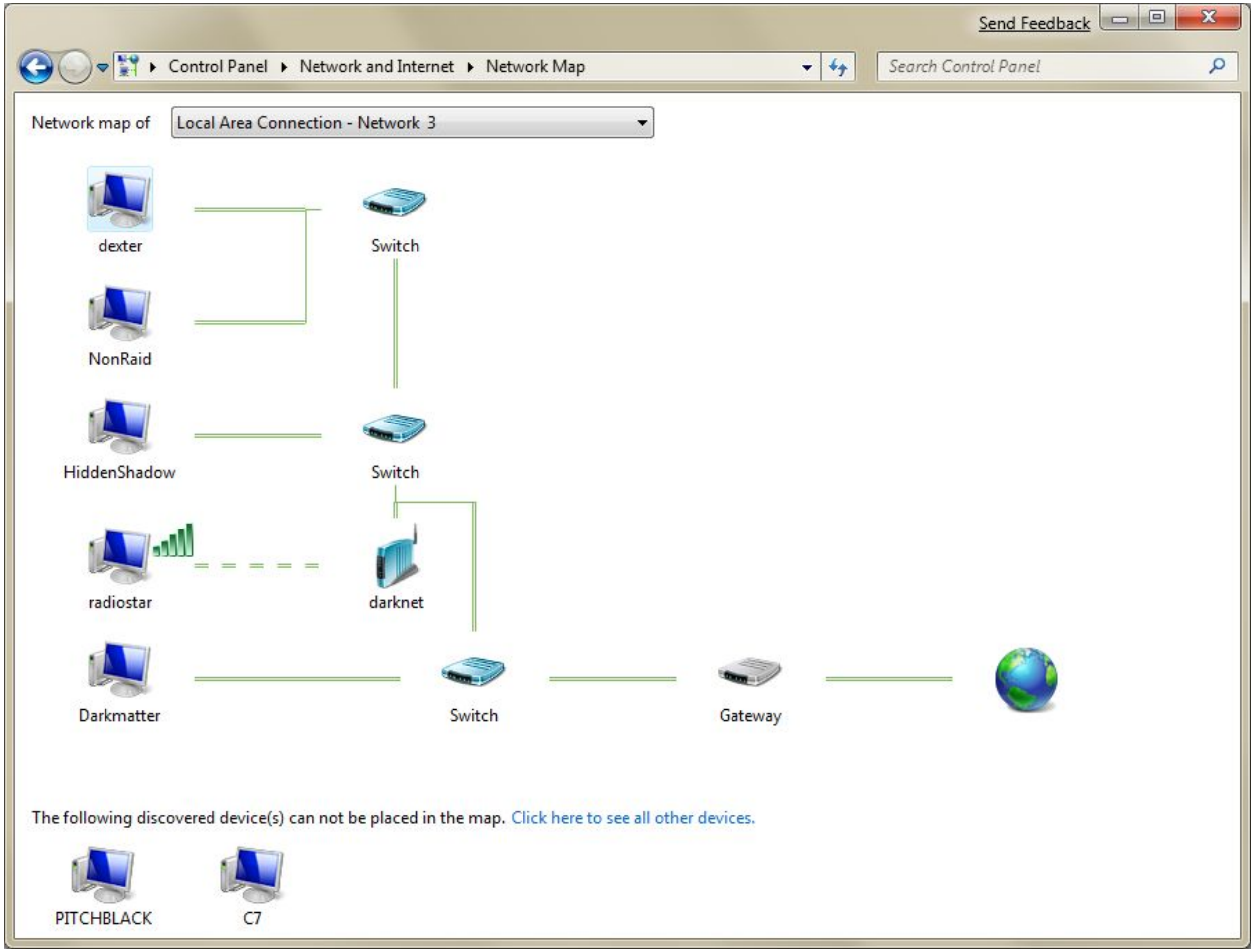
- In addition to illustrating the layout of a network with representative icons for the hosts and interconnecting lines, each device icon may be explored to produce a popup information box summarizing important network and host parameters, such as MAC address and IP address (both IPv4 and IPv6).
- Icons are labelled with the hostnames (or first component of their fully qualified domain names), or a representative name of the function of the device, e.g., "gateway".
- If the device has reported the presence of a management Web interface, clicking on the icon will open a HTTP session to the host.

