Internet-Draft
draft-ietf-ipcdn-cable-gateway-security-mib-00.txt
Expires: December 2003

E. Cardona
K. Luehrs
CableLabs

S. Higgins
Ashley-Laurent

D. Jones
YAS BBV
June 2003

Cable Gateway Security Management Information Base for CableHome compliant Residential Gateways

Status of this Memo

Copyright Notice

Abstract

This memo defines a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. In particular, it defines a basic set of managed objects for SNMP-based security management of CableHome 1.0 compliant residential gateway devices.

This memo specifies a MIB module in a manner that is compliant to the SNMP SMIv2 [5][6][7]. The set of objects is consistent with the SNMP framework and existing SNMP standards.

Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119 [2].

Table of Contents

1. The Internet-Standard Management Framework

For a detailed overview of the documents that describe the current Internet-Standard Management Framework, please refer to section 7 of RFC 3410 [12].

Managed objects are accessed via a virtual information store, termed the Management Information Base or MIB. MIB objects are generally

accessed through the Simple Network Management Protocol (SNMP). Objects in the MIB are defined using the mechanisms defined in the Structure of Management Information (SMI). This memo specifies a MIB module that is compliant to the SMIv2, which is described in STD 58, RFC 2578 [7], STD 58, RFC 2579 [8] and STD 58, RFC 2580 [9].

2. Glossary

The terms in this document are derived either from normal cable system usage, from normal residential gateway operation, or from the documents associated with the CableHome Specifications [21].

2.1 CableHome Residential Gateway

A CableHome Residential gateway passes data traffic between the cable operator's broadband data network (the Wide Area Network, WAN) and the Local Area Network (LAN) in the cable data service subscriber's residence or business. In addition to passing traffic between the WAN and LAN, the CableHome Residential Gateway provides several services including a DHCP client and a DHCP server (RFC2131) [22], a TFTP server (RFC1350) [23], management services as enabled by SNMPv1/v2c/v3 agent compliant with the RFCs listed in Section 1, and security services including stateful packet inspection firewall functionality and software code image verification using techniques.

2.2 Portal Services

A logical element aggregating the set of CableHome-specified functionality in a CableHome compliant cable gateway device.

2.3 LAN IP Device

A LAN IP Device is representative of a typical IP device expected to reside on home networks, and is assumed to contain a TCP/IP stack as well as a DHCP client.

2.4 WAN Management (WAN-Man) Address

WAN Management Addresses are intended for network management traffic on the cable network between the network management system and the PS element. Typically, these addresses will reside in private IP address space.

2.5 WAN Data (WAN-Data) Address

WAN Data Addresses are intended for subscriber application traffic on the cable network and beyond, such as traffic between LAN IP Devices

and Internet hosts. Typically, these addresses will reside in public IP address space.

2.6 LAN Translated (LAN-Trans) Address

LAN Translated Addresses are intended for subscriber application and management traffic on the home network between LAN IP Devices and the PS element. Typically, these addresses will reside in private IP address space, and can typically be reused across subscribers.

2.7 LAN Passthrough (LAN-Pass) Address

LAN Passthrough Addresses are intended for subscriber application traffic, such as traffic between LAN IP Devices and Internet hosts, on the home network, the cable network, and beyond. Typically, these addresses will reside in public IP address space.

2.8 Cable Gateway DHCP Portal (CDP)

A logical element residing within the PS that encapsulates DHCP functionality within a Cable Gateway Device. This includes both DHCP client as well as DHCP server capabilities.

2.9 Denial of Service

A type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic.

2.10 Firewall

A system designed to prevent unauthorized access to or from a private network. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet.

2.11 Hash

A hash value (or simply hash) is a number generated from a string of text. The hash is substantially smaller than the text itself, and is generated by a formula in such a way that it is extremely unlikely that some other text will produce the same hash value. Hashes play a role in security systems where they're used to ensure that transmitted messages have not been tampered with.

2.12 Rule Set

The rule set is derived from the security policy and defines the collection of access control rules (filter and proxy action rules) which then determines which packets the firewall forwards and which it rejects.

2.13 Security Policy

The security policy defines the desired level of security/functionality for a subscriber's firewall.

3. Overview

This MIB provides a set of security objects required for the management of CableHome compliant residential gateway devices. The specification is derived from the CableHome 1.0 specification [21].

3.1 Structure of the MIB

This MIB is structured into two groups:

û cabhSecFwObjects is used to manage the firewall functionality.

û cabhSecCertObjects is used to hold the gateway device certificate, which is used to authenticate the gateway.

3.2 Management Requirements

3.1.1. Firewall Enable

The cabhSecFwPolicyFileEnable object enables or disables firewall rule set filtering functions.

3.1.2. Firewall Configuration File Download

The firewall configuration file download process is documented in [21]. From a network management station, the operator:

û sets cabhSecFwPolicyFileHash to the hash value calculated using the firewall configuration file.

û sets cabhSecFwPolicyFileURL to the name and IP address of the firewall configuratrion file using TFTP URL format. When this value changes, it triggers the file download.

Download status and the version of the firewall configuration file can be obtained from the cabhSecFwPolicyFileOperStatus and cabhSecFwPolicyCurrentVersion MIB objects.

3.1.3 Firewall Event Management

There are three types of firewall events that can be logged. The following objects allow the operator to enable or disable the logging of these events:

û cabhSecFwEventType1Enable controls the logging of Type 1 event messages which indicate attempts from both private and public clients to traverse the firewall that violate the security policy.

û cabhSecFwEventType2Enable controls the logging of Type 2 event messages which indicate the detection of Denial-of-Service attacks.

û cabhSecFwEventType3Enable controls the logging of Type 3 event messages which indicate changes in firewall management parameters.

Event messaging details are documented in [21].

3.1.4 Firewall Attack Alert

The Firewall Attack Alert MIB objects enable an MSO to be notified when a firewall as been attacked a certain number of times within a given period.

The cabhSecFwEventAttackAlertThreshold object is set with the number of Type 1 or Type 2 hacker attacks that are allowed within the time period attacks exceed this number an event message MUST be logged.

The cabhSecFwEventAttackAlertPeriod object indicates the period to be used (in hours) for the cabhSecFwEventAttackAlertThreshold. This MIB object should always keep track of the last x hours of event meaning that if the variable is set to track events for 10 hours then when the 11th hour is reached, the 1st hour of events is deleted from the tracking log. A default value is set to zero, meaning zero time, so that this MIB variable will not track any events unless configured.

