Network Working Group
Internet Draft
Expires January 2001

K. Chan
J. Seligson
Nortel Networks
K. McCloghrie
M. Fine
Cisco Systems
S. Hahn
Intel
A. Smith
No Affiliation
F. Reichmeyer
IP Highway

14 July 2000

The Policy Device Auxiliary MIB

draft-ietf-rap-pol-aux-mib-00.txt

Status of this Memo

Distribution of this document is unlimited. Please send comments to the Resource Allocation Protocol (RAP) Working Group at rap@iphighway.com.

1. Introduction

This memo defines a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. In particular, it describes managed objects used for managing Policy Client devices, including the relationship between device interfaces and policy role combinations. Policy role combinations are used as part of the data model for policy information when a Policy Client is provisioned using the COPS protocol [COPS-PR] and a Policy Information Base (PIB) [FRAMEPIB].

2. The SNMP Network Management Framework

The SNMP Management Framework presently consists of five major components:

- An overall architecture, described in RFC 2571 [RFC2571].

- Mechanisms for describing and naming objects and events for the purpose of management. The first version of this Structure of Management Information (SMI) is called SMIv1 and described in STD 16/RFC 1155 [RFC1155], STD 16/RFC 1212 [RFC1212] and RFC 1215 [RFC1215]. The second version, called SMIv2, is described in STD 58, which consists of RFC 2578 [RFC2578], RFC 2579 [RFC2579] and RFC 2580 [RFC2580].

- Message protocols for transferring management information. The first version of the SNMP message protocol is called SNMPv1 and described in STD 15/RFC 1157 [RFC1157]. A second version of the SNMP message protocol, which is not an Internet standards track protocol, is called SNMPv2c and described in RFC 1901 [RFC1901] and RFC 1906 [RFC1906]. The third version of the message protocol is called SNMPv3 and described in RFC 1906 [RFC1906], RFC 2572 [RFC2572] and RFC 2574 [RFC2574].

- Protocol operations for accessing management information. The first set of protocol operations and associated PDU formats is described in STD 15/RFC 1157 [RFC1157]. A second set of protocol operations and associated PDU formats is described in RFC 1905 [RFC1905].

- A set of fundamental applications described in RFC 2573 [RFC2573] and the view-based access control mechanism described in RFC 2575 [RFC2575].

A more detailed introduction to the current SNMP Management Framework can be found in RFC 2570 [RFC2570].

Managed objects are accessed via a virtual information store, termed the Management Information Base or MIB. Objects in the MIB are defined using the mechanisms defined in the SMI.

This memo specifies a MIB module that is compliant to the SMIv2. A MIB conforming to the SMIv1 can be produced through the appropriate translations. The resulting translated MIB must be semantically equivalent, except where objects or events are omitted because no translation is possible (e.g., use of Counter64). Some machine readable information in SMIv2 will be converted into textual descriptions in SMIv1 during the translation process. However, this loss of machine readable information is not considered to change the semantics of the MIB.

3. Role Combinations for Interfaces

Policy is being defined using the concept of "roles" [COREMODEL]. A first application of roles is to assign one or more roles to each interface on a network device. The combination of all roles assigned to an interface is termed a "role combination". The Framework PIB [FRAMEPIB] uses role combinations as the means to specify policy information which applies to multiple interfaces. Each Policy Client/Policy Enforce Point (PEP) notifies the Policy Server/Policy Decision Point (PDP) of the role combinations for which it needs policy. It is the PEP which locally resolves the relationship between role combinations and its local interfaces. The relationship of role combination to interface is a one-to-many association, i.e, many interfaces can have the same role combination, but each interface has one and only one role combination.

The Policy Interface Table defined in this MIB can be used to configure each interface of a PEP with its role combination. The whole role combination is modified rather than individual roles within the role combination to avoid race conditions if and when multiple managers were updating the values at the same time. The table can also be read to determine which interfaces are configured with a particular role combination. This allows information available on a per-interface basis to be aggregated and compared to information available on a per-role combination basis. Such comparisons can be useful for trouble-shooting the effectivesness of policies, for aggregate statistics and/or for accounting purposes.