LLTD Derived Network MAP



Name: Dlink123
Type: Accesspoint
Connected to: Linksys XYZ,
Peters,
Status: Working fine

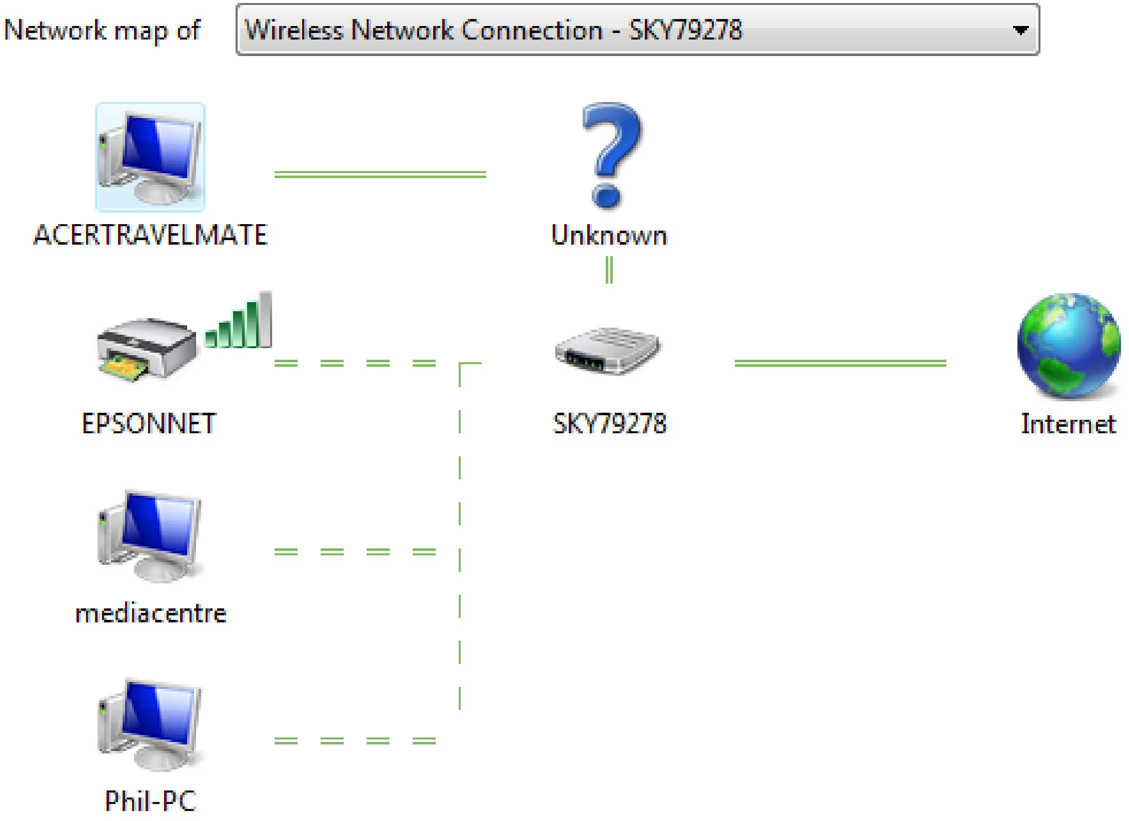
LLTD Network Map EX2



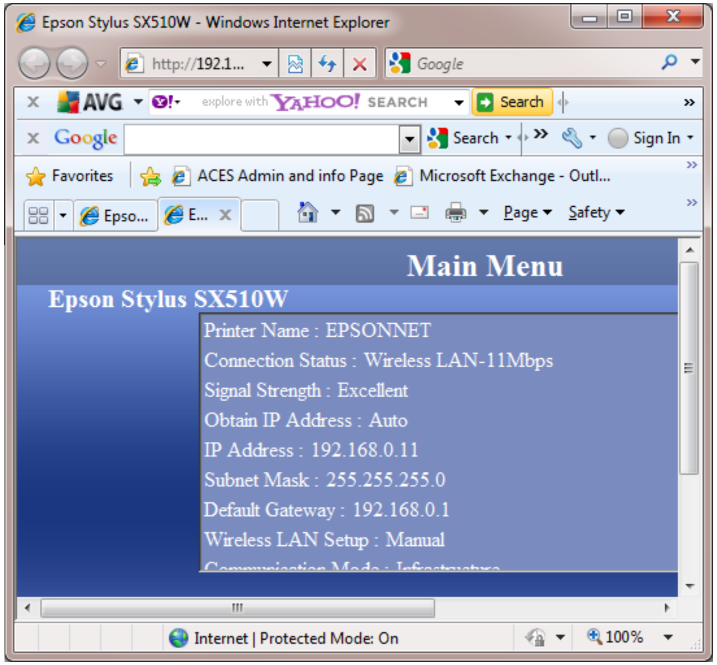
Network map of: Local Area Connection - Network 3

The following discovered device(s) can not be placed in the map. Click here to see all other devices.

Homenet



Network map of Wireless Network Connection - SKY79278



Epson Stylus SX510W - Windows Internet Explorer
http://192.1...
Google
AVG
explore with YAHOO! SEARCH
Search
Google
Search
Sign In
Favorites
ACES Admin and info Page
Microsoft Exchange - Outl...
Epso...
E...
Page
Safety
Internet | Protected Mode: On
100%

Main Menu

Epson Stylus SX510W

Printer Name : EPSONNET
Connection Status : Wireless LAN-11Mbps
Signal Strength : Excellent
Obtain IP Address : Auto
IP Address : 192.168.0.11
Subnet Mask : 255.255.255.0
Default Gateway : 192.168.0.1
Wireless LAN Setup : Manual
Communication Mode : Infrastructure

Link Layer Discovery Protocol

- **LLDP** is a vendor-neutral Data Link Layer protocol used by network devices for advertising of their identity, capabilities, and interconnections on a IEEE 802 LAN network.
- LLDP performs functions similar to several proprietary protocols, such as Cisco Discovery Protocol, and Microsoft Link Layer Topology Discovery.

RMON

- RMON protocol is an extension to SNMP, which allows data to be processed at the point of collection.
- RMON can be implemented in software on an existing device or in hardware called probes.
- Data is organised in the same manner as with SNMP, described in an RMON MIB and retrieved with SNMP commands.
