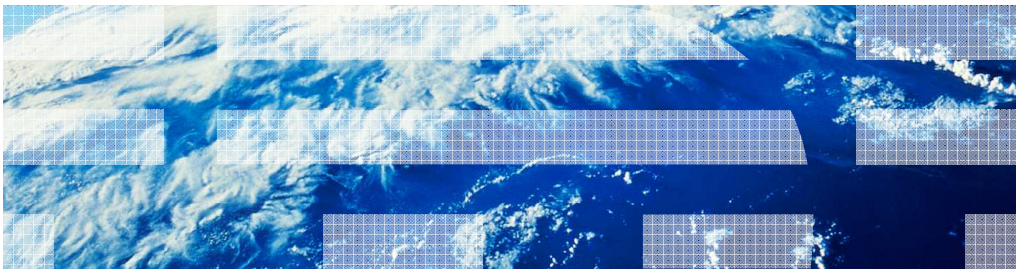
IBM WebSphere CloudBurst Appliance V2.0

SNMP overview

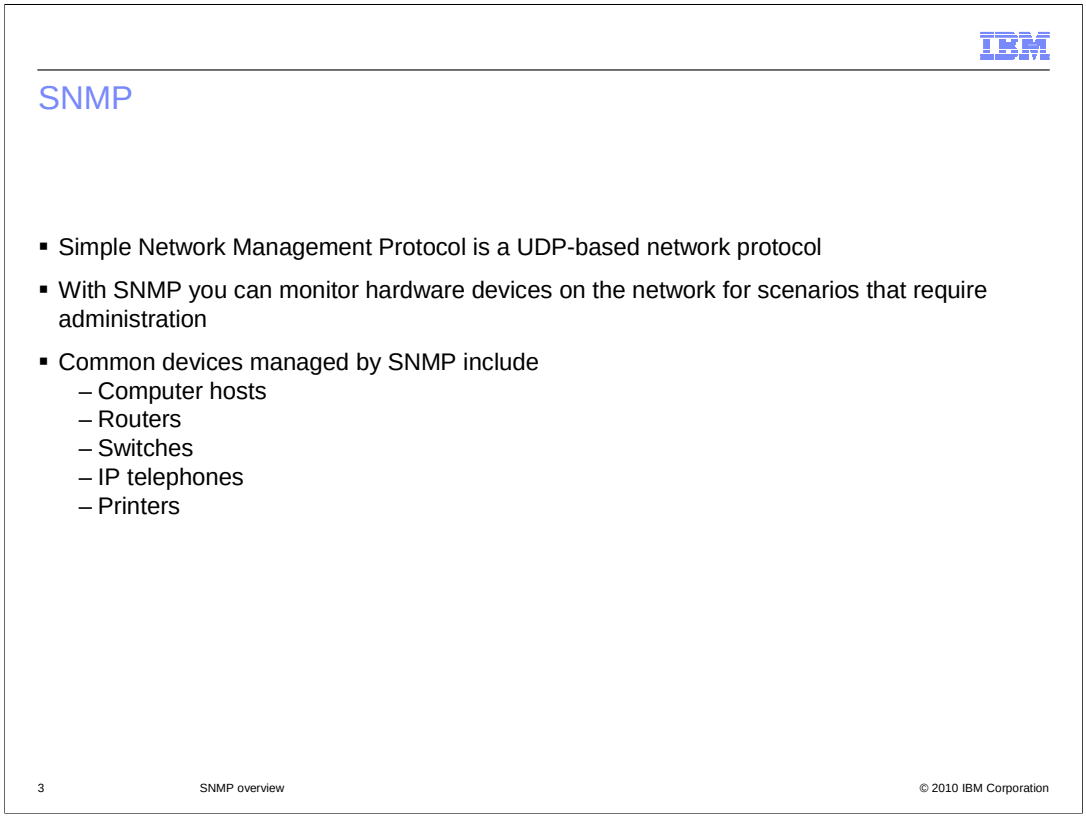


This presentation will discuss the Simple Network Management Protocol.