4. Policy Device Auxiliary MIB Definitions

```
POLICY-DEVICE-AUX-MIB DEFINITIONS ::= BEGIN


IMPORTS
        MODULE-IDENTITY, OBJECT-TYPE, experimental
                                            FROM SNMPv2-SMI
        MODULE-COMPLIANCE, OBJECT-GROUP     FROM SNMPv2-CONF
        TEXTUAL-CONVENTION, RowStatus, StorageType
                                            FROM SNMPv2-TC
        SnmpAdminString                     FROM SNMP-FRAMEWORK-MIB
        InterfaceIndex                      FROM IF-MIB;


policyDeviceAuxMib MODULE-IDENTITY
        LAST-UPDATED    "200007121800Z" -- 12 July 2000
        ORGANIZATION    "IETF RAP WG"
        CONTACT-INFO
                "Kwok Ho Chan
                 Nortel Networks, Inc.
                 600 Technology Park Drive
                 Billerica, MA 01821 USA
                 Phone: +1 978 288 8175
                 Email: khchan@nortelnetworks.com

                 John Seligson
                 Nortel Networks, Inc.
                 4401 Great America Parkway
                 Santa Clara, CA USA 95054
                 Phone: +1 408 495-2992
                 Email: jseligso@nortelnetworks.com

                 Keith McCloghrie
                 Cisco Systems, Inc.
                 170 West Tasman Drive,
                 San Jose, CA 95134-1706 USA
                 Phone: +1 408 526 5260
                 Email: kzm@cisco.com"
        DESCRIPTION
            "This module defines an infrastructure used
            for support of policy-based provisioning of
            a network device."
        ::= { experimental 999 }
```

```
policyDeviceAuxObjects     OBJECT IDENTIFIER ::= { policyDeviceAuxMib 1 }
policyDeviceAuxConformance OBJECT IDENTIFIER ::= { policyDeviceAuxMib 2 }


policyDeviceConfig    OBJECT IDENTIFIER ::= { policyDeviceAuxObjects 1 }

Role ::= TEXTUAL-CONVENTION
    STATUS       current
    DESCRIPTION
        "A role represents a functionality characteristic or
        capability of a resource to which policies are applied.
        Examples of roles include Backbone interface, Frame Relay
        interface, BGP-capable router, web server, firewall, etc.

        Valid characters are a-z, A-Z, 0-9, period, hyphen and
        underscore.  A role must not start with an underscore."
    REFERENCE
        "Policy Core Information Model,
        draft-ietf-policy-core-info-model-06.txt"
    SYNTAX SnmpAdminString  (SIZE (1..31))

RoleCombination ::= TEXTUAL-CONVENTION
    STATUS       current
    DESCRIPTION
        "A Display string consisting of a set of roles concatenated
        with a '+' character where the roles are in lexicographic
        order from minimum to maximum.

        For example, a+b and b+a are NOT different role-combinations;
        rather, they are different formating of the same (one) role-
        combination.

        Notice the roles within a role-combination are in lexicographic
        order from minimum to maximum, hence, we declare:
          a+b is the valid formating of the role-combination,
          b+a is an invalid formating of the role-combination.

        Notice the need of zero-length role-combination as the role-
        combination of interfaces to which no roles have been assigned.
        This role-combination is also known as the null role-combination.
        (Note the deliberate use of lower case leters to avoid confusion
        with the ASCII NULL character which has a value of zero but length
        of one.)"
    SYNTAX SnmpAdminString  (SIZE (0..255))
```

```
-- The Policy Interface Table supports
-- associating an interface with a specific role combination.

-- This table satisfy the need to monitor the configuration of
-- roles on a per interface basis, and is no less scalable as
-- other required per interface parameters.
-- This does not preclude roles being associated with some less
-- granular entities, and should be addressed when such need arise.

policyInterfaceTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF PolicyInterfaceEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Policy information about a device's interfaces."
    ::= { policyDeviceConfig 1 }


policyInterfaceEntry OBJECT-TYPE
    SYNTAX      PolicyInterfaceEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "A conceptual row in the policyInterfaceTable.
            Each row identifies policy infromation about a
            particular interface."
    INDEX { policyInterfaceIfIndex }
    ::= { policyInterfaceTable 1 }


PolicyInterfaceEntry ::= SEQUENCE {
    policyInterfaceIfIndex    InterfaceIndex,
    policyInterfaceRoleCombo  RoleCombination,
    policyInterfaceStorage    StorageType,
    policyInterfaceStatus     RowStatus
}


policyInterfaceIfIndex OBJECT-TYPE
    SYNTAX      InterfaceIndex
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The ifIndex value for which this conceptual row provides
            policy information."
```

```
    ::= { policyInterfaceEntry 1 }


policyInterfaceRoleCombo OBJECT-TYPE
    SYNTAX      RoleCombination
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The role combination that is associated with this interface
            for the purpose of assigning policies to this interface."
    ::= { policyInterfaceEntry 2 }


policyInterfaceStorage OBJECT-TYPE
    SYNTAX      StorageType
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The storage type for this conceptual row.


            Conceptual rows having the value permanent(4) need not
            allow write-access to any columnar objects in the row.


            This object may not be modified if the associated
            policyInterfaceStatus object is equal to active(1)."
    DEFVAL  { volatile }
    ::= { policyInterfaceEntry 3 }


policyInterfaceStatus OBJECT-TYPE
    SYNTAX      RowStatus
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The status of this row.


            An entry may not exist in the active state unless all
            objects in the entry have an appropriate value. Row
            creation using only default values is supported."
    ::= { policyInterfaceEntry 4 }
```

```
--
-- Conformance Section
--


policyDeviceCompliances
                   OBJECT IDENTIFIER ::= { policyDeviceAuxConformance 1 }
policyDeviceGroups OBJECT IDENTIFIER ::= { policyDeviceAuxConformance 2 }


policyDeviceCompliance MODULE-COMPLIANCE
    STATUS  current
    DESCRIPTION
            "Describes the requirements for conformance to the
            Policy  Auxiliary MIB."


    MODULE  -- this module
        MANDATORY-GROUPS { policyInterfaceGroup }


        OBJECT        policyInterfaceRoleCombo
        MIN-ACCESS    read-only
        DESCRIPTION  "Write access is not required."


        OBJECT        policyInterfaceStorage
        MIN-ACCESS    read-only
        DESCRIPTION  "Write access is not required, nor is
                      support for the nonVolatile(2) enumeration."


        OBJECT        policyInterfaceStatus
        MIN-ACCESS    read-only
        DESCRIPTION  "Write access is not required."
    ::= { policyDeviceCompliances 1 }


policyInterfaceGroup OBJECT-GROUP
    OBJECTS {
             policyInterfaceRoleCombo,
             policyInterfaceStorage,
             policyInterfaceStatus
    }
    STATUS  current
```

```
    DESCRIPTION
            "Objects used to define interface to role combination
             mappings."
    ::= { policyDeviceGroups 1 }

END
```

