What MIB Document Editors need to know

Bert Wijnen
bwijnen@lucent.com
What MIB Document Editors Need to Know About

- SNMP
- the MIB,
- MIB Modules and
- MIB Documents
Agenda

• SNMP and MIB context/background
• When does it make sense to define a MIB module for a protocol?
• Scope and Content of a MIB document.
• What tools are available to check/review MIB modules?
• What are the I-D checklist items related to MIB documents?
• What is a MIB doctor? When do I need one, and how do I find one?
• How to get MIB expertise in the WG?
The Varbinds are (your) MIB objects
Can be from multiple MIB modules
MIB modules are defined using the SMI (structure of Management Information) data modeling language
SNMP Status and Versions

• SNMP Message Wrappers:
  – SNMPv1
  – SNMPv2c
  – SNMPv3

• SNMP Protocol Operations (PDUs):
  – SNMPv1 Protocol Operations
  – SNMPv2 Protocol Operations

• Structure of Management Information (SMI):
  – SMIv1
  – SMIv2
SNMP Status – version 1

• SNMPv1 message wrapper
  – no Security,
  – i.e. community string (plain text password)

• SNMPv1 Protocol Operations
  – GET, GETNEXT,
  – SET
  – GETRESPONSE,
  – TRAPv1

• SMIv1 data types
  – MIB Modules in SMIv1 format
SNMP Status – version 1 (cont)

• SNMPv1 - (Full) Internet Standard
  
  ===⇒ but now HISTORIC

• RFC1157 (STD 15)  
  
  ===⇒ but now HISTORIC
  
  – Specifies Message Wrapper
  – Specifies Protocol Operations (PDUs)

• SMIv1 - (Full) Internet Standard
  
  – RFC1155 and RFC1212 (STD16) 
  
  – RFC1215 (informational)

• MIB II - (Full) Internet Standard

  – RFC 1213 (STD 17)
  – Various Other MIB Documents (Proposed and Draft Stds)
SNMP Status – version 2c

- message wrapper
  - no Security (community string (plain text password))

- SNMPv2 Protocol Operations
  - Improved PDU error codes, exceptions
  - GET, GETNEXT, GETBULK
  - SET
  - GETRESPONSE
  - TRAPv2, INFORMS

- SMIv2 data types
  - Textual Conventions
  - Conformance
  - MIB Modules in SMIv2 format
SNMP Status – v2c (continued)

• SNMPv2c - Mixed Standardization Levels
  – RFC1901 – experimental ➔ but now HISTORIC
    • Specifies Message Wrapper
  – RFC3416 (STD)
    • Specifies Protocol Operations (PDUs)
  – RFC3417 (STD)
    • Specifies Transport Mappings

• SMIv2 - (Full) Internet Standard (STD 58)
  – RFC2578 - SMIv2
  – RFC2579 - Textual Conventions for SMIv2
  – RFC2580 - Conformance Statements for SMIv2

• Various MIB Modules
  – RFC3418 (STD) and many others
SNMP Status - Architecture

• SNMP Architecture
  – Modular Approach, Extensible
  – Multiple Security Protocols/Mechanisms
  – View Based Access Control Model
  – Coexistence of multiple SNMP versions
    • Specifically SNMPv1, SNMPv2c, SNMPv3
    • Also future versions (if any)
  – Remotely Configurable via SNMP
    • users and their security mechanisms/secrets
    • access to MIB objects
    • notification destinations and filtering
    • proxy configuration
SNMP Status – version 3

• SNMPv3 message wrapper
  – Real Message Security
  – User Based Security Model
    • Authentication (SHA-1 and MD5)
    • Privacy (CBC-DES encryption)
  – Allows 3 security Levels
    • not Authenticated, no Privacy (same as SNMPv1/v2c)
    • authenticated but no Privacy
    • authenticated with Privacy
  – Replay protection (limited)
  – Message level error reporting (Reports)
  – Scoped PDU allows for Multiple Contexts
SNMP Status – version 3 (cont)

• SNMPv3 – (full) Internet Standard (STD 62)
  – RFC3410 - Introduction (Informational)
  – RFC3411 - Architecture
  – RFC3412 - Message Processing
  – RFC3413 - Applications
  – RFC3414 - User Based Security Model
  – RFC3415 - View-Based Access Control Model
  – RFC3416 - Protocol Operations
  – RFC3417 - Transport Mappings

• SMIv2 - (Full) Internet Standard (STD 58)
  – RFC2578 - SMIv2
  – RFC2579 - Textual Conventions for SMIv2
  – RFC2580 - Conformance Statements for SMIv2
SNMP Status – version 3 (cont)

• Various MIB Modules (full Internet Standard)
  – RFC3411 - SNMP-FRAMEWORK-MIB
  – RFC3412 - SNMP-MPD-MIB
  – RFC3413 - 3 MIB modules
    • SNMP-TARGET-MIB
    • SNMP-NOTIFICATION-MIB
    • SNMP-PROXY-MIB
  – RFC3414 - SNMP-USER-BASED-SM-MIB
  – RFC3415 - SNMP-VIEW-BASED-ACM-MIB
  – RFC3418 - SNMPv2 MIB
  – and many others at various standards levels