Agenda

- Simple Network Management Protocol (SNMP)
- Basic SNMP components
- Summary

This presentation will discuss Simple Network Management Protocol and it’s components.



Simple Network Management Protocol is commonly known as SNMP. SNMP is a UDP-based network protocol that is commonly used to communicate with hardware devices on a computer network. SNMP provides a mechanism for monitoring hardware devices, and altering their configurations by requesting information from a service running on the hardware called an agent, and sending the agent requests to alter the hardware's configuration. Hardware devices that are commonly monitored and managed using SNMP include computer hosts, routers, switches, IP telephones, and network printers. Using an SNMP client to communicate with the hardware's SNMP agent, information about the current state of the hardware can be determined. Based on this information, requests can be sent to the device using SNMP to alter it's configuration.

Basic SNMP components

- Managed device (also called the ‘slave’)
- Agent (software service running as a daemon on the slave)
- Network management system (commonly referred to as NMS)
  - Read-only or read-write access to slave
  - Gathers information from the managed device and can send settings to alter the managed devices configuration if granted read-write access
  - SNMP client to interface with slave’s agent
- Managed device is monitored by one or more network management systems
  - Executes applications to monitor and control the slave

The three basic components of an SNMP scenario are a hardware device to be managed, a service that runs on that device called an agent, and a network management system. The service that runs on the hardware to be managed using SNMP is called an agent. The agent is commonly run as a daemon on the device and is constantly listening for requests. When the agent receives an SNMP request from a client, it will return information requested about the state of the hardware. One example of a commonly requested piece of information for a computer system is it’s hard drive capacity. SNMP clients can request the capacity of the hardware to determine how close the managed device is to having a full hard drive. A network management system consists of one or more computers on the network that are accessing information about the hardware using the managed device’s agent, and making adjustments to the device using SNMP based on that information. In order to make adjustments to the hardware device’s configuration the SNMP client must be granted read-write access by the hardware’s SNMP agent. If a client has read-only access, it will only be allowed to receive information about the hardware’s state and is not granted permission to change it’s configuration using SNMP. SNMP client applications can be developed to monitor a device’s configuration, and automatically send requests to make adjustments to the hardware based on it’s monitored data.

