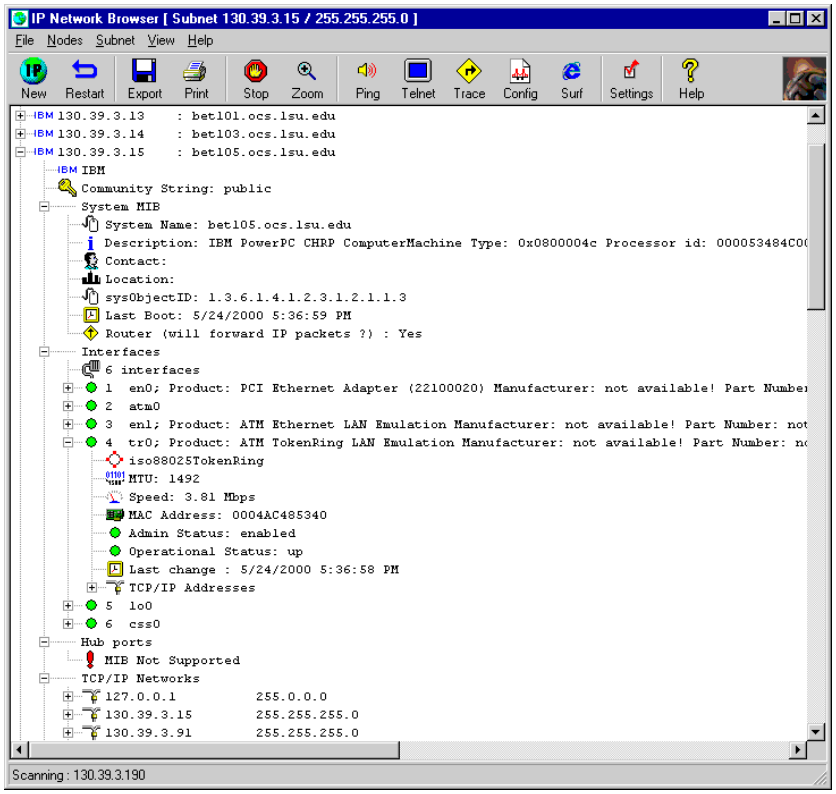
5.7.1

NETWORK DISCOVERY: ICMP & SNMP

(SolarWinds)



Objective

At the end of this lab students will be able to use Solarwinds IP Network Browser to discover detailed information of any hosts on the local TCP/IP network.

Information for Laboratory

A. Students will utilize Solarwinds IP Network Browser, a TCP/IP network discovery utility
B. Students will utilize Simple Network Management Protocol on Windows XP and Cisco equipment.

Student Preparation

The student will have completed requisite reading. The student will require paper for notes and should be prepared to discuss the exercises upon completion.

Instructor Preparation

You will need Solarwinds IP Network Browser installed and functional on your computer. You will also need to install SNMP on Windows XP and if possible on any available Cisco equipment.

An evaluation copy of IP Network Browser is available at www.solarwinds.net.

Estimated Completion Time

60 Minutes

Network Discovery

You may be surprised to find what, and possibly, who is connected to your network. Network discovery can help you quickly and easily learn how your network is setup, take an equipment inventory, discover unknown equipment, discover unknown IP addresses with access to your network, discover network bottlenecks, misconfigurations, and single points of failure. Network discovery is an important and useful network management utility. In large, constantly growing networks, it is difficult to tell how exactly the network is layed out. This is extremely important when making decisions to troubleshooting problems and adding new hardware to an existing network. A good network discovery utility can help in these situations.

SNMP

SNMP has two different basic levels of security access, Read-only and Read-write. These different levels of security are referred to as SNMP communities. The SNMP community string is like a user id or password that allows access to a device's statistics or information. The SNMP Read-only community string enables a remote device to retrieve "read-only" information from a device. The SNMP Read-write community string allows a remote device to read information from a device and to modify settings on that device. The most commonly used SNMP community strings are Public for Read-only, and Private for Read-write access.

Solarwinds IP Network Browser

IP Network Browser is an interactive TCP/IP network browser for Windows. It can scan an IP subnet and show what devices are responding on that subnet. It can discover details about each interface, Frame Relay DLCIs, IOS levels, flash memory, hub ports, installed cards, routes, ARP table, and many other details. IP Network Browser is a part of the Solarwinds Professional edition toolset, and is a commercially licensed

product, with a 30 day evaluation demo available for download.

