Elwin Eliazer (Corona)
Samuel Hancock (Corona)

Internet Draft
Expiration Date: August 2002

February 2002

IP Services Management Information Base Using SMIv2

draft-elwin-ipservices-mib-00.txt

1.0 Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet- Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at:
http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at:
http://www.ietf.org/shadow.html.

2.0 Abstract

This memo defines a portion of the Management Information Base (MIB) for use with network management protocols in TCP/IP based internets. In particular, it defines objects for managing networks using IP Service Profiles.

3.0 Table of Contents

4.0 Terminologies

IP Service Profile
An IP Service Profile contain the rules and specific configuration information for an IPSec, IP Qos, or Firewall services.

5.0 Introduction

This MIB is designed to help administrators to provision their IP Services by using a uniform mechanism.

6.0 The SNMP Network Management Framework

The SNMP Management Framework presently consists of five major components:

- An overall architecture, described in RFC 2571 [1].
- 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 [2], STD 16, RFC 1212 [3] and RFC 1215 [4]. The second version, called SMIv2, is described in STD 58, which consists of RFC 2578 [5], RFC 2579 [6] and RFC 2580 [7].
- Message protocols for transferring management information. The first version of the SNMP message protocol is called SNMPv1 and described in STD 15, RFC 1157 [8]. A second version of the SNMP message protocol, which is not an Internet standards track protocol, is called SNMPv2c and described in RFC 1901 [9] and RFC 1906 [10]. The third version of the message protocol is called SNMPv3 and described in RFC 1906 [10], RFC 2572 [11] and RFC 2574 [12].
- Protocol operations for accessing management information. The first set of protocol operations and associated PDU formats is

described in STD 15, RFC 1157 [8]. A second set of protocol operations and associated PDU formats is described in RFC 1905

[13].

- o A set of fundamental applications described in RFC 2573 [14] and the view-based access control mechanism described in RFC 2575 [15].

A more detailed introduction to the current SNMP Management Framework can be found in RFC 2570 [22].

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.

7.0 Overview of the IP-SERVICES-MIB

The ipServicesIfTable provides a uniform mechanism for attaching IP Services Profiles to the interfaces. This is achieved specifying the profile name for the appropriate interface.

To enable and disable the an IP Service Profile for the interface, use the ipServicesIfSecurityEnabled, ipServicesIfQosEnabled, or ipServicesIfFirewallEnabled objects. By default the values of these objects are false(2), meaning the profile is not enabled.

8.0 Sample IP Services MIB Configuration Scenario

To attach an IPSec Profile named "ipsec-phoenix1" on ipServicesIfIfIndex=2.

```
    SetRequest {
        ipServicesIfSecurityProfile.2     "ipsec-phoenix1"
    }
```

To enable the IPSec Profile on ipServicesIfIfIndex=2,

```
    SetRequest {
```

```
        ipServicesIfSecurityEnabled.2     true(1)
    }
```

To disable the IPSec Profile on ipServicesIfIfIndex=2,

```
    SetRequest {
        ipServicesIfSecurityEnabled.2     false(2)
    }
```

9.0 Definition of the IP Services MIB

```
-- ************************************************************
-- ipServicesMIB.mib
-- ************************************************************

IP-SERVICES-MIB DEFINITIONS ::= BEGIN

    IMPORTS
        experimental, Unsigned32,
        MODULE-IDENTITY, OBJECT-TYPE
            FROM SNMPv2-SMI
        TruthValue, DisplayString
            FROM SNMPv2-TC
        MODULE-COMPLIANCE, OBJECT-GROUP
            FROM SNMPv2-CONF
        InterfaceIndex
            FROM IF-MIB;

    ipServicesMIB MODULE-IDENTITY
        LAST-UPDATED "0202211200Z"
        ORGANIZATION
            "Corona Networks, Inc."
        CONTACT-INFO
            "Corona Networks, Inc.
            630 Alder Drive
            Milpitas, CA  95035
            USA

            Tel: +1 408 519 3800
            Fax: +1 408 519 3830
            Email:  sam@coronanetworks.com
                    elwinietf@yahoo.com"
        DESCRIPTION
            "The MIB is the definition of the managed objects for
            the managing the IP Services Profiles for an Interface."
        REVISION "0202211200Z"
        DESCRIPTION
            "Initial Revision."
        ::= { experimental 12345 }   -- To be assigned
```