- RMON probes appear like super MIBs but provide continuous monitoring and remote data processing capabilities.

RMON Groups

GROUP	**Function**	**Elements**
Statistics	Stats measured by probe	packets/bytes sent dropped, broadcasts/ multicasts, CRC errors, runts, jabbers, collisions
History	Trend analysis based on data from stats group	Sample period, number of samples, items sampled
Alarm	Configure generation of event if threshold crossed	Type, interval, starting threshold, stop threshold
Host	Collects stats based on Host MAC addresses	MAC address, packets, bytes received/transmitted + broadcast, multicast and error packets
HostTopN	Collects stats for busiest hosts	Statistics, host(s), sample start and stop periods, rate base, duration.
Traffic Matrix	Collects data based on pairs of addresses	Source/destination address – packets, bytes and errors for each pair
Filters	Match packets by filter equation	Bit filter type (mask or not mask), filter expression, conditional expression
Packet Capture	Controls packet capture	Size or buffer for captured packets, full status (alarm), number of captured packets
Events	Logs and generates traps	Event type, description, last time event sent.

RMON Example

- Data pertinent to the health of Ethernet segments includes another very specific set of statistical data available on Ethernet RMON probes. This data provides detailed insights into utilization, errors and events.
- Additionally, RMON has the detailed capability to tell you what types of errors are being experienced on the ring. Table 2 show examples of rates to monitor.