5. References

[RFC2026] S. Bradner, "The Internet Standards Process -- Revision 3", RFC 2026, October 1996.

[RFC2571] Harrington, D., Presuhn, R., and B. Wijnen, "An Architecture for Describing SNMP Management Frameworks", RFC 2571, April 1999.

[RFC1155] Rose, M., and K. McCloghrie, "Structure and Identification of Management Information for TCP/IP-based Internets", STD 16, RFC 1155, May 1990.

[RFC1212] Rose, M., and K. McCloghrie, "Concise MIB Definitions", STD 16, RFC 1212, March 1991.

[RFC1215] M. Rose, "A Convention for Defining Traps for use with the SNMP", RFC 1215, March 1991.

[RFC2578] McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., and S. Waldbusser, "Structure of Management Information Version 2 (SMIv2)", STD 58, RFC 2578, April 1999.

[RFC2579] McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., and S. Waldbusser, "Textual Conventions for SMIv2", STD 58, RFC 2579, April 1999.

[RFC2580] McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., and S. Waldbusser, "Conformance Statements for SMIv2", STD 58, RFC 2580, April 1999.

[RFC1157] Case, J., Fedor, M., Schoffstall, M., and J. Davin, "Simple Network Management Protocol", STD 15, RFC 1157, May 1990.

