SNMP in the IPv6 Context

Glenn Mansfield Keeni, Kazuhide Koide, Debasish Chakraborty, Norio Shiratori

Cyber Solutions Inc.
Contents

- **Introduction**
  - Network Monitoring and Multi-Protocol Issues

- **Status Survey**
  - MIB investigation

- **Solution: Development of IPv6 ready SNMP-agent**
  - Transport
  - Proxy (SNMP Proxy between IPv4/IPv6)
  - Access Control (Access Control based on IPv6-address)

- **Application: Passive Monitor**
  - Agent that Collects IPv6 Traffic Information
  - Visualization

- **Conclusion**
Issues of SNMP in IPv6 Network

Ex.) Network Monitoring Environment using SNMP polling
Issues of SNMP in IPv6 Network

P1: Transport issue
Issues of SNMP in IPv6 Network

IPv6 InOctets?

P2:MIB issue

viewer

manager
The *Multi-Protocol* Issues:

- **MIB definitions & Implementations**
  - MIB data structure supports IPv6
  - Number of IPv6 Packets, Octets
  - Metric of an IPv6 route
  
  Today: RFC under construction
  <draft-ietf-ipv6-rfc2011-update-*.txt><draft-ietf-ipv6-rfc2012-update-*.txt>
  <draft-ietf-ipv6-rfc2012-update-*.txt><draft-ietf-ipv6-rfc2096-update-*.txt>

- **Transport Definitions & Implementations**
  - Multi-protocol in transporting SNMP, proxy, access control
  - IPv4/IPv6, TCP/UDP, SNMPv1/v2/v3
  
  Today:
  RFC 3291 (Textual Conventions for Internet Network Addresses)
  Implementation: net-snmp5.0.6
Survey: MIBs using “IP Address”

- These MIBs need to update to support IPv6 (Focus on MIBs defined by RFC)

<table>
<thead>
<tr>
<th>MIB name</th>
<th>No. of OBJECTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIB-II</td>
<td>8</td>
</tr>
<tr>
<td>AppleTalk MIB</td>
<td>2</td>
</tr>
<tr>
<td>BGPv3 MIB</td>
<td>8</td>
</tr>
<tr>
<td>SNA APPN MIB</td>
<td>2</td>
</tr>
<tr>
<td>DNS Server MIB</td>
<td>3</td>
</tr>
<tr>
<td>DNS Resolver MIB</td>
<td>4</td>
</tr>
<tr>
<td>BGP4-MIB</td>
<td>11</td>
</tr>
<tr>
<td>SMDS-if MIB</td>
<td>1</td>
</tr>
<tr>
<td>RIPv2-MIB</td>
<td>4</td>
</tr>
<tr>
<td>OSPF-MIB</td>
<td>13</td>
</tr>
<tr>
<td>MIP-MIB</td>
<td>18</td>
</tr>
<tr>
<td>IP-MIB</td>
<td>3</td>
</tr>
<tr>
<td>TCP-MIB</td>
<td>2</td>
</tr>
<tr>
<td>UDP-MIB</td>
<td>1</td>
</tr>
<tr>
<td>RMON2-MIB</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MIB name</th>
<th>No. of OBJECTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP-FORWARD-MIB</td>
<td>6</td>
</tr>
<tr>
<td>IOPA-MIB</td>
<td>3</td>
</tr>
<tr>
<td>IPATM-IPMC-MIB</td>
<td>10</td>
</tr>
<tr>
<td>ATM-MIB</td>
<td>1</td>
</tr>
<tr>
<td>TN3270E-MIB</td>
<td>1</td>
</tr>
<tr>
<td>RADIUS-AUTH-CLIENT-MIB</td>
<td>1</td>
</tr>
<tr>
<td>RADIUS-AUTH-SERVER-MIB</td>
<td>1</td>
</tr>
<tr>
<td>RADIUS-ACC-CLIENT-MIB</td>
<td>1</td>
</tr>
<tr>
<td>RADIUS-ACC-SERVER-MIB</td>
<td>1</td>
</tr>
<tr>
<td>IP Tunnel MIB</td>
<td>4</td>
</tr>
<tr>
<td>DOCS-CABLE-DEVICE-MIB</td>
<td>12</td>
</tr>
<tr>
<td>DOCS-IF-MIB</td>
<td>1</td>
</tr>
<tr>
<td>VRRP-MIB</td>
<td>4</td>
</tr>
<tr>
<td>DISMAN-EXPRESSION-MIB</td>
<td>1</td>
</tr>
<tr>
<td>NOTIFICATION-LOG-MIB</td>
<td>1</td>
</tr>
<tr>
<td>DOCS-BPI-MIB</td>
<td>1</td>
</tr>
</tbody>
</table>
MIBs using “IPv6 Address”

- “IPv6Address”
  - RFC exists - Only MOs in MIB-II
  - MIB-II, Forwarding MIB are under discussion