3.1.5 PS Certificate

The cabhSecCertPsCert provides the ability to read the certificate information in a compliant CableHome residential gateway device. The PS certicate is used to in the process to authenticate the device.

4. MIB Definitions

```
   CABH-IETF-SEC-MIB DEFINITIONS ::= BEGIN

   IMPORTS
       MODULE-IDENTITY,
       Unsigned32,
       zeroDotZero,
       OBJECT-TYPE,
       mib-2                      FROM SNMPv2-SMI  -- RFC2578

       DateAndTime,
       TruthValue,
       TimeStamp,
       VariablePointer            FROM SNMPv2-TC  -- RFC2579

       OBJECT-GROUP,
       MODULE-COMPLIANCE          FROM SNMPv2-CONF -- RFC2580
       InetPortNumber,
       InetAddressType,
       InetAddress                FROM INET-ADDRESS-MIB --RFC3291

       SnmpAdminString            FROM SNMP-FRAMEWORK-MIB --RFC2571

       DocsX509ASN1DEREncodedCertificate FROM DOCS-BPI2-MIB
       --TC available in draft-ietf-ipcdn-bpiplus-mib-09.txt or after

       ZeroBasedCounter32         FROM RMON2-MIB

       docsDevFilterIpEntry       FROM DOCS-CABLE-DEVICE-MIB;

   cabhSecMib MODULE-IDENTITY
       LAST-UPDATED    "200306210000Z" -- Jun 21, 2003
       ORGANIZATION    "IETF IPCDN Working Group"
       CONTACT-INFO
               "Kevin Luehrs
               Postal: Cable Television Laboratories, Inc.
               400 Centennial Parkway
               Louisville, Colorado 80027-1266
               U.S.A.
               Phone:  +1 303-661-9100
               Fax:    +1 303-661-9199
               E-mail: k.luehrs@cablelabs.com; mibs@cablelabs.com

               IETF IPCDN Working Group
               General Discussion: ipcdn@ietf.org
               Subscribe: http://www.ietf.org/mailman/listinfo/ipcdn
```

```
               Archive: ftp://ftp.ietf.org/ietf-mail-archive/ipcdn
               Co-chairs: Richard Woundy,
                          Richard_Woundy@cable.comcast.com
                          Jean-Francois Mule, jf.mule@cablelabs.com"
       DESCRIPTION
               "This MIB module supplies the basic management
               objects for the Security Portal Services.

               Copyright (C) The Internet Society (2003). This version
               of this MIB module is part of RFC xxxx; see the RFC
   itself
               for full legal notices."
       REVISION         "200306210000Z" -- Jun 21, 2003
       DESCRIPTION
               "Initial version, published as RFC xxxx."
               -- RFC editor to assign xxxx
       ::= { mib-2 xx }
       -- xx to be assigned by IANA

   -- Textual Conventions

      cabhSecMibObjects  OBJECT IDENTIFIER ::= { cabhSecMib 1 }
      cabhSecFwObjects   OBJECT IDENTIFIER ::= { cabhSecMibObjects 1 }
      cabhSecFwBase      OBJECT IDENTIFIER ::= { cabhSecFwObjects 1 }
      cabhSecFwLogCtl    OBJECT IDENTIFIER ::= { cabhSecFwObjects 2 }

      cabhSecCertObjects OBJECT IDENTIFIER ::= { cabhSecMibObjects 2 }
      cabhSecKerbObjects OBJECT IDENTIFIER ::= { cabhSecMibObjects 3 }
      cabhSecKerbBase    OBJECT IDENTIFIER ::= { cabhSecKerbObjects 1 }

      cabhSec2FwObjects  OBJECT IDENTIFIER ::= { cabhSecMibObjects 4 }
      cabhSec2FwBase     OBJECT IDENTIFIER ::= { cabhSec2FwObjects 1 }
      cabhSec2FwEvent    OBJECT IDENTIFIER ::= { cabhSec2FwObjects 2 }
      cabhSec2FwLog      OBJECT IDENTIFIER ::= { cabhSec2FwObjects 3 }
      cabhSec2FwFilter   OBJECT IDENTIFIER ::= { cabhSec2FwObjects 4 }


   --
   --    CableHome 1.0 Base Firewall Functions
   --

   cabhSecFwPolicyFileEnable OBJECT-TYPE
       SYNTAX      INTEGER {
                       enable(1),
                       disable(2)
                   }
       MAX-ACCESS  read-write
       STATUS      current
       DESCRIPTION
```

"This parameter indicates whether or not to enable the

```
               firewall functionality."
       DEFVAL {enable}
       ::= { cabhSecFwBase 1 }

   cabhSecFwPolicyFileURL OBJECT-TYPE
       SYNTAX      SnmpAdminString
       MAX-ACCESS  read-write
       STATUS      current
       DESCRIPTION
               "Contains the location of the last successfull downloaded
               policy rule set file in the format pointed in the
               reference. A policy rule set file download is triggered
               when the value used to SET this MIB is different than the
               value in the cabhSecFwPolicySuccessfulFileURL object."
       REFERENCE
               "CableHome 1.0 Specification, CH-SP-I04-030411,
               11.3.5.2 Firewall Rule Set Management Parameters"
       ::= { cabhSecFwBase 2 }

   cabhSecFwPolicyFileHash OBJECT-TYPE
       SYNTAX OCTET STRING (SIZE(0|20))
       MAX-ACCESS read-write
       STATUS current
       DESCRIPTION
               "Hash of the contents of the rules set file, calculated
               and sent to the PS prior to sending the rules set file.
               For the SHA-1 authentication algorithm the length of the
               hash is 160 bits. This hash value is encoded in binary
               format."
       DEFVAL {''h}
       ::= { cabhSecFwBase 3 }

   cabhSecFwPolicyFileOperStatus OBJECT-TYPE
       SYNTAX     INTEGER    {
                       inProgress(1),
                       complete(2),
                     -- completeFromMgt(3), deprecated
                       failed(4)
                  }
       MAX-ACCESS read-only
       STATUS current
       DESCRIPTION
               "inProgress(1) indicates a firewall configuration file
               download is underway.
               complete (2) indicates the firewall configuration file
               downloaded and configured successfully.
               completeFromMgt(3) This state is deprecated.
               failed(4) indicates the last attempted firewall
               configuration file download or processing failed
```

