Protocol Deep Dive - SNMP

OVERVIEW OF SNMP

Greg Dickinson
NETWORK ENGINEER

@GBDickinson www.hyperpowered.com

Overview

Versions

Data Format

- Gets
- Puts

Community Strings

- Read-Only
- Read-Write

Traps

Packet Structure

SNMP

Allows a Network Management System to collect data on a managed device and modify device parameters. It uses a Management Information Base to determine what parameters to gather.

Simple Network Management Protocol

Managed devices

Router/server/refrigerator, etc

SNMP Agent

Runs on managed devices

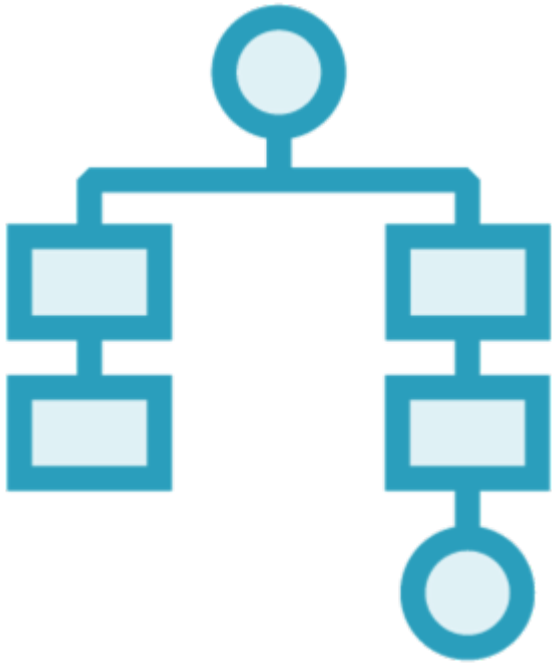
Network management station

Collects and displays SNMP data

Management Information Base

Translates raw SNMP data

SNMP v1



Formally introduced in 1988

- RFCs 1065-1068

Superseded in 1990

- RFCs 1155-1157

Poor security

- Requires external security
- Transmits community name in cleartext

SNMP v2

RFCs 1441 and 1452

Adds functionality

- GetBulkRequest

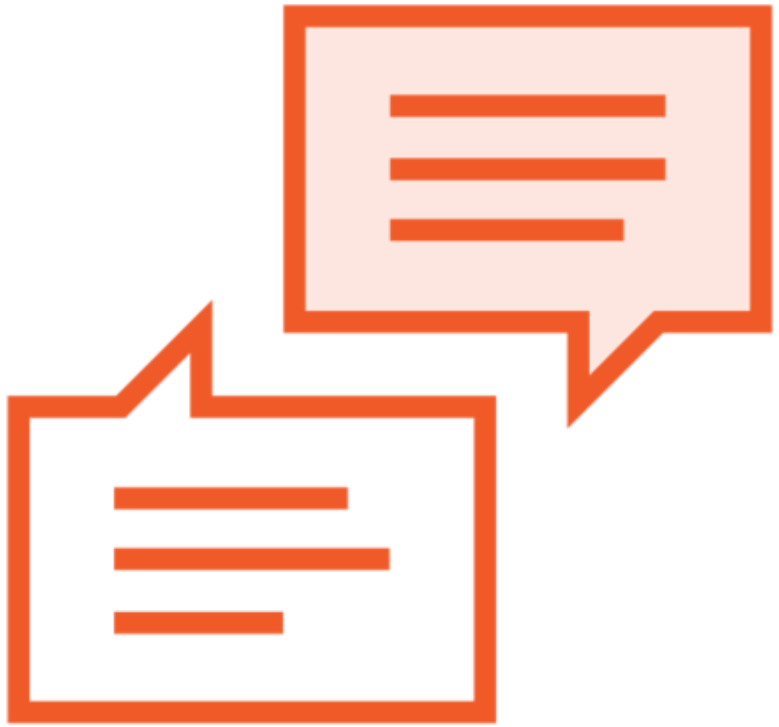
Added a security model

- Not accepted

SNMP v2c (RFCs 1901-1908)

- Takes the functionality without the security

SNMP v1 and v2c Interoperability



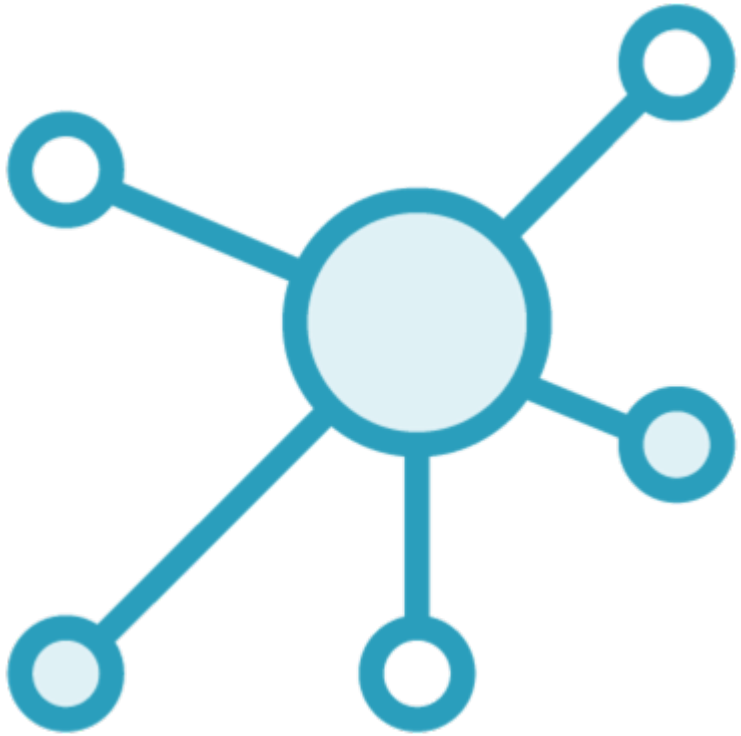
The two protocols are incompatible

- UDP header
- Protocol Data Unit format
- SNMP operations

Proxy agent

NMS supports both versions

SNMP v3



RFCs 3411-3418

Introduced a strong security model

- Communication encryption
- Identity verification
- User-based security model (USM)