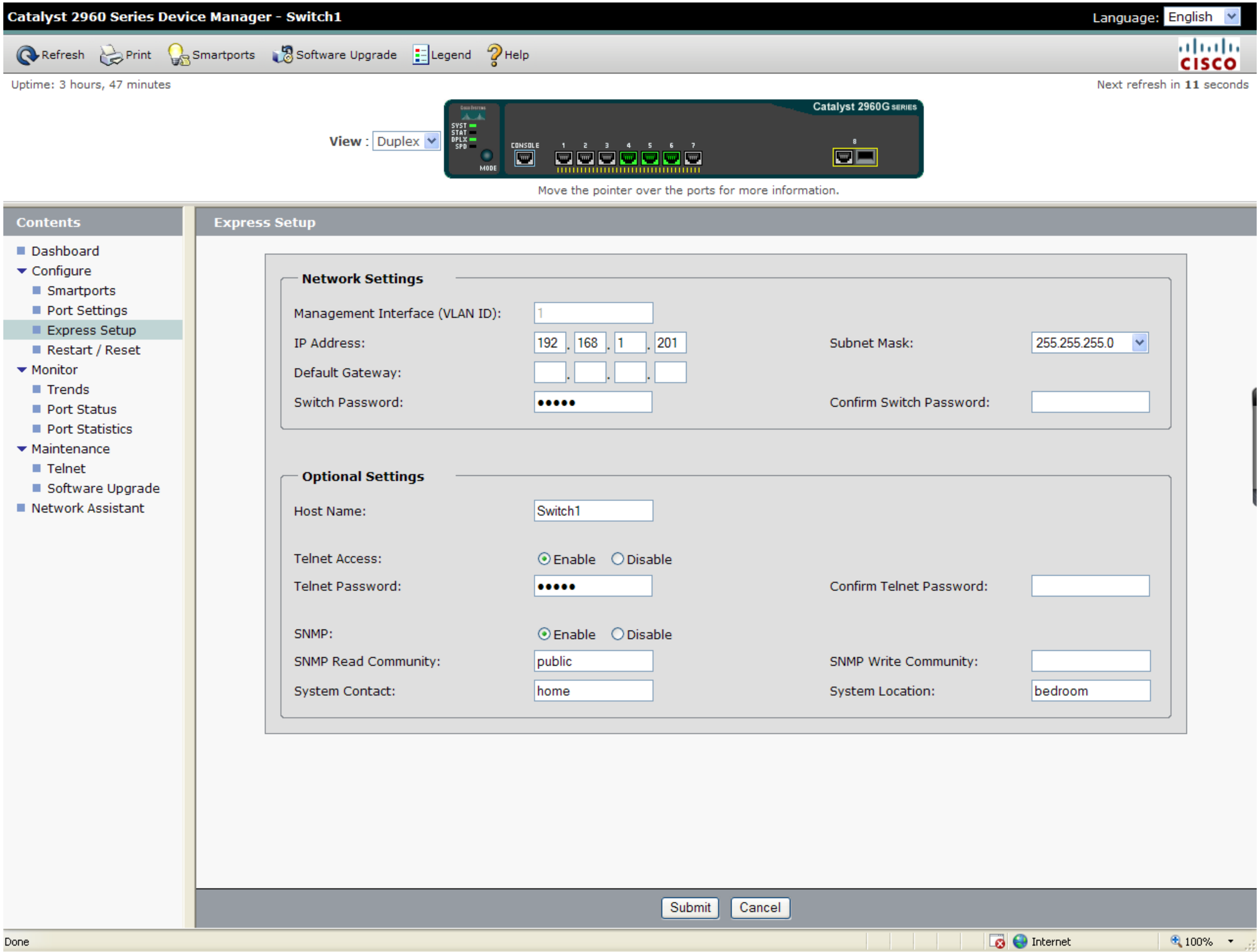
Table 2

	Avg Util (%)	**Peak Util (%)**	**Errors (%)**	**Collisions (%)**
Warning threshold	>15	>25	>0.1	>5
Critical threshold	>20	>40	>1	>10

Non SNMP Approaches and Protocols

- SNMP is not the only way to retrieve information or monitor remote systems. Apart from SNMP there are a number of remote administration options including third party commercial tools.
- HTTP server (agents)
- Telnet and SSH Command Line Interface (CLI)
- Vendor tools such as Cisco CNA
- VNC remote control
- Terminal services
- NetFlow and SFlow

Web Interface for Cisco 2960



Catalyst 2960 Series Device Manager - Switch1

Language: English

Uptime: 3 hours, 47 minutes

Next refresh in **11** seconds

View : Duplex

Move the pointer over the ports for more information.