ordinarily due to TFTP timeout."

```
       ::= { cabhSecFwBase 4 }


   cabhSecFwPolicyFileCurrentVersion OBJECT-TYPE
       SYNTAX      SnmpAdminString
       MAX-ACCESS  read-only
       STATUS      current
       DESCRIPTION
               "The rule set version currently operating in the PS
               device. This object should be in the syntax used by the
               individual vendor to identify software versions.  Any PS
               element MUST return a string descriptive of the current
               rule set file load. If this is not applicable, this
               object MUST contain an empty string."
       ::= { cabhSecFwBase 5 }

   cabhSecFwPolicySuccessfulFileURL OBJECT-TYPE
       SYNTAX      SnmpAdminString
       MAX-ACCESS  read-only
       STATUS      current
       DESCRIPTION
               "Contains the location of the last successfull downloaded
               policy rule set file in the format pointed in the
               reference. If a successful download has not yet occurred,
               this MIB object should report empty string."
       REFERENCE
               "CableHome 1.0 Specification, CH-SP-I04-030411,
               11.3.5.2 Firewall Rule Set Management Parameters"
       ::= { cabhSecFwBase 6 }

   --
   --    CableHome 1.0 Firewall Event MIBs
   --


   cabhSecFwEventType1Enable OBJECT-TYPE
       SYNTAX    INTEGER {
                     enable (1), -- log event
                     disable (2) -- do not log event
                 }
       MAX-ACCESS read-write
       STATUS    current
       DESCRIPTION
               "This object enables or disables logging of type 1
               firewall event messages. Type 1 event messages report
               attempts from both private and public clients to traverse
               the firewall that violate the Security Policy."
       DEFVAL { disable }
       ::= { cabhSecFwLogCtl 1 }
```

```
   cabhSecFwEventType2Enable OBJECT-TYPE
       SYNTAX    INTEGER {
                    enable (1), -- log event
                    disable (2) -- do not log event
                 }
       MAX-ACCESS read-write
       STATUS current
       DESCRIPTION
               "This object enables or disables logging of type 2
               firewall event messages. Type 2 event messages report
               identified Denial of Service attack attempts."
       DEFVAL { disable }
       ::= { cabhSecFwLogCtl 2 }

   cabhSecFwEventType3Enable OBJECT-TYPE
       SYNTAX INTEGER {
                 enable (1), -- log event
                 disable (2) -- do not log event
              }
       MAX-ACCESS read-write
       STATUS current
       DESCRIPTION
               "Enables or disables logging of type 3 firewall event
               messages.
               Type 3 event messages report changes made to the
               following firewall management parameters:
               cabhSecFwPolicyFileURL,
               cabhSecFwPolicyFileCurrentVersion,
               cabhSecFwPolicyFileEnable"
       DEFVAL { disable }
       ::= { cabhSecFwLogCtl 3 }

   cabhSecFwEventAttackAlertThreshold  OBJECT-TYPE
       SYNTAX     INTEGER    (0..65535)
       MAX-ACCESS read-write
       STATUS current
       DESCRIPTION
               "If the number of type 1 or 2 hacker attacks exceeds
               this threshold in the period define by
               cabhSecFwEventAttackAlertPeriod, a firewall message
               event MUST be logged with priority level 4."
       DEFVAL { 65535 }
       ::= { cabhSecFwLogCtl 4 }


   cabhSecFwEventAttackAlertPeriod OBJECT-TYPE
       SYNTAX    INTEGER (0..65535)
       MAX-ACCESS read-write
       STATUS current
```

```
        DESCRIPTION
```

```
               "Indicates the period to be used (in hours) for the
               cabhSecFwEventAttackAlertThreshold. This MIB variable
               should always keep track of the last x hours of events
               meaning that if the variable is set to track events for
               10 hours then when the 11th hour is reached, the 1st hour
               of events is deleted from the tracking log. A default
               value is set to zero, meaning zero time, so that this MIB
               variable will not track any events unless configured."
       DEFVAL { 0 }
       ::= { cabhSecFwLogCtl 5 }


   --
   -- CableHome PS device certificate
   --

       cabhSecCertPsCert OBJECT-TYPE
       SYNTAX         DocsX509ASN1DEREncodedCertificate
       MAX-ACCESS    read-only
       STATUS         current
       DESCRIPTION
               "The X509 DER-encoded PS certificate."
       ::= { cabhSecCertObjects 1 }



   --
   --  CableHome 1.1 Firewall Management MIBs
   --

   cabhSec2FwEnable OBJECT-TYPE
       SYNTAX      INTEGER    {
                      enabled(1),
                      disabled(2)
                     }
       MAX-ACCESS  read-write
       STATUS      current
       DESCRIPTION
               "This parameter indicates whether to enable or disable
               the firewall."
       DEFVAL {enabled }
       ::= { cabhSec2FwBase 1 }


   cabhSec2FwPolicyFileURL OBJECT-TYPE
       SYNTAX      SnmpAdminString
       MAX-ACCESS  read-write
       STATUS      current
       DESCRIPTION
               "Contains the location of the last successfull downloaded
```

```
               policy rule set file in the format pointed in the
               reference. A policy rule set file download is triggered
               when the value used to SET this MIB is different than the
               value in the cabhSec2FwPolicySuccessfulFileURL object."
        REFERENCE
                "CableHome 1.1 Specification, CH-1.1-SP-I01-030418,
                11.6.4.7.1 Firewall Rule Set Management MIB Objects"
       ::= { cabhSec2FwBase 2 }


   cabhSec2FwPolicyFileHash OBJECT-TYPE
       SYNTAX OCTET STRING (SIZE(0|20))
       MAX-ACCESS read-write
       STATUS current
       DESCRIPTION
               "Hash of the contents of the firewall configuration file.
               For the SHA-1 authentication algorithm the length of the
               hash is 160 bits. This hash value is encoded in binary
               format."
       DEFVAL { ''h}
       ::= { cabhSec2FwBase 3 }


   cabhSec2FwPolicyFileOperStatus OBJECT-TYPE
       SYNTAX      INTEGER {
                       inProgress(1),
                       complete(2),
                       failed(3)
                   }
       MAX-ACCESS  read-only
       STATUS      current
       DESCRIPTION
               "InProgress(1) indicates a firewall configuration file
               download is underway. Complete(2) indicates the firewall
               configuration file was downloaded and processed
               successfully. Failed(3) indicates that the last attempted
               firewall configuration file download or processing
               failed."
       ::= { cabhSec2FwBase 4 }


   cabhSec2FwPolicyFileCurrentVersion OBJECT-TYPE
       SYNTAX      SnmpAdminString
       MAX-ACCESS  read-write
       STATUS      current
       DESCRIPTION
               "A label set by the cable operator that can be used to
               track various versions of configured rulesets. Once the
               label is set it and configured rules are changed, it may
```