SNMP agents

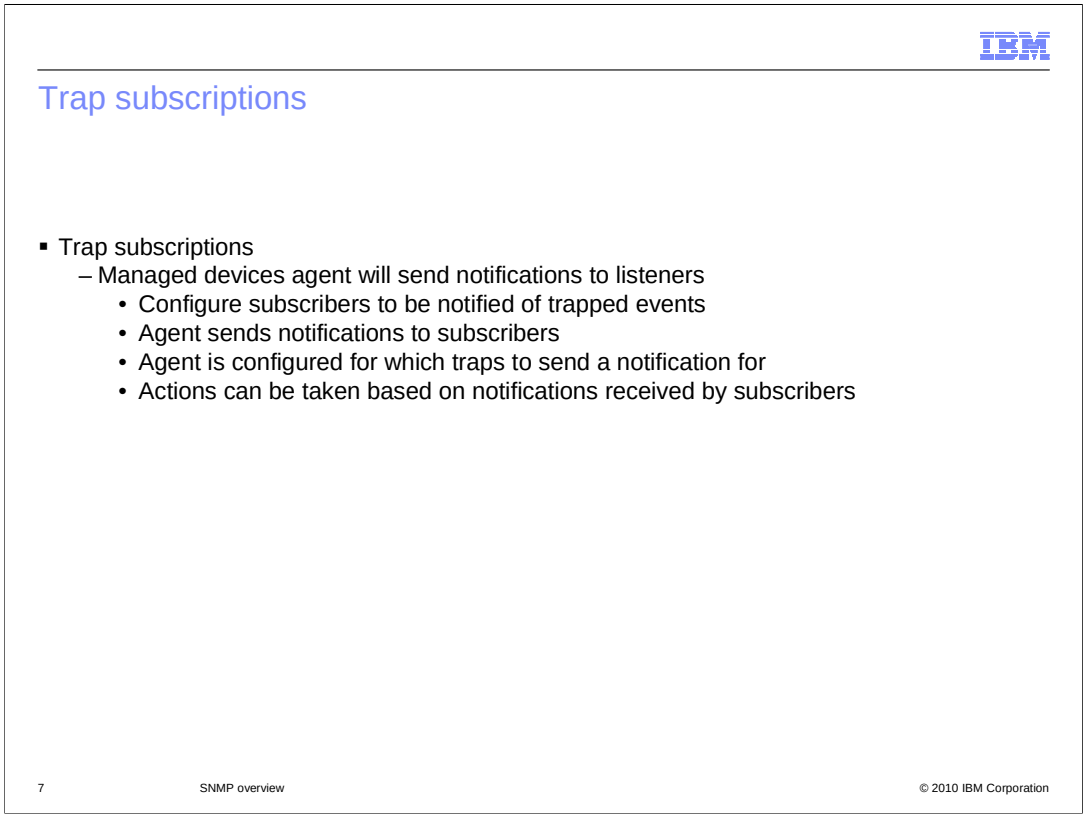
- An SNMP agent on a managed device exposes status information as variables
  - Various data can be made available about the device using SNMP for example:
    - System name
    - Free memory
    - Processor usage
    - Uptime
- SNMP agent can also accept requests from clients to perform ‘active’ administration
  - Modify managed devices configuration
- Agent status information and active administration commands are defined in “MIB” files

The SNMP agent provides information to SNMP clients, and makes adjustments to the hardware device’s configuration based on requests it receives from those clients. Agents can provide a wide variety of data about the hardware device. The information that an agent has available to send to an SNMP client is defined in a management information base, or MIB file. SNMP clients will use the agent’s MIB file to see what requests it can make, and what information it can gather from the agent. It will also use the agent’s MIB files to see what requests it can make to alter the hardware’s configuration.