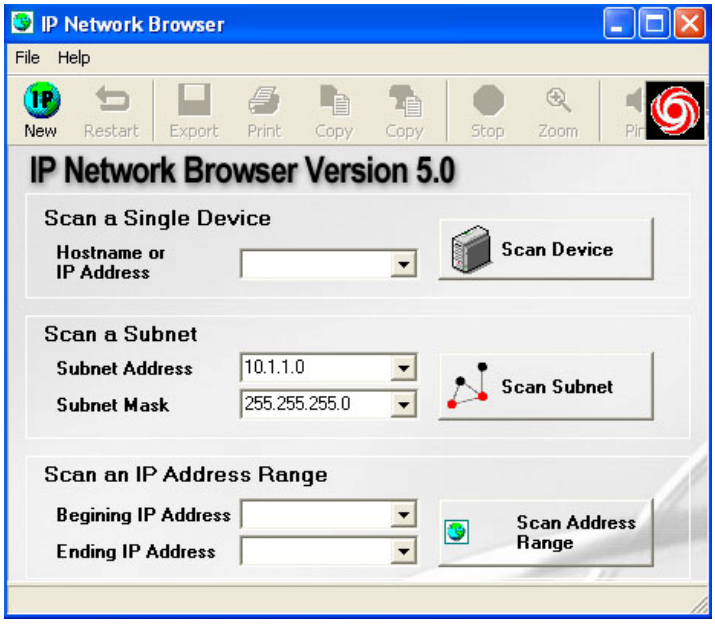
Step 1: Scan Local subnet for hosts

From START, Run, type CMD in the Open Box, and click OK.

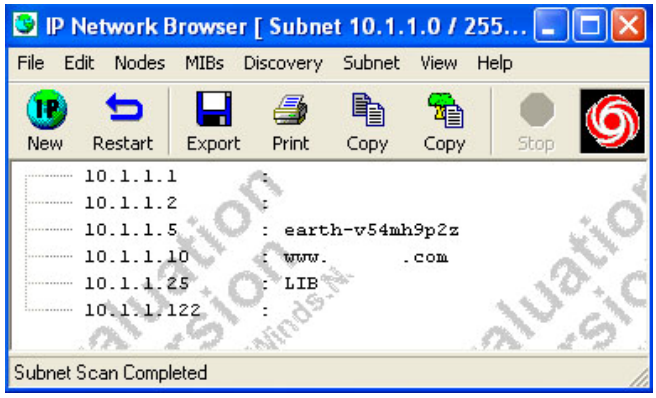
At the prompt, type IPCONFIG and press enter

This will display your current TCP/IP configuration. Note the IP address and Subnet Mask. Using the above example, 10.1.1.5 with a 255.255.255.0 Subnet Mask, belongs to the 10.1.1.0 Subnet.

Next, from START, All Programs, Solarwinds, Network Discover, launch IP Network Browser.



Enter your local Subnet address, and Subnet Mask in the Scan a Subnet boxes, and Click Scan Subnet.



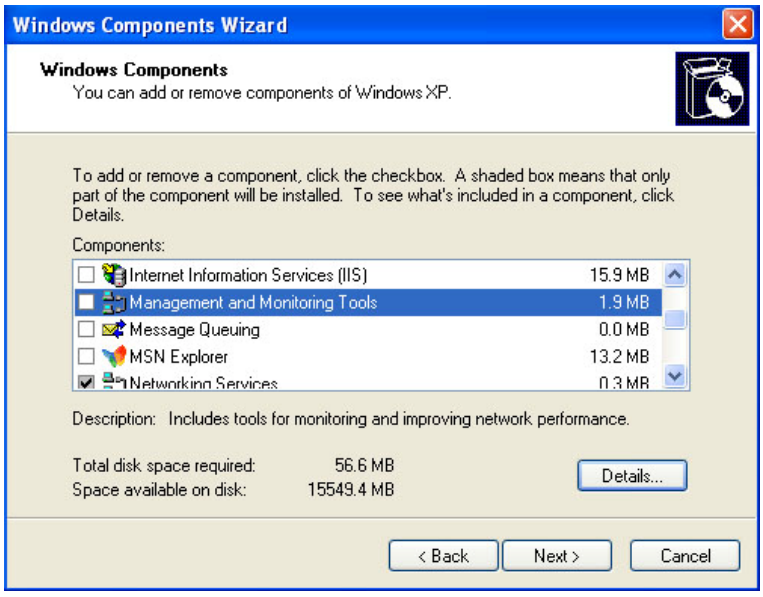
IP Network Browser performed a ping sweep, attempting to ping all hosts on the subnet entered. All hosts on that network are listed in the box, with the DNS host name if available.