Express Setup

Network Settings

Management Interface (VLAN ID): 1

IP Address: 192 . 168 . 1 . 201

Subnet Mask: 255.255.255.0

Default Gateway: . . .

Switch Password: •••••

Confirm Switch Password:

Optional Settings

Host Name: Switch1

Telnet Access: ● Enable ○ Disable

Telnet Password: •••••

Confirm Telnet Password:

SNMP: ● Enable ○ Disable

SNMP Read Community: public

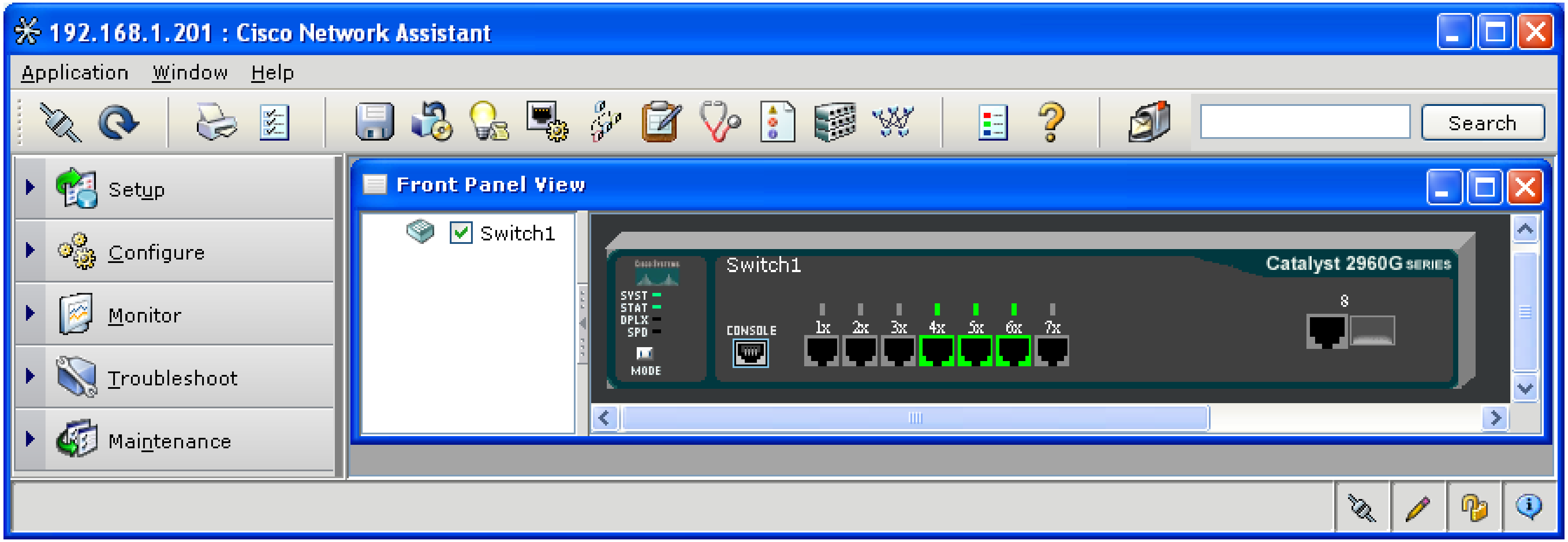
SNMP Write Community:

System Contact: home

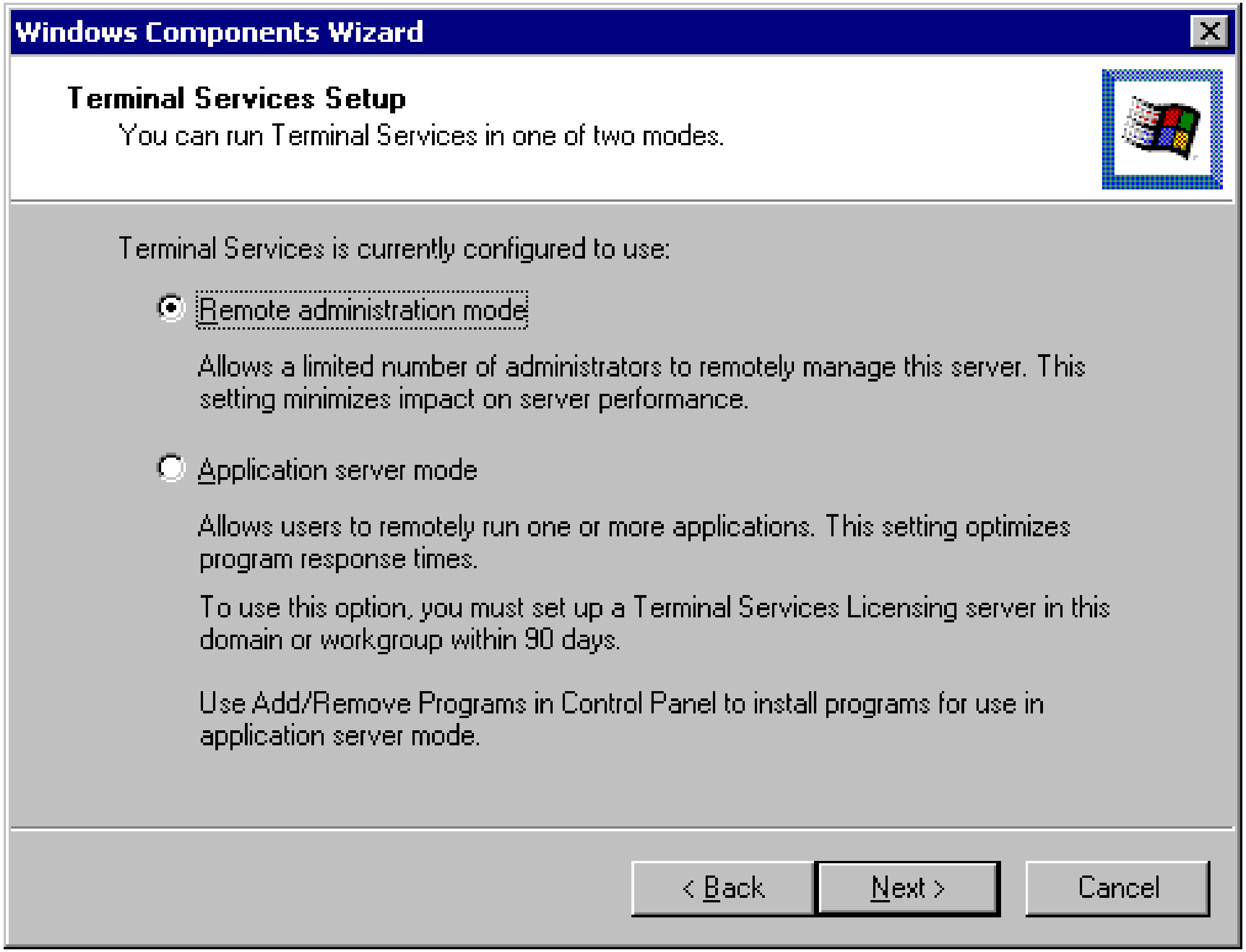
System Location: bedroom

Done

Cisco Network Assistant



Terminal Services



Windows Components Wizard

Terminal Services Setup

You can run Terminal Services in one of two modes.

Terminal Services is currently configured to use:

● Remote administration mode

Allows a limited number of administrators to remotely manage this server. This setting minimizes impact on server performance.