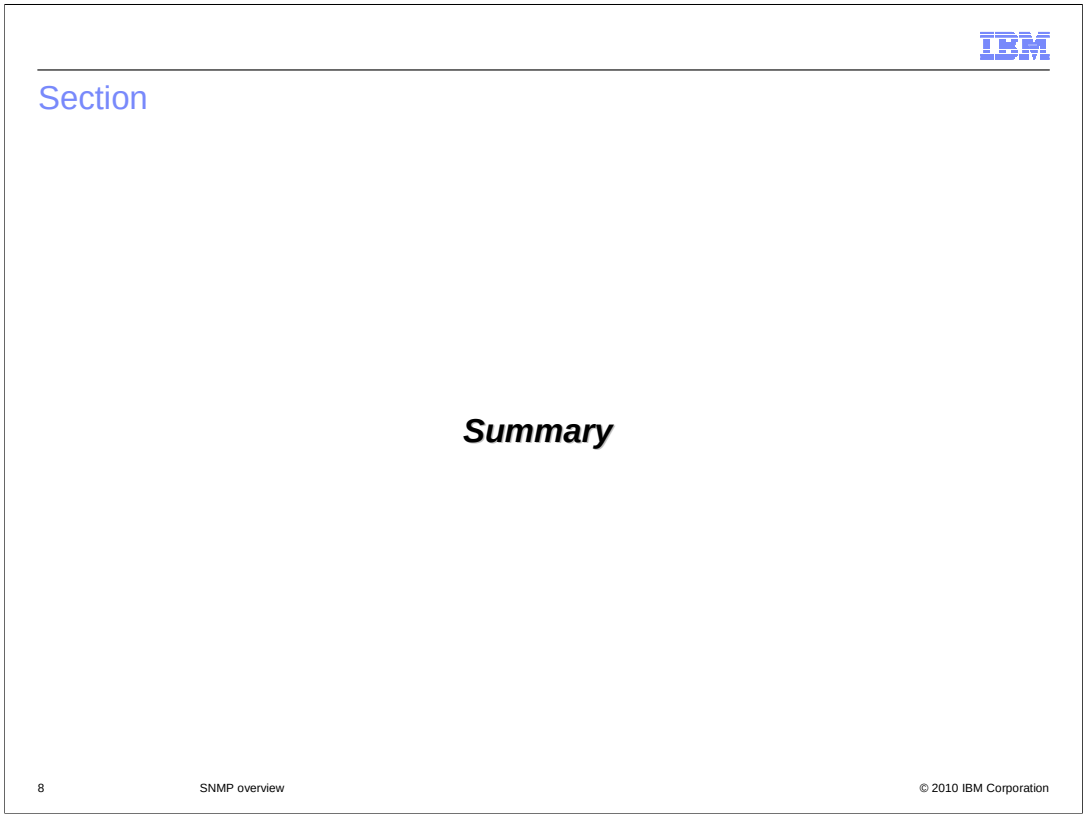
SNMP MIB files

- MIB
  - Management information base
  - File that defines variables that can be read or set on the managed device using SNMP
    - Defines information about the managed device that can be polled for using SNMP clients
    - Defines active management settings that can be set or changed to alter the device configuration using SNMP

An SNMP management information base file contains variables that can be read or set on the managed device using SNMP. Clients get a copy of the hardware agent's MIB files, and use them to access data and send requests to change the hardware's configuration using SNMP requests. MIB files are flat text files.



Trap subscriptions are notifications that can be sent out by the SNMP agent to SNMP clients that subscribe to receive them. SNMP agents define variables for events, such as error conditions, and will send a notification to registered SNMP clients when those events occur. The clients to receive SNMP trap notifications are configured on the agent. The managed device's agent will send SNMP notifications to configured clients on the port number they specify. Setting up a trap subscription is performed by a system administrator who is responsible for configuring the managed device's SNMP agent settings. Trap subscription events can be used by SNMP clients to automatically take action to correct hardware configuration of the managed device based on the trap that occurs.



This section will summarize the SNMP overview.

Summary

- SNMP agents are a running service that can be probed for status information or send notifications to subscribers
- SNMPv2c communities can be used to restrict access to the SNMP agent
- Trap subscriptions can be configured to send notifications to listeners using a trap daemon client
- Trap subscribers are configured on the agent

SNMP is a network protocol that allows clients to gather information about a hardware device, and manage it's configuration. The SNMP agent can be probed for status information, and send notifications to clients using traps and trap subscriptions. SNMP communities specify credentials to access the SNMP agent. Community settings allow SNMP clients to have read or read/write access to hardware information, and can restrict access to the SNMP agent based on host name. Traps are configurable items that can fire event notifications to clients based on a specific hardware event occurring, for example, a client can be notified of a processor cooling fan failure. Clients that want to be notified of Trap events must be configured on the agent as a trap subscriber. Trap subscribers are configured using their host names or IP addresses, the port number their SNMP trap daemon is running on, and a community configuration that the trap daemon specifies.

Feedback

Your feedback is valuable

You can help improve the quality of IBM Education Assistant content to better meet your needs by providing feedback.

- Did you find this module useful?
- Did it help you solve a problem or answer a question?
- Do you have suggestions for improvements?

Click to send email feedback:

mailto:iea@us.ibm.com?subject=Feedback_about_CB20_SNMPManagement.ppt

This module is also available in PDF format at: ../CB20_SNMPManagement.pdf

You can help improve the quality of IBM Education Assistant content by providing feedback.

Trademarks, disclaimer, and copyright information

IBM, the IBM logo, ibm.com, CloudBurst, Tivoli, and WebSphere are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of other IBM trademarks is available on the Web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS OR SOFTWARE.