

Audio/Video Working Group
Internet-Draft
Expires: January 15, 2005

Alan Clark
Telchemy
Amy Pendleton
Nortel Networks

Proposed Real-Time Transport Protocol
Management Information Base Version 2
[draft-clark-avt-rtpmibv2-01.txt](#)

Status of this Memo

This document is an Internet-Draft and is subject to all provisions of [section 3 of RFC 3667](#). By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she become aware will be disclosed, in accordance with [RFC 3668](#).

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/lid-abstracts.txt>.

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

This Internet-Draft will expire on January 15, 2005.

Copyright Notice

Copyright (C) The Internet Society (2004). All Rights Reserved.

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 objects for managing Real-Time Transport Control Protocol Extended Reports (RTCP XR) VoIP Metrics ([RFC3611](#)).

Clark

Expires January 2005

[Page 1]

Table of Contents

1. The Network Management Framework	2
2. Overview	3
2.1 Components	3
2.2 Applicability of the MIB to RTP System Implementations	4
2.3 The Structure of the RTCP XR MIB	4
3 Definitions	4
4. Security Considerations	11
5. Acknowledgements	11
6. Intellectual Property	11
7. References	12
8. Authors' Addresses	14
9. Full Copyright Statement	14

[1. The SNMP Management Framework](#)

The SNMP Management Framework presently consists of five major components:

- o An overall architecture, described in [RFC 2571](#) [[RFC2571](#)].
- o 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, [RFC 2578](#), [RFC 2579](#) and [RFC 2580](#).
- o 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](#)].
- o 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](#)].
- o 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.

Clark

Expires January 2005

[Page 2]

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 (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.

2. Overview

An "RTP System" may be a host end-system that runs an application program that sends or receives RTP data packets, or it may be an intermediate-system that forwards RTP packets. RTP Control Protocol (RTCP) packets are sent by senders and receivers to convey information about RTP packet transmission and reception [[RFC3550](#)]. RTP monitors may collect RTCP information on senders and receivers to and from an RTP host or intermediate-system.

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](#).

2.1 Components

The RTCP XR MIB is structured around "Session," "Receiver" and "Sender" conceptual abstractions.

2.1.1 An RTP Session is an association of two or more participants communicating with RTP. For each participant, the session is defined by a particular pair of destination transport addresses (one network address plus a port pair for RTP and RTCP). The destination transport addresses may be common for all participants, as in the case of IP multicast, or may be different for each, as in the case of individual unicast addresses plus a common port pair," as defined in [section 3 of \[RFC3550\]](#).

2.1.2 A "Sender" is identified within an RTP session by a 32-bit numeric "Synchronization Source," or "SSRC", value and is "...the source of a stream of RTP packets" as defined in [section 3 of \[RFC3550\]](#). The sender is also a source of RTCP Sender Report packets as specified in [section 6 of \[RFC3550\]](#).

2.1.3 A "Receiver" of a "stream of RTP packets" can be a unicast or multicast Receiver as described in 2.1.1, above. An RTP Receiver has an SSRC value that is unique to the session. An RTP Receiver is a source of RTCP Receiver Reports as specified in [section 6 of \[RFC3550\]](#).

Clark

Expires January 2005

[Page 3]

2.2 Applicability of the MIB to RTP System Implementations

The RTCP XR MIB may be used in RTP Host Systems (end systems), see [section 3 of \[RFC3550\]](#) that are supporting Voice over IP (VoIP host systems).

2.2.1 VoIP host Systems are end-systems that may use the RTCP XR MIB to collect RTP Voice over IP session data that the host is sending or receiving; these data may be used by a network manager to detect and diagnose faults that occur over the lifetime of a VoIP session as in a "help-desk" scenario.

2.2.2 Monitors of RTP Voice over IP sessions may be third-party or may be located in the RTP host. Monitors may use the RTCP XR MIB to collect Voice over IP session statistical data; these data may be used by a network manager for capacity planning and other network-management purposes. A Monitor may use the RTCP XR MIB to collect data to permit a network manager to detect and diagnose faults in VoIP sessions.

2.2.3 Many host systems will want to keep track of streams beyond what they are sending and receiving. In a host monitor system, a host agent would use RTP data from the host to maintain data about streams it is sending and receiving, and RTCP data to collect data about other hosts in the session.

2.3 The Structure of the RTCP XR MIB

There is one table in the RTCP XR MIB. The rtpXrVoipTable contains objects that describe completed sessions at the host or monitor.

rtpXrVoipIndex is a global object that permits a network-management application to obtain a unique index for conceptual row creation in the rtpSessionTable. In this way the SNMP Set operation MAY be used to configure a monitor.