Functionally equivalent to SNMP v2/v2c

Managing Network Devices

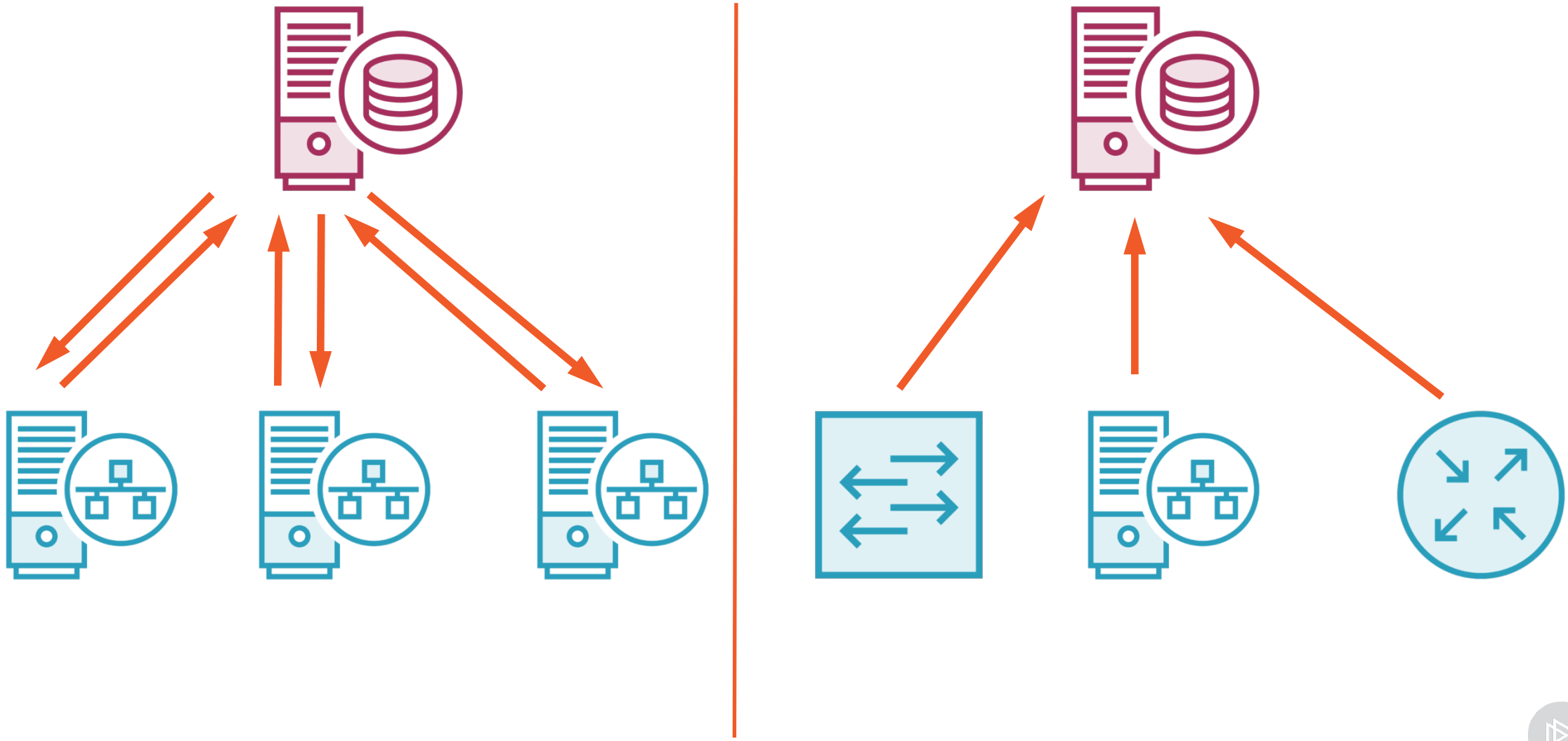
SNMP Get

Gathers information from networked devices. Uses a MIB to determine what OID to poll. Uses RO access.

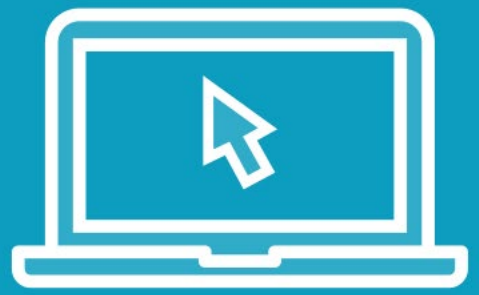
SNMP Put

Modifies information on a networked device. Can do everything from change an interface name to rebooting the device. Requires RW access.

SNMP Polling Versus Traps



Demo



Examine SNMP packets

Discuss security implications