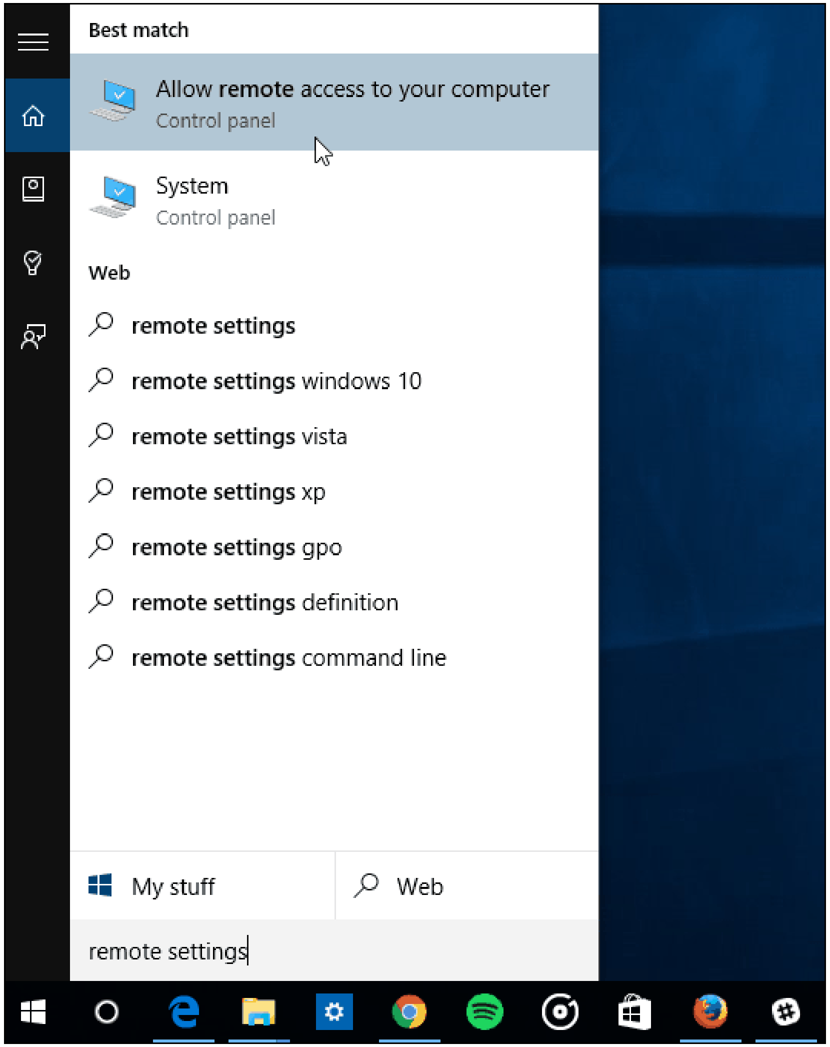
○ Application server mode

Allows users to remotely run one or more applications. This setting optimizes program response times.

To use this option, you must set up a Terminal Services Licensing server in this domain or workgroup within 90 days.

Use Add/Remove Programs in Control Panel to install programs for use in application server mode.