• SNMP Co-existence – (BCP)
  – RFC3584 - SNMP-COMMUNITY-MIB
SNMP Status – SNMPv3 Features

• Comes with Modular and Extensible Architecture
• Improved SNMPv2 Operations
  – GetBulk, Inform
  – Better error Codes and Exception Codes
• Security and Access Control to MIB objects
• Remote Configuration of SNMP Engine
• Coexistence with SNMPv1 and SNMPv2c
IETF Information/Data Modeling

• We have SMI as our Data Modeling Language
  – Used to write MIB modules

• Would be good to also do an Information Model first (I.e. BEFORE we write a MIB module)
  – See RFC3444: On the Difference between Information Models and Data Models
  – We (IETF) have no consensus on a formal language to do so (or so I believe)
  – Could be done using plain English too, see RFC3290 (An Informal Management Model for Diffserv Routers) as an example.
Summary so far

- We have:
  - SNMP Messages (Snmpv3)
  - SNMP Protocol Operations (PDUs: GET, GETNEXT, GET-RESPONSE, SET, TRAPv2 INFORM) containing varBinds (MIB objects)
  - Structure of Management Information (SMIv2) used to define MIB modules
  - One MIB, composed of many MIB Modules

- MIB document defines one (or more) MIB modules.
When to define a MIB module for a protocol?

- The Internet Standard for NM is SNMPv3
- That means (a) MIB module(s) needed for devices, protocols and applications that we want to manage with SNMP
- In principle we (IETF) want all new technologies from IETF to be (SNMP) manageable
When to define a MIB module for a protocol?

• In principle that means MIB work in the technology specific WG
• At a Minimum we want monitoring and notification of faults in functionality.
• Control (write access) is often handy but not mandatory
• Configuration (write and create access) not mandatory, but fine if you want it.
MIB Module scope/content

• Specify those MIB objects that operators need/want for:
  – Monitoring
  – Control
  – Configuration
• Think first about what needs to be managed and how such managed objects can help deployment and operations.
• Probably do NOT want to specify objects for debugging protocol implementation.
• Re-use objects and Textual Conventions when possible. See:
MIB Module scope/content

- Be clear in DESCRIPTION clauses so a (new) reader/implementer can properly implement
- Be clear in DESCRIPTION clauses so all behavior is deterministic (for example persistence of writable objects)
- Add proper/good REFERENCE clauses
- Think about a good (or possibly multiple) MODULE-COMPLIANCE statement(s).
  - Allow for read-only (monitoring) compliance
  - Allow for full (monitoring/control/configuration) compliance
  - Allow for subset compliance if that makes sense.
Tools to check/review MIB modules

- Mstrip – to extract MIB
- SMICng – to compile/syntax check
  - Commercial product
- SMIIlint – to compile/syntax check etc
  - Free, plus mail service
- There are others
- [http://www.ops.ietf.org/mib-review-tools.html](http://www.ops.ietf.org/mib-review-tools.html)
Checklist items for MIB documents

- MIB Review Guidelines:
  - RFC4181
- Seems a big document (40 pages), but it has a two page step by step list of checkpoints (Appendix A)
- Rest of doc is details and clarifications
  - Good to read through before writing MIB doc
  - Then use Appendix A for checking and rest as reference and explanatory text.
Checklist items for MIB documents

1.) I-D Boilerplate
2.) Abstract
3.) MIB Boilerplate
   - www.ops.ietf.org/mib-boilerplate.html
4.) IPR notice
5.) References
6.) Security Considerations Section
   - www.ops.ietf.org/mib-security.html
Checklist items for MIB documents

• 7.) IANA Considerations Section
• 8.) Copyrights
• 9.) Other issues
• 10.) Technical content
  – Including MIB SYNTAX check (compile)
MIB doctor

- AD Selected SNMP/MIB expert
- Commits to MIB review and Mentoring
- Reviews MIB documents upon AD request or sometimes spontaneous.
  - Can do early review and help/guide
  - Always does a MIB Doctor review after WG Last Call, (preferably) before IETF Last Call
- Can function as a SNMP/MIB Advisor to a WG
MIB doctor

• In role as SNMP/MIB Advisor to WG:
  – Is not supposed to be writing the MIB document(s)
  – Is often not very familiar with the technology
  – Can help find other MIB modules/objects for re-use
  – Can help to construct proper MIB tables

• But the WG and MIB document Editor MUST:
  – do the work
  – Must be willing to translate the technology into a Data Model that can be represented in a MIB module.
  – Often that uncovers problems/issues with the protocol and/or technology specification.
MIB expertise – how to find it

• send a request to OPS AD Dan Romascanu if you need an SNMP/MIB Advisor (copy your own AD)
•Send a request to OPS AD Dan Romascanu if you have a MIB doc ready for MIB Doctor review.
  – Make sure to first check against MIB review guidelines
  – Copy your own AD
• Ask for help on ietf-mib@ops.ietf.org where you may find people with SNMP/MIB skills and interest in your protocol/technology.
How can I motivate my WG comrades to care about MIB documents?

- Once you know how to do a MIB it is FUN
- It helps to better understand your own protocol or technology
- Users (Operators) of your protocol will be happy to hear it is manageable from the start as opposed to management being an afterthought