not accurately reflect the version of configured rules

```
               running  on the box.
               This object MUST contain the string 'null' if has never
               been configured."
       DEFVAL { "null" }
       ::= { cabhSec2FwBase 5 }


   cabhSec2FwClearPreviousRuleset OBJECT-TYPE
       SYNTAX      INTEGER    {
                      increment(1),
                      complete(2),
                      incrementDefault(3)
                    }
       MAX-ACCESS  read-write
       STATUS      current
       DESCRIPTION
               "Allows PS or firewall configuration files to contain
               either a complete firewall configured ruleset or an
               incremental to the already established configured ruleset
               depending up on its existence in the configuration file.
               If the PS receives a configuration file with firewall
               settings which includes a cabhSec2FwClearPreviousRuleset
               object setting marked as increment(1) or if this object
               setting is not included in a configuration file which
               contains filter settings for the firewall, then the PS
               MUST treat the firewall filter settings in the
               configuration file as an increment to the configured
               ruleset. If the PS receives a configuration file with
               firewall settings which includes a
               cabhSec2FwClearPreviousRuleset object setting marked as
               incrementDefault(3) then the PS MUST remove all
               previously configured rules from the configured ruleset,
               including any rules in the filter schedule table and
               increment the newly downloaded rules on top of (i.e.
               subsequent to) the factory default policy.  If the PS
               receives a configuration file with firewall settings
               which includes a cabhSec2FwClearPreviousRuleset object
               setting marked as complete(2), then the PS MUST remove
               all previously configured rules from the configured
               ruleset, including any rules in
               cabhSec2FwFilterScheduleTable table before applying
               the firewall filter settings contained in the
               configuration file.

               If cabhSec2FwClearPreviousRuleset is set to increment(1)
               using SNMP, the PS MUST treat all of the following
               firewall filter settings using SNMP as an increment to
               the configured ruleset.
```

```
                 If cabhSec2FwClearPreviousRuleset is set to
```

```
               incrementDefault(3) using SNMP, the PS MUST remove all
               previously configured rules from the configured ruleset,
               including any rules in the filter schedule table and
               treat all of the following firewall filter settings using
               SNMP as an increment on top of the factory default
               policy. If cabhSec2FwClearPreviousRuleset is set to
               complete(2), then the PS MUST remove all rules from the
               configured ruleset, including any rules in the filter
               schedule table. In this scenario the PS will operate
               without any configured rules, (e.g. there will be no
               defined filtering rules, but the firewall will still
               provide the minimum set of capabilities and
               architecture)."
       REFERENCE
               "CableHome 1.1 Specification, CH-1.1-SP-I01-030418,
               11.6.4.4 Firewall Filtering"
       DEFVAL { increment }
       ::= { cabhSec2FwBase 6 }

   cabhSec2FwPolicySelection  OBJECT-TYPE
       SYNTAX      INTEGER {
                      factoryDefault(1),
                      configuredRuleset(2)
                   }
       MAX-ACCESS  read-write
       STATUS      current
       DESCRIPTION
               "This parameter indicates which policy should currently
               be running in the firewall, either the factoryDefault
               policy or the configuredRuleset."
       DEFVAL { factoryDefault }
       ::= { cabhSec2FwBase 7 }

   cabhSec2FwEventSetToFactory  OBJECT-TYPE
       SYNTAX      TruthValue
       MAX-ACCESS  read-write
       STATUS      current
       DESCRIPTION
               "If set to 'true', entries in cabhSec2FwEventControlEntry
               are set to their default values. Reading this value
               always returns false."
       DEFVAL { false }
       ::= { cabhSec2FwBase 8 }


   cabhSec2FwEventLastSetToFactory OBJECT-TYPE
       SYNTAX       TimeStamp
       MAX-ACCESS   read-only
       STATUS       current
       DESCRIPTION
```

```
               "The value of sysUpTime when cabhSec2FwEventSetToFactory
               was last set to true. Zero if never reset."
       ::= { cabhSec2FwBase 9 }


   cabhSec2FwPolicySuccessfulFileURL OBJECT-TYPE
       SYNTAX      SnmpAdminString
       MAX-ACCESS  read-only
       STATUS      current
       DESCRIPTION
               "Contains the location of the last successfull downloaded
               policy rule set file in the format pointed in the
               reference. If a successful download has not yet occurred,
               this MIB object should report empty string."
       REFERENCE
               "CableHome 1.1 Specification, CH-1.1-SP-I01-030418,
               11.6.4.7.1 Firewall Rule Set Management MIB Objects"
       ::= { cabhSec2FwBase 10 }

   --
   -- CableHome 1.1 Firewall Event MIBS
   --


   cabhSec2FwEventControlTable OBJECT-TYPE
       SYNTAX      SEQUENCE OF CabhSec2FwEventControlEntry
       MAX-ACCESS  not-accessible
       STATUS      current
       DESCRIPTION
               "This table controls the reporting of the Firewall
               Attacks events"
       ::= { cabhSec2FwEvent 1 }


   cabhSec2FwEventControlEntry OBJECT-TYPE
       SYNTAX      CabhSec2FwEventControlEntry
       MAX-ACCESS  not-accessible
       STATUS      current
       DESCRIPTION
               "Allows configuration of the reporting mechanisms for a
               particular type of attack."
       INDEX { cabhSec2FwEventType }
       ::= { cabhSec2FwEventControlTable 1 }

   CabhSec2FwEventControlEntry ::= SEQUENCE {
       cabhSec2FwEventType        INTEGER,
       cabhSec2FwEventEnable      INTEGER,
       cabhSec2FwEventThreshold   Unsigned32,
       cabhSec2FwEventInterval    Unsigned32,
       cabhSec2FwEventCount       ZeroBasedCounter32,
       cabhSec2FwEventLogReset    TruthValue,
       cabhSec2FwEventLogLastReset TimeStamp

       }

   cabhSec2FwEventType OBJECT-TYPE
       SYNTAX INTEGER     {
                 type1(1),
                 type2(2),
                 type3(3),
                 type4(4),
                 type5(5),
                 type6(6)
              }
       MAX-ACCESS  not-accessible
       STATUS      current
       DESCRIPTION
           "Classification of the different types of attacks.