Windows Remote Desktop



Best match

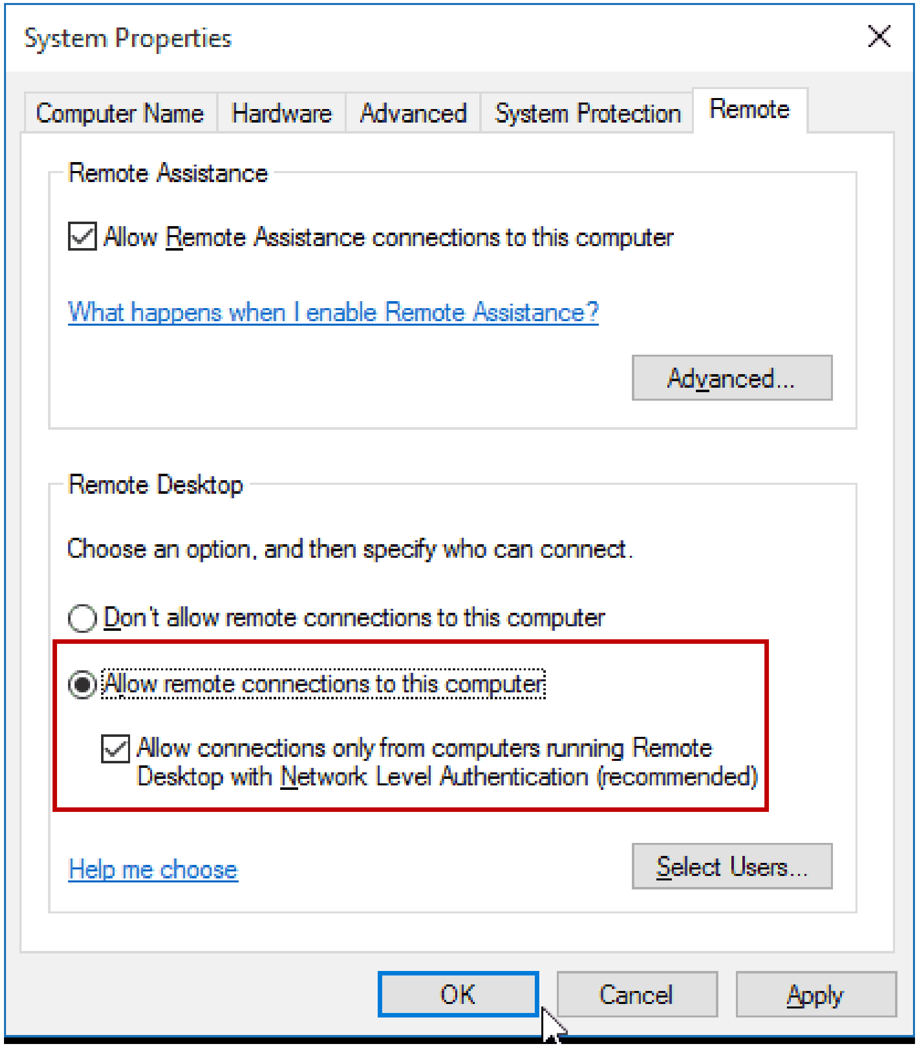
Allow remote access to your computer
Control panel

System
Control panel

Web

- **remote settings**
- **remote settings** windows 10
- **remote settings** vista
- **remote settings** xp
- **remote settings** gpo
- **remote settings** definition
- **remote settings** command line

remote settings



System Properties

Remote Assistance

☑ Allow Remote Assistance connections to this computer

What happens when I enable Remote Assistance?

Remote Desktop

Choose an option, and then specify who can connect.

○ Don't allow remote connections to this computer

● Allow remote connections to this computer

☑ Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)

Help me choose

NetFlow and sFlow

- Vendors of network equipment have introduced their own network monitoring and analysis protocols.
- NetFlow is found in Cisco IOS equipment.
- sFlow is found in HP and other equipment.
- Both are standard traffic reporting mechanisms embedded in certain routers and switches,
- Use UDP to collect and summarise traffic statistics.

Self-Study Resources

- Overview of Cisco Prime Infrastructure https://www.youtube.com/watch?v=Zjtl-P4tpsk
- Log Management and Graphing https://www.youtube.com/watch?v=ASM1qEtNMl0
- MicroNugget: Configuring SPAN and RSPAN on a Cisco Switch https://www.youtube.com/watch?v=GyDpkVoix00
- SNMP Operation https://www.youtube.com/watch?v=tg47MZdtcAE
- MicroNugget: Understanding and Configuring SNMPv3 https://www.youtube.com/watch?v=YZ5gBrA0B0U
- An Overview of Networking Monitoring Tools https://www.youtube.com/watch?v=NNCmjk0LpCU&list=PLVRajpWUvpnM0SfQR00MjILdjTrx1u-18
- How LMS can help with Network Performance Monitoring https://www.youtube.com/watch?v=TmVGgKuHaxM