As you can see, there is not much information on each host, only IP Address and DNS name if available. From this information, you would never know that 10.1.1.5 is a Windows XP computer, and 10.1.1.122 is a Cisco Router. To find more information on each network host, SNMP is needed.

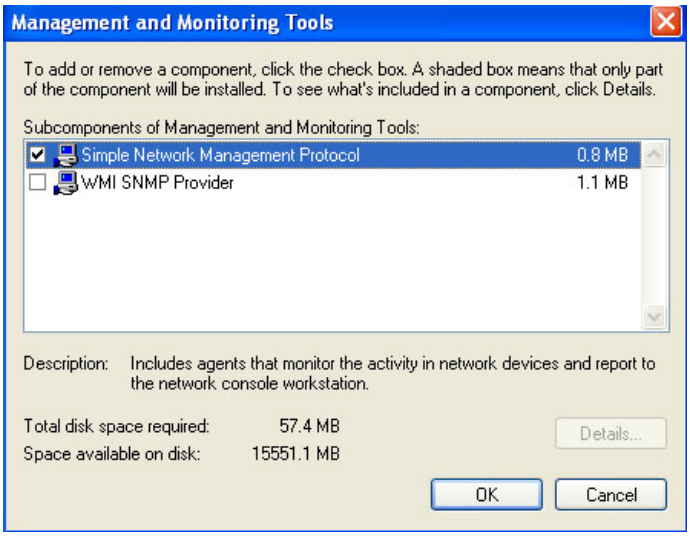
Close the IP Network Browser.

Step 2: Enable SNMP on Windows XP

From START, Control Panel, Add or Remove Programs, Click Add/Remove Windows Components on the left hand side.



Scroll down and click on Management and Monitoring Tools. Then Click the Details button.

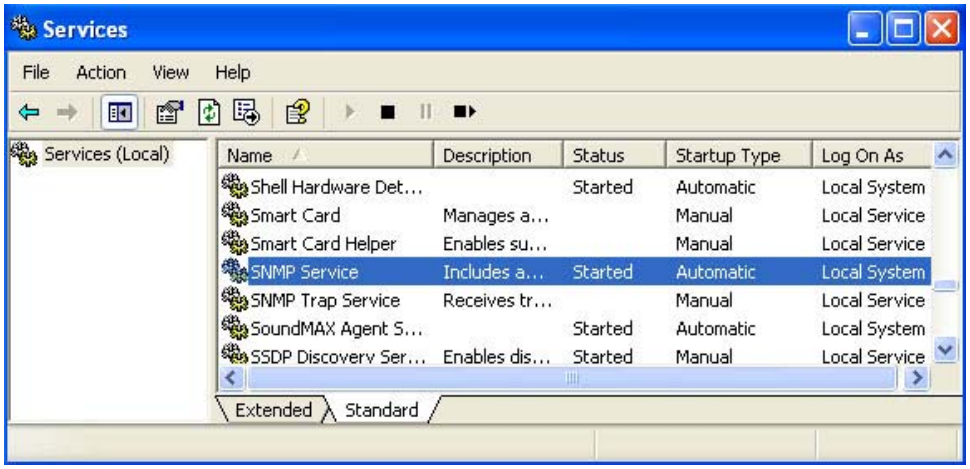


Click OK to accept and close the box. Click Next on the Windows Components Wizard box to finish the install. Close Add/Remove programs, and the Control Panel.