           Type 1 logs all attempts from both LAN and WAN clients to
           traverse the Firewall that violate the Security Policy.
           Type 2 logs identified Denial of Service attack attempts.
           Type 3 logs all changes made to the cabhSec2FwPolicyFileURL,
           cabhSec2FwPolicyFileCurrentVersion or
           cabhSec2FwPolicyFileEnable objects.
           Type 4 logs all failed attempts to modify
           cabhSec2FwPolicyFileURL and cabhSec2FwPolicyFileEnable
           objects. Type 5 logs allowed inbound packets from the WAN.
           Type 6 logs allowed outbound packets from the LAN."
       ::= { cabhSec2FwEventControlEntry 1 }

   cabhSec2FwEventEnable OBJECT-TYPE
       SYNTAX      INTEGER    {
                      enabled(1),
                      disabled(2)
                    }
       MAX-ACCESS  read-write
       STATUS      current
       DESCRIPTION
               "Enables or disables counting and logging of firewall
               events by type as assigned by cabhSec2FwEventType."
       DEFVAL { disabled }
       ::= { cabhSec2FwEventControlEntry 2 }


   cabhSec2FwEventThreshold OBJECT-TYPE
       SYNTAX       Unsigned32 (0..65535)
       MAX-ACCESS   read-write
       STATUS       current
       DESCRIPTION
```

```
               "Number of attacks to count before sending the
               appropriate event by type as assigned by
               cabhSec2FwEventType."
        DEFVAL { 0 }
        ::= { cabhSec2FwEventControlEntry 3 }


   cabhSec2FwEventInterval OBJECT-TYPE
        SYNTAX       Unsigned32 (0..65535)
        UNITS        "hours"
        MAX-ACCESS   read-write
        STATUS      current
        DESCRIPTION
               "Indicates the time interval in hours to count and log
               occurrences of a firewall event type as assigned in
               cabhSec2FwEventType. If this MIB has a value of zero then
               there is no interval assigned and the PS will not count
               or  log events."
        DEFVAL { 0 }
        ::= { cabhSec2FwEventControlEntry 4 }

   cabhSec2FwEventCount OBJECT-TYPE
        SYNTAX       ZeroBasedCounter32
        MAX-ACCESS   read-only
        STATUS       current
        DESCRIPTION
               "Indicates the current count up to the
               cabhSec2FwEventThreshold value by type as assigned by
               cabhSec2FwEventType."
        ::= { cabhSec2FwEventControlEntry 5 }


   cabhSec2FwEventLogReset OBJECT-TYPE
        SYNTAX       TruthValue
        MAX-ACCESS   read-write
        STATUS       current
        DESCRIPTION
               "Setting this object to true clears the log table for the
               specified event type. Reading this object always returns
               false."
        DEFVAL { false }
        ::= { cabhSec2FwEventControlEntry 6 }


   cabhSec2FwEventLogLastReset     OBJECT-TYPE
        SYNTAX       TimeStamp
        MAX-ACCESS   read-only
        STATUS       current
        DESCRIPTION
               "The value of sysUpTime when cabhSec2FwEventLogReset was
```

```
                  last set to true. Zero if never reset."
```

```
        ::= { cabhSec2FwEventControlEntry 7 }



   --
   -- CableHome 1.1 Firewall Log Tables
   --
   cabhSec2FwLogTable OBJECT-TYPE
       SYNTAX      SEQUENCE OF CabhSec2FwLogEntry
       MAX-ACCESS  not-accessible
       STATUS      current
       DESCRIPTION
               "Contains a log of packet information as related to
               events enabled by the cable operator. The types are
               defined in the CableHome 1.1 specification and require
               various objects to be included in the log.
               The following is a description for what is expected in
               the log for each type Type 1, Type 2, Type 5 and Type 6
               table MUST include cabhSec2FwEventType,
               cabhSec2FwEventPriority, cabhSec2FwEventId,
               cabhSec2FwLogTime, cabhSec2FwIpProtocol,
               cabhSec2FwIpSourceAddr, cabhSec2FwIpDestAddr,
               cabhSec2FwIpSourcePort, cabhSec2FwIpDestPort,
               cabhSec2Fw, cabhSec2FwReplayCount. The other values not
               used by types 1, 2, 5 and 6 are default values. Type 3
               and Type 4 MUST include cabhSec2FwEventType,
               cabhSec2FwEventPriority,
               cabhSec2FwEventId, cabhSec2FwLogTime,
               cabhSec2FwIpSourceAddr, cabhSec2FwLogMIBPointer.
               The other values not used by type 3 and 4 are default
               values."
       ::= { cabhSec2FwLog 1 }

   cabhSec2FwLogEntry OBJECT-TYPE
       SYNTAX      CabhSec2FwLogEntry
       MAX-ACCESS  not-accessible
       STATUS      current
       DESCRIPTION
           "Each entry contains the log of firewall events"
       INDEX {cabhSec2FwLogIndex}
       ::= { cabhSec2FwLogTable 1 }

   CabhSec2FwLogEntry ::= SEQUENCE {
       cabhSec2FwLogIndex             Unsigned32,
       cabhSec2FwLogEventType         INTEGER,
       cabhSec2FwLogEventPriority     INTEGER,
       cabhSec2FwLogEventId           Unsigned32,
       cabhSec2FwLogTime              DateAndTime,
       cabhSec2FwLogIpProtocol        Unsigned32,
        cabhSec2FwLogIpAddrType        InetAddressType,
        cabhSec2FwLogIpSourceAddr      InetAddress,
        cabhSec2FwLogIpDestAddr        InetAddress,
        cabhSec2FwLogIpSourcePort      InetPortNumber,
        cabhSec2FwLogIpDestPort        InetPortNumber,
        cabhSec2FwLogMessageType       Unsigned32,
        cabhSec2FwLogReplayCount       Unsigned32,
        cabhSec2FwLogMIBPointer        VariablePointer
    }

    cabhSec2FwLogIndex OBJECT-TYPE
        SYNTAX      Unsigned32 (1..2147483647)
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
                "A sequence number for the specific events under a
                cabhSec2FwEventType."
        ::= { cabhSec2FwLogEntry 1 }

    cabhSec2FwLogEventType OBJECT-TYPE
        SYNTAX INTEGER     {
                  type1(1),
                  type2(2),
                  type3(3),
                  type4(4),
                  type5(5),
                  type6(6)
                }
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
                "Classification of the different types of attacks.
                Type 1 logs all attempts from both LAN and WAN clients to
                traverse the Firewall that violate the Security Policy.
                Type 2 logs identified Denial of Service attack attempts.
                Type 3 logs all changes made to the
                cabhSec2FwPolicyFileURL,
                cabhSec2FwPolicyFileCurrentVersion or
                cabhSec2FwPolicyFileEnable objects.
                Type 4 logs all failed attempts to modify
                cabhSec2FwPolicyFileURL and cabhSec2FwPolicyFileEnable
                objects.
                Type 5 logs allowed inbound packets from the WAN.
                Type 6 logs allowed outbound packets from the LAN."
        ::= { cabhSec2FwLogEntry 2 }

    cabhSec2FwLogEventPriority OBJECT-TYPE
