

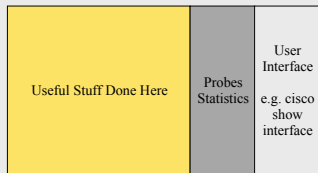
# SNMP

ITL

## Objectives

- Overview of SNMP
- SNMP Tools
- SNMP Monitoring Infrastructure

## A Perspective on Managing Network Nodes



## The Problem

- Vendor-specific code for every device is too expensive to maintain
- The device cannot spend resources interpreting complex requests
- SNMP: Simple Network Management Protocol – Simple commands, complexity placed into the management system

## SNMP Structure

- Simple Protocol Structure
  - Information retrieval
    - GET, GET-NEXT, GET-BULK
  - Setting Parameters
    - SET
  - Alarms
    - TRAP

## The Hard Part

- Create a description (database schema) for the information
  - Defines the type of information
  - Documents the meaning of the information
  - Allows many independently developed standards to be merged in a device

## MIB

- MIB: Management Information Base
- Defines an extensible classification scheme for pieces of information
- SMI: (Structure of Management Information) Codes the information and documentation into a formal specification language (ASN.1)

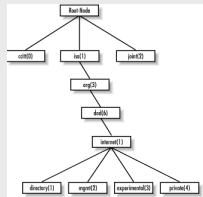
## The Classification Scheme

- Every group of related information items has a common prefix (sequence of integers)
- Prefixes are organized in a hierarchy
- Items can be single values or multiple instances of an item type

## Some Specifics

- The stuff we are interested in has the prefix "iso.org.dod.internet..."
  - iso (1)
  - org (3)
  - dod (6)
  - internet (1)
- Also written as 1.3.6.1
  - In the coded version formally defined as "internet"

## The "MIB Tree"



From: Douglas Mauro, Kevin Schmidt, "Essential SNMP", O'Reilly, 2001

## Example

- Most commonly used items are in
  - mib-2 {internet mgmt(2) mib-2(1)}
- The name assigned to an entity is
  - sysName {mib-2 system(1) sysName(5)}
- Interface-specific information
  - interfaces {mib-2 interface(2)}
- Information on router interfaces are in
  - mib-2 interface(2) ifTable(2) ifEntry(1) ifIndex(1) ....

## A more Concrete Example

```
ifNumber OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
    "The number of network interfaces (regardless of their
    current state) present on this system."
 ::= { interfaces 1 }
```

## snmpget

- Simple Unix command-line utility
- Sample Command and Output:

```
snmpget -v2c -c public sisko.csm.ohiou.edu system.sysName.0
system.sysName.0 = sisko.csm.ohiou.edu
```

*Note the ".0" at the end. The name or OID define a object class, so ".0" means an actual instance of the object type. In some cases there can be more than one instance.*

## snmpwalk

```
snmpwalk -v2c -c public sisko.csm.ohiou.edu interfaces
```

```
interfaces.ifNumber.0 = 3
interfaces.ifTable.ifEntry.ifIndex.1 = 1
interfaces.ifTable.ifEntry.ifIndex.2 = 2
interfaces.ifTable.ifEntry.ifIndex.3 = 3
interfaces.ifTable.ifEntry.ifDescr.1 = Ethernet0
interfaces.ifTable.ifEntry.ifDescr.2 = Ethernet1
interfaces.ifTable.ifEntry.ifDescr.3 = Serial0
interfaces.ifTable.ifEntry.ifType.1 = ethernetCsmacd(6)
....
```

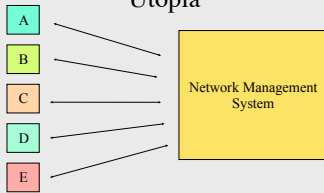
```
interfaces.ifTable.ifEntry.ifSpecific.3 = OID: .ccitt.nullOID
```

## SNMP Versions

- SNMP v1, SNMP v2, and SNMPv3 are currently standardized (but not always implemented)
  - Version 2 added new variable types and some new functions (e.g., get-bulk)
  - Version 3 addresses security (RFC 3414)

## Additional Slides

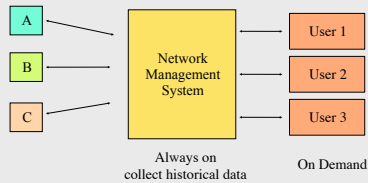
## The Network Management Utopia



## Final Thoughts

- SNMP's current primary use is for monitoring, not for configuration
  - SNMPv3 is proposed for a particular type of real-time device configuration
  - Non-SNMP based configuration systems are common
- Several high-end commercial network management systems exist that are based on SNMP for monitoring (HP Openview, Aprisma SPECTRUM, many others)
- Open Source systems include nagios, MRTG...

## Management System Structure



## The Formal Version

```
RFC1155-SMI DEFINITIONS ::= BEGIN
  nullOID OBJECT IDENTIFIER ::= { ccitt 0 }
  internet OBJECT IDENTIFIER ::= { iso org(3) dod(6) 1 }
  directory OBJECT IDENTIFIER ::= { internet 1 }
  mgmt OBJECT IDENTIFIER ::= { internet 2 }
  experimental OBJECT IDENTIFIER ::= { internet 3 }
  private OBJECT IDENTIFIER ::= { internet 4 }
  enterprises OBJECT IDENTIFIER ::= { private 1 }
END
```