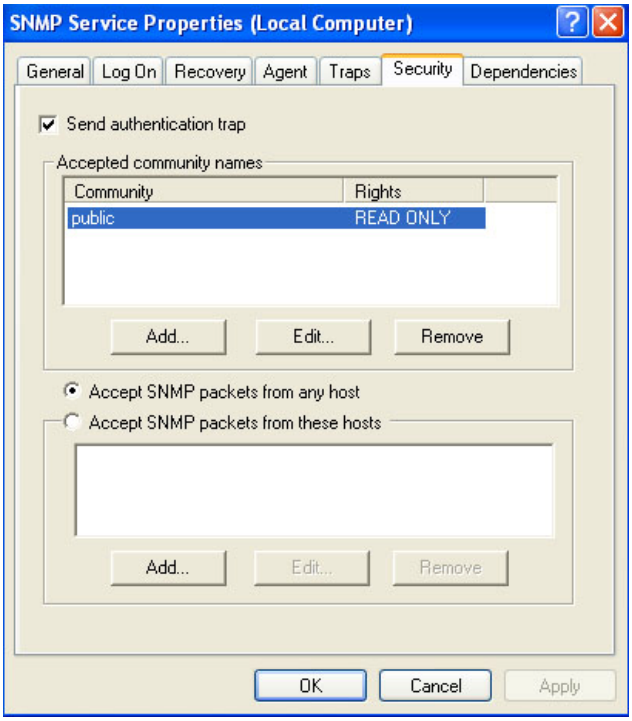
Note: You may need access to the original Windows XP installation disk to properly install the SNMP service. Check with your instructor for further details if necessary.

Step 3: Viewing the default WinXP SNMP community string

From START, All Programs, Administrative Tools, launch Services, or from START, Administrative Tools, lauch Services. Double click on the SNMP Service as below.



From the SNMP Service Properties box, Click on the Security Tab at the top. Notice the default SNMP Community string of public. Leave the community string public with READ ONLY access.



Step 4: Enable SNMP on Cisco equipment

Connect and enter Exec mode on the router or switch. Enter config mode. From the prompt, type
'snmp community public ro' and press enter. The RO is short for read-only access.

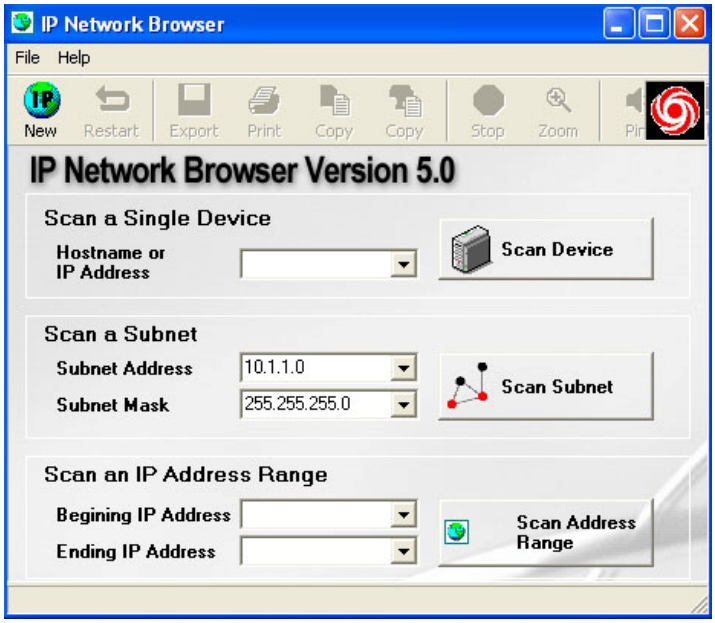
Ex. Router(config)#snmp community public ro

Show the running config 'sh run' to verify. You should see the following in the config…

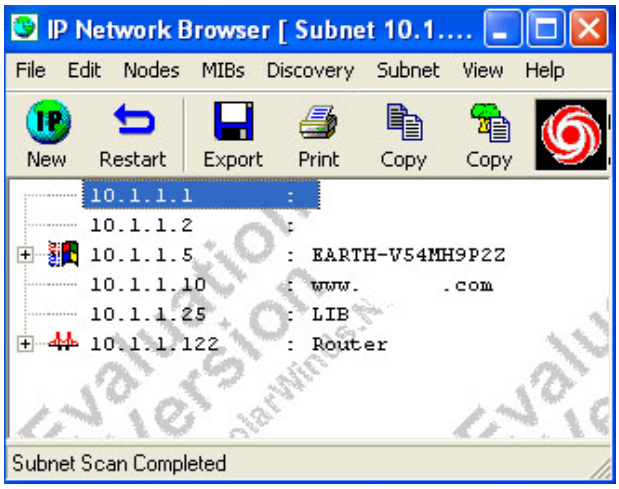
snmp-server community public RO

Step 5: Scan Local subnet for hosts

Launch Solarwinds IP Network Browser.