        SYNTAX     INTEGER     {
                      emergency(1),
                      alert(2),
                                critical(3),
                                error(4),
                                warning(5),
                                notice(6),
                                information(7),
                                debug(8)
                             }
                  MAX-ACCESS  read-only
                  STATUS      current
                  DESCRIPTION
                          "The priority level of this event as defined by CableHome
                          Specification. If a priority is not assigned in the
                          CableHome specification for a particular event then the
                          vendor or cable operator may assign priorities. These are
                          ordered from most serious (emergency) to least serious
                          (debug)."
                  ::= { cabhSec2FwLogEntry 3 }


              cabhSec2FwLogEventId  OBJECT-TYPE
                  SYNTAX      Unsigned32
                  MAX-ACCESS  read-only
                  STATUS      current
                  DESCRIPTION
                          "The assigned event ID."
                  ::= { cabhSec2FwLogEntry 4 }


              cabhSec2FwLogTime OBJECT-TYPE
                  SYNTAX      DateAndTime
                  MAX-ACCESS  read-only
                  STATUS      current
                  DESCRIPTION
                          "The time that this entry was created by the PS."
                  ::= { cabhSec2FwLogEntry 5 }


              cabhSec2FwLogIpProtocol OBJECT-TYPE
                  SYNTAX      Unsigned32 (0..256)
                  MAX-ACCESS  read-only
                  STATUS      current
                  DESCRIPTION
                          "The IP Protocol"
                  ::= { cabhSec2FwLogEntry 6 }


              cabhSec2FwLogIpAddrType OBJECT-TYPE
                  SYNTAX      InetAddressType
                  MAX-ACCESS  read-only
                  STATUS      current
```

```
        DESCRIPTION
```

```
               "The type of IP addresses in the packet"
       ::= { cabhSec2FwLogEntry 7 }


   cabhSec2FwLogIpSourceAddr OBJECT-TYPE
       SYNTAX      InetAddress
       MAX-ACCESS  read-only
       STATUS      current
       DESCRIPTION
               "The Source IP Address of the packet logged.
               The address type of this object is specified by
               cabhSec2FwLogIpAddrType."
       ::= { cabhSec2FwLogEntry 8 }


   cabhSec2FwLogIpDestAddr OBJECT-TYPE
       SYNTAX      InetAddress
       MAX-ACCESS  read-only
       STATUS      current
       DESCRIPTION
               "The Destination IP Address of the packet logged.
               The address type of this object is specified by
               cabhSec2FwLogIpAddrType."
       ::= { cabhSec2FwLogEntry 9 }


   cabhSec2FwLogIpSourcePort OBJECT-TYPE
       SYNTAX      InetPortNumber
       MAX-ACCESS  read-only
       STATUS      current
       DESCRIPTION
               "The Source IP Port of the packet logged"
       ::= { cabhSec2FwLogEntry 10 }


   cabhSec2FwLogIpDestPort OBJECT-TYPE
       SYNTAX      InetPortNumber
       MAX-ACCESS  read-only
       STATUS      current
       DESCRIPTION
               "The Source IP Port of the packet logged"
       ::= { cabhSec2FwLogEntry 11 }


   cabhSec2FwLogMessageType OBJECT-TYPE
       SYNTAX      Unsigned32
       MAX-ACCESS  read-only
       STATUS      current
       DESCRIPTION
               "The ICMP defined types."
```

```
       ::= { cabhSec2FwLogEntry 12 }


   cabhSec2FwLogReplayCount OBJECT-TYPE
       SYNTAX      Unsigned32
       MAX-ACCESS  read-only
       STATUS      current
       DESCRIPTION
               "The number of identical attack packets that were seen by
               the firewall based on cabhSec2FwLogIpProtocol,
               cabhSec2FwLogIpSourceAddr, cabhSec2FwLogIpDestAddr,
               cabhSec2FwLogIpSourcePort, cabhSec2FwLogIpDestPort and
               cabhSec2FwLogMessageType"
       DEFVAL { 0 }
       ::= { cabhSec2FwLogEntry 13 }

   cabhSec2FwLogMIBPointer OBJECT-TYPE
       SYNTAX      VariablePointer
       MAX-ACCESS  read-only
       STATUS      current
       DESCRIPTION
               "Identifies if the cabhSec2FwPolicyFileURL or the
               cabhSec2FwEnable MIB object changed or an attempt was
               made to change it."
       DEFVAL { zeroDotZero }
       ::= { cabhSec2FwLogEntry 14 }


   -- ============================================================
   --
   --  CableHome 1.1 PS IP Filter Scheduling Table
   --
   --  The cabhSec2FwFilterScheduleTable contains the firewall
   --  policy identification and links that policy as defined
   --  in RFC 2669 to specific time of day restrictions.
   --
   -- =============================================================


   cabhSec2FwFilterScheduleTable OBJECT-TYPE
       SYNTAX SEQUENCE OF CabhSec2FwFilterScheduleEntry
       MAX-ACCESS    not-accessible
       STATUS        current
       DESCRIPTION
               "Extends the filtering matching parameters of
               docsDevFilterIpTable defined in RFC 2669 for CableHome
               Residential Gateways to include time day intervals and
               days of the week."
       ::= { cabhSec2FwFilter 1 }
```

```
   cabhSec2FwFilterScheduleEntry OBJECT-TYPE
       SYNTAX CabhSec2FwFilterScheduleEntry
       MAX-ACCESS not-accessible
       STATUS current
       DESCRIPTION
               "Extended values for entries of docsDevFilterIpTable.
               If the PS has not acquired ToD the entire
               docsDevFilterIpEntry rule set is ignored."
       AUGMENTS { docsDevFilterIpEntry }
       ::= { cabhSec2FwFilterScheduleTable 1 }


   CabhSec2FwFilterScheduleEntry ::= SEQUENCE {
       cabhSec2FwFilterScheduleStartTime    DateAndTime,
       cabhSec2FwFilterScheduleEndTime      DateAndTime,
       cabhSec2FwFilterScheduleDOW          BITS
       }


   cabhSec2FwFilterScheduleStartTime OBJECT-TYPE
       SYNTAX         DateAndTime
       MAX-ACCESS     read-create
       STATUS        current
       DESCRIPTION
               "The start time, with optional time zone, for a firewall
               filter ruleset. Only the time portion of the DateAndTime
               TEXTUAL-CONVENTION have a meaning."
       ::= { cabhSec2FwFilterScheduleEntry 1 }

   cabhSec2FwFilterScheduleEndTime OBJECT-TYPE
       SYNTAX            DateAndTime
       MAX-ACCESS        read-create
       STATUS            current
       DESCRIPTION
               "The end time, with optional time zone, for a firewall
               filter ruleset. Only the time portion of the DateAndTime
               TEXTUAL-CONVENTION have a meaning."
       ::= { cabhSec2FwFilterScheduleEntry 2 }


   cabhSec2FwFilterScheduleDOW OBJECT-TYPE
       SYNTAX BITS {
                sunday(0),
                monday(1),
                tuesday(2),