<draft-ietf-ipv6-rfc2011-update-*.txt><draft-ietf-ipv6-rfc2012-update-*.txt>
<draft-ietf-ipv6-rfc2012-update-*.txt><draft-ietf-ipv6-rfc2096-update-*.txt>

- Not sufficient

<table>
<thead>
<tr>
<th>MIB name</th>
<th>Managed Object</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPV6-TCP-MIB</td>
<td>ipv6TcpConnLocalAddress</td>
</tr>
<tr>
<td></td>
<td>ipv6TcpConnRemAddress</td>
</tr>
<tr>
<td>IPV6-UDP-MIB</td>
<td>ipv6UdpLocalAddress</td>
</tr>
<tr>
<td>IPV6-MIB</td>
<td>ipv6AddrAddress</td>
</tr>
<tr>
<td></td>
<td>ipv6RouteDest</td>
</tr>
<tr>
<td></td>
<td>ipv6RouteNextHop</td>
</tr>
<tr>
<td></td>
<td>ipv6NetToMediaNetAddress</td>
</tr>
</tbody>
</table>
Solution: transport issues
Development of IPv6 ready SNMP-agent

- **Design of IPv6 ready SNMP-agent**
  - RFC 3291
    (Textual Conventions for Internet Network Addresses)

- **Deployment based on net-snmp-5.0pre1**
  - Transport implementation
  - Proxy implementation
  - ACL implementation
  - Merged into net-snmp(mainstream)

- The latest Ver.: net-snmp-5.0.6
  - IPv6 transport is available
Traffic Pattern of ‘snmpwalk’ in IPv4/IPv6

Equipment: FreeBSD4.6(KAME) + net-snmp5.0.6
Use of SNMP Proxy (IPv4/v6)
Use of Access control (ACL) in IPv6

IPv6 ready SNMP-agent

2001:200:1a0:ff00::/64 IPv6 Network

2001:200:1a0:ff01::/64 IPv6 Network

2001:200:1a0:ff00::/64

Segment A (Allowed Network)

2001:200:1a0:ff01::/64

Segment B (Denied Network)

# sec.name source community
con2sec mynetwork 2001:200:1a0:ff00::/64 RI GHT
Current status

<table>
<thead>
<tr>
<th>Current status</th>
<th>Our Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP transport over IPv6</td>
<td></td>
</tr>
<tr>
<td>IPv4 and IPv6 Transport Proxy</td>
<td></td>
</tr>
<tr>
<td>Access Control based on IPv6 Address</td>
<td></td>
</tr>
<tr>
<td>USM Authentication in IPv6 Environment</td>
<td></td>
</tr>
<tr>
<td>USM Authentication/Privacy in IPv6 Environment</td>
<td></td>
</tr>
<tr>
<td>VACM in IPv6 Environment</td>
<td></td>
</tr>
</tbody>
</table>
Application: IPv6 Network Monitoring

- In many existing IPv6 network:
  - SNMP-functions of Equipments: insufficient

- Monitoring of IPv6 Network or Traffic by SNMP:
  - Difficult

Proposal

RMON-type(add-on) passive monitoring agent
Passive Monitoring

- Strategy of Network Monitoring
- Sniffing link using Tapping Kit (Ex. RMON)

- Merits:
  - Do NOT affect to Network Operation
  - Capability to access details in each packet
    - Capable of getting ANY(IPv4/IPv6) information
    - Also capable of getting Application-layer Information

`Managing Equipment (Router, Host, Network)`

`Agent`

`Tapping Kit`  `Passive Monitor`
Multi-Protocol Passive Monitor

Feature:

- Any kind of Info. about packets
  - {Packets, Octets}
  - {IPv4, IPv6}
  - {TCP, UDP, ICMP}
  - {Application wise..}
  - {VLAN1, VLAN2,..}
- Information provision in MIBs
  - Remote Monitoring
- Multi-protocol Transport
  - SNMP over IPv4/v6
  - SNMP v1/v2c/v3
Designing

- **Probe - Backend**
  - Collecting Information of every packets
  - pcap, filtering

- **SNMP agent - Frontend**
  - Information Provision in MIB form
    - Programmable MIB
  - Multi-protocol Transport

**Implementation:**

`pcap + net-snmp + new MIB`
Agent(1-box)
Agent(Tapping Kit(100baseTX) + PC)
Tapping Kit(1000base-SX)
Experiment

- Environment: JGN-IPv6 (IPv6 test-bed)
  - From Nov. 2001
  - TOHOKU-HOKKAIDO NOC in Tohoku Univ.
    - 6-sites are connected
Environment: JGN-IPv6 Tohoku-NOC