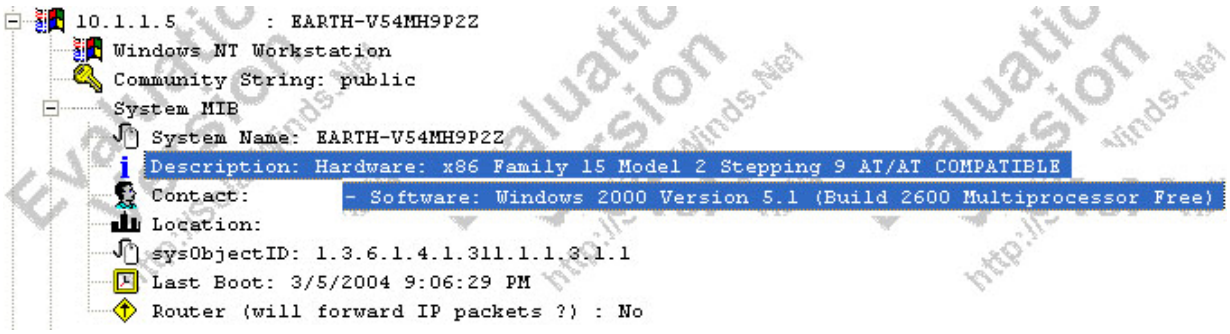


Enter your local Subnet address, and Subnet Mask in the Scan a Subnet boxes, and Click Scan Subnet.



As you can see from the example above, IP Network Browser was able to detect that 10.1.1.5 is a Windows Computer, and 10.1.1.122 is a Cisco router.

Double Click on your Windows XP workstation, and expand the System MIB node. Click on Description, and notice that it is listed as Windows 2000 version 5.1, otherwise known as Windows XP.

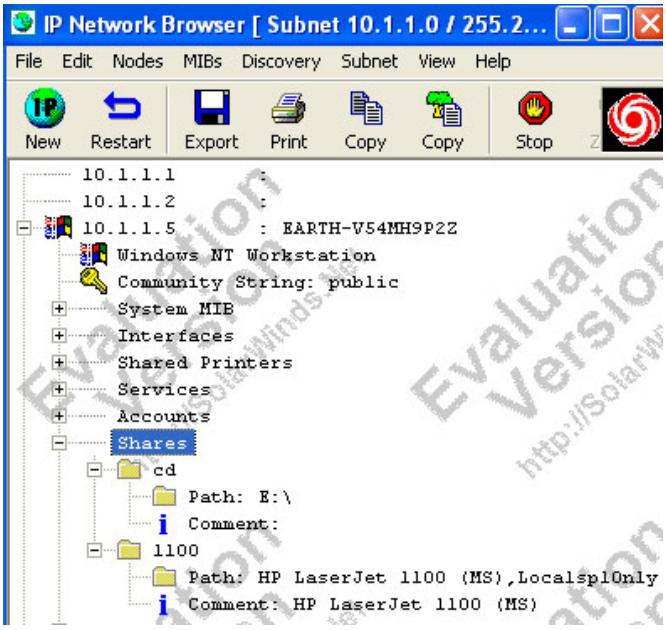


From START, Run, type CMD in the Open Box, and click OK.

At the prompt, type VER and press enter. Verify that it is infact Windows Version 5.1 build 2600 as reported by IP Network Browser.

Click and expand the Shares node, and expand all shares.

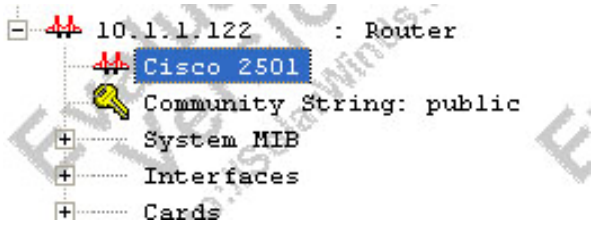
Notice the share name, and the given path. In this example, the share 1100 is a Hewlett Packard LaserJet 1100 Printer.