                wednesday(3),
                thursday(4),
                friday(5),
                saturday(6)
```

```
              }
          MAX-ACCESS   read-create
          STATUS       current
          DESCRIPTION
                  "If the day of week bit associated with the PS given day
                  is '1', this object criteria matches."
          ::= { cabhSec2FwFilterScheduleEntry 3 }

      --
      -- Kerberos MIBs
      --


      cabhSecKerbPKINITGracePeriod    OBJECT-TYPE
          SYNTAX                 Unsigned32 (15..600)
          UNITS                  "minutes"
          MAX-ACCESS             read-write
          STATUS                 current
          DESCRIPTION
                  "The PKINIT Grace Period is needed by the PS to know when
                  it should start retrying to get a new ticket. The PS MUST
                  obtain a new Kerberos ticket (with a PKINIT exchange);
                  this may be many minutes before the old ticket expires."
          DEFVAL { 30 }
          ::= { cabhSecKerbBase 1}

          cabhSecKerbTGSGracePeriod    OBJECT-TYPE
          SYNTAX            Unsigned32 (1..600)
          UNITS             "minutes"
          MAX-ACCESS        read-write
          STATUS            current
          DESCRIPTION
                  "The TGS Grace Period is needed by the PS to know when it
                  should start retrying to get a new ticket. The PS MUST
                  obtain a new Kerberos ticket (with a TGS Request); this
                  may be many minutes before the old ticket expires."
          DEFVAL { 10 }
          ::= { cabhSecKerbBase 2}

      cabhSecKerbUnsolicitedKeyMaxTimeout    OBJECT-TYPE
          SYNTAX            Unsigned32 (15..600)
          UNITS             "seconds"
          MAX-ACCESS        read-write
          STATUS            current
          DESCRIPTION
                  "This timeout applies to PS initiated AP-REQ/REP key
                  management exchange with NMS. The maximum timeout is the
                  value which may not be exceeded in the exponential
                  backoff algorithm."
```

```
        DEFVAL { 600 }
        ::= { cabhSecKerbBase 3}


   cabhSecKerbUnsolicitedKeyMaxRetries    OBJECT-TYPE
       SYNTAX              Unsigned32 (1..32)
       MAX-ACCESS          read-write
       STATUS              current
       DESCRIPTION
               "The number of retries the PS is allowed for AP-REQ/REP
               key management exchange initiation with the NMS. This is
               the maximum number of retries before the PS gives up
               attempting to establish an SNMPv3 security association
               with NMS."
       DEFVAL { 8 }
         ::= { cabhSecKerbBase 4}

   cabhSecNotification OBJECT IDENTIFIER ::= { cabhSecMib 2 }
   cabhSecConformance  OBJECT IDENTIFIER ::= { cabhSecMib 3 }
   cabhSecCompliances  OBJECT IDENTIFIER ::= { cabhSecConformance 1 }
   cabhSecGroups       OBJECT IDENTIFIER ::= { cabhSecConformance 2 }

   --
   --    Notification Group for future extension
   --

   -- compliance statements

       cabhSecCompliance MODULE-COMPLIANCE
       STATUS     current
       DESCRIPTION
               "The compliance statement for CableHome Security."
       MODULE   --cabhSecMib



   -- unconditionally mandatory groups

   MANDATORY-GROUPS {
           cabhSecCertGroup,
           cabhSecKerbGroup
           }


   -- conditional mandatory groups

   GROUP cabhSecGroup
       DESCRIPTION
               "This group is implemented only for CH 1.0 gateways."
```

```
   GROUP  cabhSec2Group
       DESCRIPTION
               "This group is implemented only for CH 1.1 gateways."

   OBJECT cabhSec2FwLogIpAddrType
          SYNTAX InetAddressType { ipv4(1) }
          DESCRIPTION
              "An implementation is only required to support IPv4
               addresses."

   OBJECT cabhSec2FwLogIpSourceAddr
          SYNTAX  InetAddress (SIZE(4))
          DESCRIPTION
              "An implementation is only required to support IPv4
               addresses."

   OBJECT cabhSec2FwLogIpDestAddr
          SYNTAX  InetAddress (SIZE(4))
          DESCRIPTION
              "An implementation is only required to support IPv4
               addresses."

   ::= { cabhSecCompliances 1}

   cabhSecGroup OBJECT-GROUP
       OBJECTS {
           cabhSecFwPolicyFileEnable,
           cabhSecFwPolicyFileURL,
           cabhSecFwPolicyFileHash,
           cabhSecFwPolicyFileOperStatus,
           cabhSecFwPolicyFileCurrentVersion,
           cabhSecFwPolicySuccessfulFileURL,

           cabhSecFwEventType1Enable,
           cabhSecFwEventType2Enable,
           cabhSecFwEventType3Enable,
           cabhSecFwEventAttackAlertThreshold,
           cabhSecFwEventAttackAlertPeriod
        }
       STATUS    current
       DESCRIPTION
               "Group of objects in CableHome 1.0 Firewall MIB."
       ::= { cabhSecGroups 1 }


   cabhSecCertGroup OBJECT-GROUP
       OBJECTS {
           cabhSecCertPsCert
       }
```

```
        STATUS    current
```

```
       DESCRIPTION
               "Group of objects in CableHome gateway for PS
               Certificate."
       ::= { cabhSecGroups 2 }


   cabhSecKerbGroup OBJECT-GROUP
       OBJECTS {
           cabhSecKerbPKINITGracePeriod,
           cabhSecKerbTGSGracePeriod,
           cabhSecKerbUnsolicitedKeyMaxTimeout,
           cabhSecKerbUnsolicitedKeyMaxRetries
       }
       STATUS    current
       DESCRIPTION
               "Group of objects in CableHome gateway for Kerberos."
       ::= { cabhSecGroups 3 }

   cabhSec2Group OBJECT-GROUP
       OBJECTS {
           cabhSec2FwEnable,
           cabhSec2FwPolicyFileURL,
           cabhSec2FwPolicyFileHash,
           cabhSec2FwPolicyFileOperStatus,
           cabhSec2FwPolicyFileCurrentVersion,
           cabhSec2FwClearPreviousRuleset,
           cabhSec2FwPolicySelection,
           cabhSec2FwEventSetToFactory,
           cabhSec2FwEventLastSetToFactory,
           cabhSec2FwPolicySuccessfulFileURL,
           cabhSec2FwEventEnable,
           cabhSec2FwEventThreshold,
           cabhSec2FwEventInterval,
           cabhSec2FwEventCount,
           cabhSec2FwEventLogReset,
           cabhSec2FwEventLogLastReset,
           cabhSec2FwLogEventType,
           cabhSec2FwLogEventPriority,
           cabhSec2FwLogEventId,
           cabhSec2FwLogTime,
           cabhSec2FwLogIpProtocol,
           cabhSec2FwLogIpAddrType,
           cabhSec2FwLogIpSourceAddr,
           cabhSec2FwLogIpDestAddr,
           cabhSec2FwLogIpSourcePort,
           cabhSec2FwLogIpDestPort,
           cabhSec2FwLogMessageType,
           cabhSec2FwLogReplayCount,
           cabhSec2FwLogMIBPointer,
            cabhSec2FwFilterScheduleStartTime,
            cabhSec2FwFilterScheduleEndTime,
            cabhSec2FwFilterScheduleDOW
            }
        STATUS    current
        DESCRIPTION
                "Group of objects in CableHome 1.1 Firewall MIB."
        ::= { cabhSecGroups 4 }

    END
```