--

```
-- Managed objects
--
    ipServicesMIBObjects OBJECT IDENTIFIER ::= { ipServicesMIB 1 }

    ipServicesIfTable OBJECT-TYPE
        SYNTAX SEQUENCE OF IpServicesIfEntry
        MAX-ACCESS not-accessible
        STATUS current
        DESCRIPTION
            "The table is used to map ip services to the appropriate
            interfaces."
        ::= { ipServicesMIBObjects 1 }

    ipServicesIfEntry OBJECT-TYPE
        SYNTAX IpServicesIfEntry
        MAX-ACCESS not-accessible
        STATUS current
        DESCRIPTION
            "An entry in this table binds the IP Service Profiles
            to an interface.

            Interfaces are specified in ifTable from the IF-MIB."
        INDEX { ipServicesIfIfIndex }
        ::= { ipServicesIfTable 1 }

    IpServicesIfEntry ::=
        SEQUENCE {
            ipServicesIfIfIndex             InterfaceIndex,
            ipServicesIfSecurityProfile     DisplayString,
            ipServicesIfSecurityEnabled     TruthValue,
            ipServicesIfQosProfile          DisplayString,
            ipServicesIfQosEnabled          TruthValue,
            ipServicesIfFirewallInProfile   DisplayString,
            ipServicesIfFirewallOutProfile  DisplayString,
            ipServicesIfFirewallEnabled     TruthValue
         }

    ipServicesIfIfIndex OBJECT-TYPE
        SYNTAX InterfaceIndex
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
            "This object is used to identify the interface to map
            the IP service profiles."
        ::= { ipServicesIfEntry 1 }

    ipServicesIfSecurityProfile OBJECT-TYPE
```

```
        SYNTAX DisplayString
        MAX-ACCESS read-write
        STATUS current
```

```
        DESCRIPTION
            "This object is used to specify the ip security (IPSec)
            profile to use for the interface.

            If no value is specified, '0' indicates that an IPSec
            profile has not been applied to this interface."
        ::= { ipServicesIfEntry 2 }

    ipServicesIfSecurityEnabled OBJECT-TYPE
        SYNTAX TruthValue
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
            "This object is used to enable and disable the IPSec
            profile to use on the interface."
        DEFVAL { false }
        ::= { ipServicesIfEntry 3 }

    ipServicesIfQosProfile OBJECT-TYPE
        SYNTAX DisplayString
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
            "This object is used to specify the IP QoS (DSCP)
            profile to use for the interface.

            If no value is specified, '0' indicates that a
            ip qos profile has not been applied to this interface."
        ::= { ipServicesIfEntry 4 }

    ipServicesIfQosEnabled OBJECT-TYPE
        SYNTAX TruthValue
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
            "This object is used to enable and disable the IP
            QoS profile to use on the interface."
        DEFVAL { false }
        ::= { ipServicesIfEntry 5 }

    ipServicesIfFirewallInProfile OBJECT-TYPE
        SYNTAX DisplayString
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
            "This object is used to specify the firewall profile
            to use for the interface.
```

```
            If no value is specified, '0' indicates that a
            profile has not been applied to this interface."
```

```
        ::= { ipServicesIfEntry 6 }

    ipServicesIfFirewallOutProfile OBJECT-TYPE
        SYNTAX DisplayString
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
            "This object is used to specify the firewall profile
            to use for the interface.

            If no value is specified, '0' indicates that a
            profile has not been applied to this interface."
        ::= { ipServicesIfEntry 7 }

    ipServicesIfFirewallEnabled OBJECT-TYPE
        SYNTAX TruthValue
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
            "This object is used to enable and disable the
            firewall on the interface."
        DEFVAL { false }
        ::= { ipServicesIfEntry 8 }

--
-- Conformance information
--

    ipServicesConformance OBJECT IDENTIFIER ::=
                                { ipServicesMIB 3 }

    ipServicesCompliances OBJECT IDENTIFIER ::=
                                { ipServicesConformance 1 }

    ipServicesGroups OBJECT IDENTIFIER ::=
                                { ipServicesConformance 2 }

    ipServicesCompliance MODULE-COMPLIANCE
        STATUS current
        DESCRIPTION
            "The compliance statement for SNMPv2 entities which
            implement the IP Services MIB."
        MODULE -- this module
        MANDATORY-GROUPS { ipServicesIfGroup }
        ::= { ipServicesCompliances 1 }

    ipServicesIfGroup OBJECT-GROUP
        OBJECTS {   ipServicesIfIfIndex,
```

```
                    ipServicesIfSecurityProfile,
                    ipServicesIfSecurityEnabled,
```

```
                    ipServicesIfQosProfile,
                    ipServicesIfQosEnabled,
                    ipServicesIfFirewallInProfile,
                    ipServicesIfFirewallOutProfile,
                    ipServicesIfFirewallEnabled }
        STATUS current
        DESCRIPTION
            "A collection of objects providing configuration
            information of the IP Services."
        ::= { ipServicesGroups 1 }

END


--
-- IP-SERVICES-MIB.mib
--
```

10.0 Security Considerations

TBD

11.0 Acknowledgments

TBD

12.0 References

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

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

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

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

[5] 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.

[6] McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose,

M. and S. Waldbusser, "Textual Conventions for SMIv2", STD 58, RFC 2579, April 1999.

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

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

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

[10] 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

[15] Wijnen, B., Presuhn, R. and K. McCloghrie, "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)", RFC 2575, January 1998.

[16] Bradner, S., "Key words for use in RFCs to Indicate Requirements Levels", BCP 14, RFC 2119, March 1997.

13.0 Authors' Addresses

Elwin Stelzer Eliazer
Corona Networks, Inc.
630 Alder Drive
Milpitas, CA 95035
Phone: 408-519-3832
Email: elwinietf@yahoo.com

Samuel Hancock
Corona Networks, Inc.
630 Alder Drive
Milpitas, CA 95035
Phone: 408-519-3800 Ext 421
Email: sam@coronanetworks.com