- **JGN-IPv6**
- **IPv4 cloud**

**CISCO 7206**
- Summit 24 (3ffe:516:3010::/64)
- IPv6Router

**IPv4 cloud**
- v4Router
- v6Router

**agent1**
- manager
- 130.34.38.128/26
- 3ffe:516:3010:10::/64

**agent2**
- 192.168.0.0/24
- 3ffe:516:3005::/64

**agent3**
- :Tap Kit

Locations:
- Iwamizawa
- Sapporo
- Hachinohe
- Iwate
- Sendai
- Aizu

**IPv4-cloud**
- 130.34.38.128/26
- 3ffe:516:3010:10::/64

**IPv4-router**
- 192.168.0.0/24
- 3ffe:516:3005::/64

**IPv6-router**
- 3ffe:516:3010::/64

**IPv6-router**
- 3ffe:516:3005::/64

**IPv4-router**
- 130.34.38.128/26
- 3ffe:516:3010:10::/64

**IPv6-router**
- 192.168.0.0/24
- 3ffe:516:3005::/64
Visualization

- 2002/Nov./9 JGN Symposium (MPEG traffic, Video Conference)
Conclusion

Status Survey:
MIB Investigation

Solutions:
Transport: Design and Implementation of IPv6 transport SNMP-agent
Proxy: Ready - IPv6 SNMP Proxy
ACL: Ready - IPv6 Access Control

Application:
*Multi-protocol Passive Monitor*
Capability to Monitor *ANY* Network

Status:
*Prototype operation*
at JGN-IPv6 Tohoku-Hokkaido NOC
Future Works

- Implementation of IPv6-ready MIBs

- “Programmable Monitoring”
  - Using
    - “Light-weight Multi-Protocol Passive Monitor”
      - “Very Light RMON”
    - Easy Use
  - For IPv6 Monitoring
Appendix A.

Definition of SNMP over UDP/IPv4

- Definition of TRANSPORT

```{-- SNMPv2 over UDP over IPv4
snmpUDPDoman OBJECT-IDENTITY
  STATUS current
  DESCRIPTION
  “The SNMPv2 over UDP transport domain. The corresponding
  transport address is of the type SNMPUDPAddress.”
  ::= { snmpDomains 1}
SnmpUDPAddress ::= TEXTUAL-CONVENTION
  DISPLAY-HINT “1d.1d.1d.1d/2d”
  STATUS current
  DESCRIPTION
  “Represents a UDP address:
  octets contents encoding
  1-4 IP-address network-byte order
  5-6 UDP-port network-byte order
  ”

SYNTAX OCTET STRING (SIZE(6))
```

J. Case, K. McCloghrie, M. Rose, S. Waldbusser, RFC1906,
(SNMPv2)
Appendix B.

Definition of SNMP over UDP/IPv6

- Definition of TRANSPORT in IPv6 network

```
transportDomainUdpIpv6 OBJECT IDENTITY
  STATUS        current
  DESCRIPTION   "The UDP over IPv6 transport domain. The corresponding
                transport address is of type TransportAddressIPv6."
  ::= { transportDomains 2 }

TransportAddressIPv6 ::= TEXTUAL-CONVENTION
  DISPLAY-HINT  "0a[2x:2x:2x:2x:2x:2x:2x:2x]0a:2d"
  STATUS        current
  DESCRIPTION   "Represents a UDP/TCP/SCTP over IPv6 transport address:
                octets   contents   encoding
                1-16      IPv6 address network-byte order
                17-18     port number network-byte order

This textual convention SHOULD NOT be used directly in object
definitions since it restricts addresses to a specific format.
However, if it is used, it MAY be used either on its own or
in conjunction with TransportAddressType or TransportDomain
as a pair."
  SYNTAX        OCTET STRING (SIZE (18))
```

M. Daniele, J. Schoenwaelder, Textual Conventions for Transport Address,
draft-ietf-ops-taddress-mib-02.txt
Appendix C.

snmpd.conf for proxy

# proxy to SNMP over IPv6 agent
proxy -v1 -c COMMUNITY 2001:200:1a0:ff00::ffff .enterprise.73.15.1.1
proxy -v2c -c COMMUNITY 2001:200:1a0:ff00::ffff .enterprise.73.15.2.1
proxy -v3 -u user -l authNoPriv -a MD5 -A AUTHPASS 2001:200:1a0:ff00::ffff .enterprise.73.15.3.1
proxy -v3 -u user -l authPriv -a MD5 -A AUTHPASS -x DES -X PRIVPASS 2001:200:1a0:ff00::ffff .enterprise.73.15.4.1

# proxy to SNMP over IPv4 agent
proxy -v1 -c COMMUNITY 192.168.0.254 .enterprise.73.14.1.1
proxy -v2c -c COMMUNITY 192.168.0.254 .enterprise.73.14.2.1
proxy -v3 -u user -l authNoPriv -a MD5 -A AUTHPASS 192.168.0.254 .enterprise.73.14.3.1
proxy -v3 -u user -l authPriv -a MD5 -A AUTHPASS -x DES -X PRIVPASS 192.168.0.254 .enterprise.73.14.4.1
Appendix D.
Programmable MIB

```plaintext
# cpMonitorBE.conf
preprocessor CGpMonitor: 22 23 80 161 162
```