5. Acknowledgements

Nancy Davoust û YAS Broadband Ventures
Jim Hinsey û Broadcom
John Bevilacqua û YAS Broadband Ventures

Funding for the RFC Editor function is currently provided by the Internet Society.

6. Formal Syntax

The following syntax specification uses the augmented Backus-Naur Form (BNF) as described in RFC-2234 [3].

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.

It is thus important to control even GET access to these objects and possibly to even encrypt the values of these objects when sending them over the network via SNMP. Not all versions of SNMP provide features for such a secure environment.

SNMP versions prior to SNMPv3 did not include adequate security. 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 module.

It is RECOMMENDED that implementers consider the security features as provided by the SNMPv3 framework (see [RFC3410], section 8),

including full support for the SNMPv3 cryptographic mechanisms (for authentication and privacy).

Further, deployment of SNMP versions prior to SNMPv3 is NOT RECOMMENDED. Instead, it is RECOMMENDED to deploy SNMPv3 and to enable cryptographic security. It is then a customer/operator responsibility to ensure that the SNMP entity giving access to an instance of this MIB module, 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. Normative References

1 Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

2 Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997

3 Crocker, D. and Overell, P.(Editors), "Augmented BNF for Syntax Specifications: ABNF", RFC 2234, Internet Mail Consortium and Demon Internet Ltd., November 1997

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

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

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

7 McCloghrie, K., Perkins, D. and J. Schoenwaelder, "Structure of Management Information for Version 2 (SMIv2)", STD 58, RFC 2578, April 1999.

8 McCloghrie, K., Perkins, D. and J. Schoenwaelder, "Textual Conventions for SMIv2", STD 58, RFC 2579, April 1999.

9 McCloghrie, K., Perkins, D. and J. Schoenwaelder, "Conformance Statements for SMIv2", STD 58, RFC 2580, April 1999.

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

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

12 Case, J., Mundy, R., Partain, D, and B. Stewart, "Introduction and Applicability Statements for Internet Standard Management Framework", RFC 3410, December 2002.

13 Harrington D., Presuhn R. and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks", RFC 3411, December 2002.

14 Case, J., Harrington D., Presuhn R. and B. Wijnen, "Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)", RFC 3412, December 2002.

15 Levi, D., Meyer, P., and B. Stewart, ôSimple Network Management Protocol (SNMP) Applications", RFC 3413, December 2002.

16 Blumenthal, U. and B. Wijnen, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)", RFC 3414, December 2002.

17 Wijnen, B., Presuhn, R. and K. McCloghrie, "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)", RFC 3415, December 2002.

18 Presuhn, R., Case, J., McCloghrie, K., Rose, M. and S. Waldbusser, "Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMPv2)", RFC 3416, Decemeber 2002.

19 Presuhn, R., Case, J., McCloghrie, K., Rose, M. and S. Waldbusser, "Transport Mappings for the Simple Network Management Protocol (SNMPv2)", RFC 3417, December 2002.

20 Presuhn, R., Case, J., McCloghrie, K., Rose, M. and S. Waldbusser, "Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)", RFC 3418, December 2002.

21 Cable Television Laboratories, ôCableHome 1.0 Specificationö, CH-SP-I02-020920, September 2002, http://www.cablelabs.com/projects/cablehome/specifications.

9. Informative References

22 Drums, R., ôDynamic Host Configuration Protocolö, RFC 2131, March 1997.

23 Hollins, K., ôThe TFTP Protocol (Revision 2)ö, RFC 1350, July 1992.

24 Harrington, R., Presuhn, R., and B. Wijnen, ôAn Architecture for Describing SNMP Management Frameworksö, RFC 2571, April 1999.

25 Daniele, M., Haberman, B., Routhier, S., and J. Schoenwaelder, ôTextual Contentions for Internet Network Addressesö, May 2002.

10. 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 implementers 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.

11. Author's Addresses

Eduardo Cardona
Cable Television Laboratories
400 Centennial Parkway
Louisville, CO 80027
Phone: +1 303.661.9100
Email: e.cardona@cablelabs.com

Kevin Luehrs
Cable Television Laboratories
400 Centennial Parkway
Louisville, CO 80027
Phone: +1 303.661.9100
Email: k.luehrs@cablelabs.com

Scott Higgins
Ashley-Laurent
Austin, TX
Phone: +1 512.322.0676 x112
Email: shiggins@ashleylaurent.com

Doug Jones
YAS Broadband Ventures
300 Brickstone Square
Andover, MA 01810
Phone: +1 303.661.3823
Email: doug@yas.com

12. Full Copyright Statement