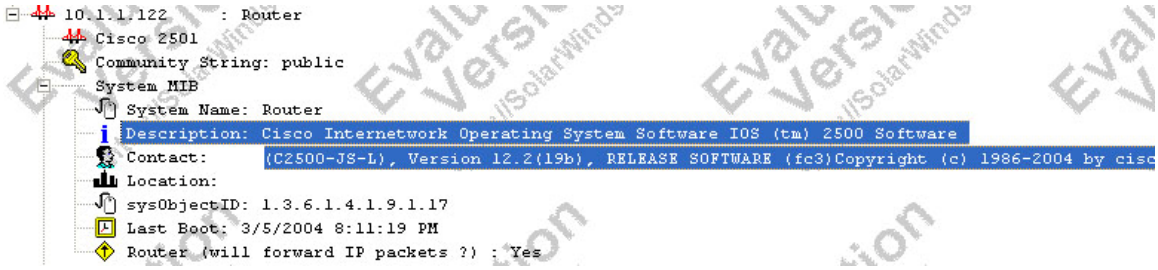
Go through the rest of the nodes, expanding them all, and take a close look at the amount of data that is available. As you can see, there is a lot more information available via SNMP discovery vs. the ICMP discovery.

Double Click on the Discovered Cisco equipment.

Notice the second line shows the model of the equipment.



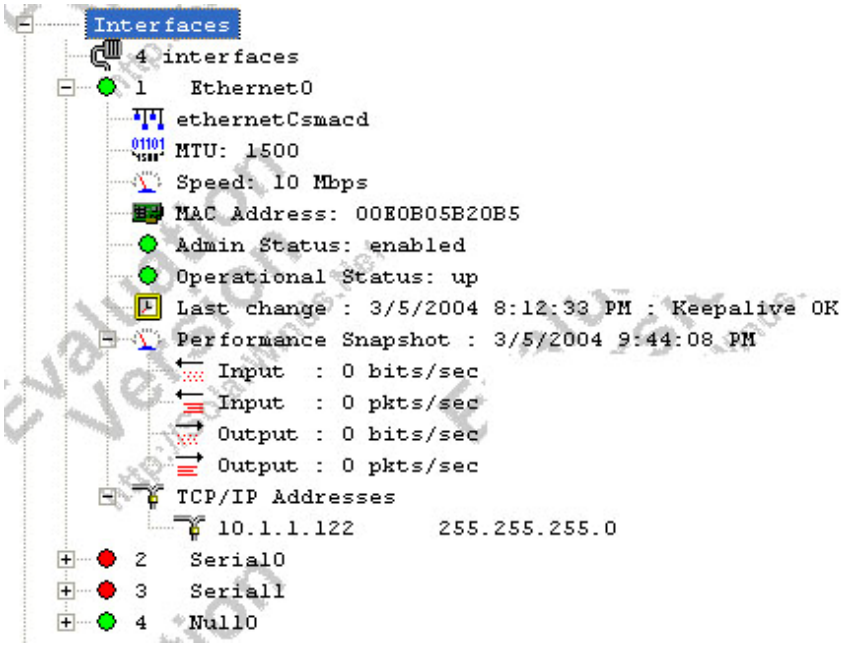
Expand the System MIB node. Notice under description it shows the Cisco IOS Verison.



From the Cisco equipment, verify the IOS version by issuing the show version command.

```
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-JS-L), Version 12.2(19b), RELEASE SOFTWARE (fc3)
Copyright (c) 1986-2004 by cisco Systems, Inc.
```

Expand the Interfaces node, and expand the first “up” Ethernet port. Notice the amount of data shown. You can tell that this ethernet interface is CSMA/CD, has a MTU of 1500, is running at 10 Mbps, the MAC hardware address is 00E0B05B20B5, and the TCP/IP address is 10.1.1.122 with a 255.255.255.0 subnet mask.



Again, go through the rest of the nodes, expanding them all, and take a close look at the amount of data that is available. As you can see, there is a lot more information available via SNMP discovery vs. the ICMP discovery.

Step 6: Analysis

1) For which applications is network discovery best suited?

2) After working with Solarwinds IP Network Browser, what about network discovery do you feel you should study further? Why?

3) Why should you enable SNMP on your network?

4) Why should you not use the SNMP community name public?

Summary Discussion

A classroom discussion should follow the lab. Review the lab questions and your analyses as a group. Share your experiences and knowledge with the class.

Appendix:

This lab was developed using Solarwinds Standard Edition Version 8. A trial of this version may be obtained using the download link from:

http://www.solarwinds.net

The OS environment for this lab was Windows XP Professional, Version 2002, Service Pack 2 (8/04).