

## 10: SNMP and Network Management Basics

### Objectives

- Upon completion of this chapter, you should be able to:
  - Explain basic Network Management concepts and terminology
- **Note:** *We'll revisit SNMP in more depth later in the class*

## What Is Network Management?

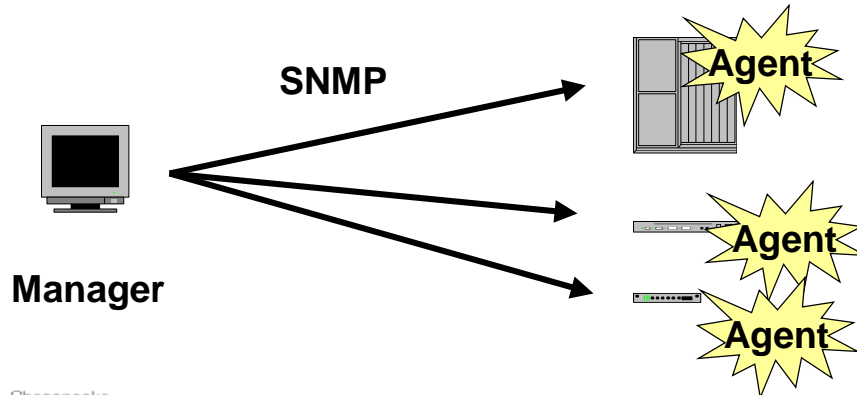
- Class discussion:
  - *What is Network Management?*
  - *Why do we do it?*

## SNMP: What Is It?

- Simple Network Management Protocol
  - Security's Not My Problem?
- Manager and agent communicate via SNMP
- HP OpenView NNM supports
  - SNMP version 1 (SNMPv1)
  - SNMP version 2, Community-based (SNMPv2C)
- Cisco IOS now supports SNMPv3 and earlier
  - SNMPv3 has its own built-in security
  - But there are no/few tools to simplify administration, so it is not widely used

## SNMP Terminology

- The manager station sends SNMP to Agents to ask for information or to tell the Agents to do something



## What Does SNMP Do?

- Manager can retrieve (**get**) information from the agent
- Manager can change (**set**) information in the agent
  - **Sets** can change variables (settings, configuration) in the agent device
  - **Sets** can initiate actions in devices
    - Reply to set indicates new setting in device
    - For example, with Cisco routers, a **set** can cause a router to reboot or send or receive a configuration file

## What Does SNMP Do -- 2

- Agents can **spontaneously** send information to the manager without a request
  - **Trap** (SNMPv1, v2, v2c, v3), unacknowledged
  - **Inform** (SNMPv2, v2c, v3), acknowledged, reliable
- The agent has to be told which management stations (managers) to send traps (notifications) to
  - Traps are supposed to indicate a significant event or problem
  - For example, a reboot

## SNMP Community String

- SNMP community strings act like passwords
- May have several valid community strings
  - Except in some of the Cisco Catalyst switches
- If manager sends one of the correct Read-Only (RO) community strings, it can **get** information but not **set** information in an agent
- If the manager uses one of the correct Read-Write (RW) community strings, it can **get** or **set** information in the agent
  - In Cisco routers, **set** access is equivalent to having the enable password
  - Choose RW community string well and guard it like the enable password!

## What is a MIB?

- MIB = Management Information Base
  - *“The documentation”*
- A MIB **object** is a piece of information available from an agent, an SNMP **variable**
- Each copy of an object is an **instance** (example: router or system interfaces)
- *More details later in course*

## SNMPv1

- Most common management protocol in use in data networks
- Provides a means of obtaining information from, and sending information to, network devices
- Based on the manager-agent model
- Uses Management Information Bases (MIBs) to exchange information

## SNMPv2C

- Includes the basic functions of SNMPv1
  - Can co-exist with SNMPv1
- Some new message types
  - Retrieval of large amounts of management information using fewer network resources (GetBulk)
- Standardized multi-protocol support
  - But now the world is predominantly IP
- Enhanced security was planned but dropped
  - The “C” stands for community-based security

## SNMPv3

- Completes the securing of SNMP
- Generalized architecture of manager and agent to describe how components interact
  - Result: the RFC's got harder to read
  - See however RFC 2570
- Many sites may use IPsec instead to secure their SNMP communications
  - IPsec is more widely known
  - IPsec administrative framework already in place

## Resources

- ***The Simple Book: An Introduction to Networking Management (Second Edition)***
  - Marshall Rose, Prentice-Hall, 1996. ISBN: 0134516591
- ***Network Management: A Practical Perspective***
  - Allan Leinwand and Karen Fang Conroy, 1996. Addison Wesley, ISBN: 020160991
- ***Windows NT SNMP. 1st Edition.***
  - James Murray, O'Reilly & Associates, 1998. ISBN: 1565923383

## Network Management Web Sites

Web Site	URL Description
<a href="http://netman.cit.buffalo.edu/">http://netman.cit.buffalo.edu/</a>	Links and net management documents
<a href="http://www.simple-times.org/">http://www.simple-times.org/</a>	The Simple Times newsletter (SNMP newsletter)
<a href="http://www.ietf.org">http://www.ietf.org</a>	Internet Engineering Task Force, RFC Standards Documents
<a href="http://www.iol.unh.edu/training/">http://www.iol.unh.edu/training/</a>	Tutorials
<a href="http://home.att.net/~p.welcher/misc/links.htm">http://home.att.net/~p.welcher/misc/links.htm</a>	Network management links
<a href="http://www.smartbooks.com">http://www.smartbooks.com</a>	Lists of books
<a href="http://www.dmtf.org">http://www.dmtf.org</a>	Desktop Management Task Force

## Review Questions

- What is an SNMP manager? Agent?
- Can they both co-exist on the same machine?
- What is the purpose of community strings?
- Explain the purpose of SNMP traps

## Summary

- Having completed this chapter, you should be able to:
  - Explain basic Network Management concepts and terminology