[RFC1901] Case, J., McCloghrie, K., Rose, M., and S. Waldbusser, "Introduction to Community-based SNMPv2", RFC 1901, January 1996.

[RFC1906] Case, J., McCloghrie, K., Rose, M., and S. Waldbusser, "Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)", RFC 1906, January 1996.

[RFC2572] Case, J., Harrington D., Presuhn R., and B. Wijnen, "Message Processing and Dispatching for the Simple Network Management

Protocol (SNMP)", RFC 2572, April 1999.

[RFC2574] Blumenthal, U., and B. Wijnen, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)", RFC 2574, April 1999.

[RFC1905] Case, J., McCloghrie, K., Rose, M., and S. Waldbusser, "Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)", RFC 1905, January 1996.

[RFC2573] Levi, D., Meyer, P., and B. Stewart, "SNMPv3 Applications", RFC 2573, April 1999.

[RFC2575] Wijnen, B., Presuhn, R., and K. McCloghrie, "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)", RFC 2575, April 1999.

[RFC2570] Case, J., Mundy, R., Partain, D., and B. Stewart, "Introduction to Version 3 of the Internet-standard Network Management Framework", RFC 2570, April 1999.

[COPS-PR] Reichmeyer, F., Herzog, S., Chan, K., Durham, D., Yavatkar, R. Gai, S., McCloghrie, K. and A. Smith, "COPS Usage for Policy Provisioning" Internet Draft, draft-ietf-rap-cops-pr-03.txt, July 2000.

[FRAMEPIB] Fine, M., McCloghrie, K., Seligson, J., Chan, K., Hahn, S., Smith, A., and F. Reichmeyer, "Framework Policy Information Base", Internet Draft, draft-ietf-rap-frameworkpib-01.txt, July 2000.

[COREMODEL] Moore, B., Ellesson, E., and J. Strassner, "Policy Framework Core Information Model -- Version 1 Specification", Internet Draft, draft-ietf-policy-core-info-model-06.txt, May 2000.

6. Authors' Addresses

Kwok Ho Chan
Nortel Networks, Inc.
600 Technology Park Drive
Billerica, MA 01821 USA
Phone: +1 978 288 8175
Email: khchan@nortelnetworks.com

John Seligson

Nortel Networks, Inc.
4401 Great America Parkway
Santa Clara, CA 95054 USA
Phone: +1 408 495 2992
Email: jseligso@nortelnetworks.com

Keith McCloghrie
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706 USA
Phone: +1 408 526 5260
Email: kzm@cisco.com

Michael Fine
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706 USA
Phone: +1 408 527 8218
Email: mfine@cisco.com

Scott Hahn
Intel
2111 NE 25th Avenue
Hillsboro, OR 97124 USA
Phone: +1 503 264 8231
Email: scott.hahn@intel.com

Andrew Smith
Fax: +1 415 345 1827
Email: ah_smith@pacbell.net

Francis Reichmeyer
IPHighway, Inc.
55 New York Avenue
Framingham, MA 01701 USA
Phone: +1 201 665 8714
Email: franr@iphighway.com

7. Security Considerations

There are a number of management objects defined in this MIB that have a MAX-ACCESS clause of read-write and/or read-create. Such objects may be considered sensitive or vulnerable in some network environments. The support for SET operations in a non-secure environment without proper protection can have a negative effect on network operations.

In particular, write-able objects allow an administrator to control the interfaces, and unauthorized access to these could cause a denial of service, or in combination with other (e.g., physical) security breaches, could cause unauthorized connectivity to a device.

SNMPv1 by itself is not a secure environment. Even if the network itself is secure (for example by using IPSec), even then, there is no control as to who on the secure network is allowed to access and GET/SET (read/change/create/delete) the objects in this MIB.

It is recommended that the implementers consider the security features as provided by the SNMPv3 framework. Specifically, the use of the User-based Security Model RFC 2574 [RFC2574] and the View- based Access Control Model RFC 2575 [RFC2575] is recommended.

It is then a customer/user responsibility to ensure that the SNMP entity giving access to an instance of this MIB, is properly configured to give access to the objects only to those principals (users) that have legitimate rights to indeed GET or SET (change/create/delete) them.

8. Notice on Intellectual Property

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

9. Full Copyright Statement