3. Definitions

RTCPXR-MIB DEFINITIONS ::= BEGIN

IMPORTS

Counter32, Counter64, Gauge32, mib-2, Integer32,	
MODULE-IDENTITY,	
OBJECT-TYPE, Unsigned32	FROM SNMPv2-SMI
OBJECT-GROUP, MODULE-COMPLIANCE	FROM SNMPv2-CONF
InterfaceIndex	FROM IF-MIB;

Clark

Expires January 2005

[Page 4]


```
rtcpXrMIB MODULE-IDENTITY
  LAST-UPDATED TBD
  ORGANIZATION
    "IETF AVT Working Group"
  DESCRIPTION
    "The managed objects of RTCP XR systems.
    Refer to RFC 3611, Real Time Control Protocol Extended
    Reports (RTCP XR) Section 4.7 VoIP Metrics"
  REVISION    TBD
  DESCRIPTION "Initial version of this MIB.
    Published as draft-clark-avt-rtpmibv2-01.txt."

 ::= { mib-2 TBD }

--
-- OBJECTS
--
rtcpXrMIBObjects OBJECT IDENTIFIER ::= { rtcpXrMIB 1 }
rtcpXrConformance OBJECT IDENTIFIER ::= { rtcpXrMIB 2 }

--
-- RTCP Extended Reports - Voice over IP Metrics
--

rtcpXrVoipTable OBJECT-TYPE
  SYNTAX SEQUENCE OF rtcpXrVoipEntry
  ACCESS not-accessible
  STATUS mandatory
  DESCRIPTION
    "Table of information about a receiver or receivers of RTCP XR
    session data. RTP hosts that receive RTCP XR session packets
    MUST create an entry in this table for that receiver/sender
    pair. RTP hosts that send RTCP XR session packets MAY create
    an entry in this table for each receiver to their stream
    using RTCP XR feedback from the RTP group. "
  ::= { rtcpXrMIBObjects 1 }

rtcpXrVoipEntry OBJECT-TYPE
  SYNTAX rtcpXrVoipEntry
  ACCESS not-accessible
  STATUS mandatory
  DESCRIPTION
    "An entry in the table of call records. A row in this table
    is created for each RTP session endpoint participating."
  INDEX { rtcpXrVoipIndex }
  ::= { rtcpXrVoipTable 1 }

rtcpXrVoipEntry ::= SEQUENCE {
  rtcpXrVoipIndex          INTEGER,
  rtcpXrVoipCallIdentifier OCTET STRING,
  rtcpXrVoipSourceIPAddress IpAddress,
```

rtcpXrVoipSourcePort

INTEGER,

Clark

Expires January 2005

[Page 5]

```
    rtcpXrVoipVocoderType          INTEGER,
    rtcpXrVoipCallDurationMs       INTEGER,
    rtcpXrVoipNetworkLossRate     INTEGER,
    rtcpXrVoipAverageDiscardRate  INTEGER,
    rtcpXrVoipBurstLossDensity    INTEGER,
    rtcpXrVoipBurstLenMs          INTEGER,
    rtcpXrVoipGapLossDensity      INTEGER,
    rtcpXrVoipGapLenMs            INTEGER,
    rtcpXrVoipAverageOneWayDelay   INTEGER,
    rtcpXrVoipEndSystemDelay       INTEGER,
    rtcpXrVoipNoiseLeveldBm       INTEGER,
    rtcpXrVoipSignalLeveldBm      INTEGER,
    rtcpXrVoipLocalRERLdB         INTEGER,
    rtcpXrVoipConversationalRCQ    INTEGER,
    rtcpXrVoipListeningMOSLQ      INTEGER,
    rtcpXrVoipConversationalMOSCQ INTEGER,
    rtcpXrVoipPlcType             INTEGER,
    rtcpXrVoipJitterBufferAdaptationMode INTEGER,
    rtcpXrVoipJitterBufferAdaptationRate INTEGER,
    rtcpXrVoipJitterBufferAverageDelay INTEGER,
    rtcpXrVoipJitterBufferMaximumDelay INTEGER,
    rtcpXrVoipJitterBufferSize    INTEGER
}
```

```
rtcpXrVoipIndex OBJECT-TYPE
    SYNTAX INTEGER (0..65535)
    ACCESS read-only
    STATUS mandatory
    DESCRIPTION
        "Index for this call."
    ::= { rtcpXrVoipEntry 1 }
```

```
rtcpXrVoipCallIdentifier OBJECT-TYPE
    SYNTAX OCTET STRING
    ACCESS read-only
    STATUS mandatory
    DESCRIPTION
        "Call identifier for this call (= SDES?)."
    ::= { rtcpXrVoipEntry 2 }
```

```
rtcpXrVoipSourceIPAddress OBJECT-TYPE
    SYNTAX IpAddress
    ACCESS read-only
    STATUS mandatory
    DESCRIPTION
        "Source IP address for this session."
    ::= { rtcpXrVoipEntry 3 }
```

```
rtcpXrVoipSourcePort OBJECT-TYPE
    SYNTAX INTEGER
    ACCESS read-only
    STATUS mandatory
```

DESCRIPTION

"Source UDP Port for this call."

Clark

Expires January 2005

[Page 6]

::= { rtcpXrVoipEntry 4 }

rtcpXrVoipVocoderType OBJECT-TYPE

SYNTAX INTEGER

ACCESS read-only

STATUS mandatory

DESCRIPTION

"Vocoder type used on this call."

::= { rtcpXrVoipEntry 5 }

rtcpXrVoipCallDurationMs OBJECT-TYPE

SYNTAX INTEGER

ACCESS read-only

STATUS mandatory

DESCRIPTION

"Duration of call in milliseconds."

::= { rtcpXrVoipEntry 6 }

rtcpXrVoipNetworkLossRate OBJECT-TYPE

SYNTAX INTEGER

ACCESS read-only

STATUS mandatory

DESCRIPTION

"Average rate of network packet loss (see [RFC3611 Section 4.7](#))."

::= { rtcpXrVoipEntry 7 }

rtcpXrVoipAverageDiscardRate OBJECT-TYPE

SYNTAX INTEGER

ACCESS read-only

STATUS mandatory

DESCRIPTION

"Average rate of discards due to jitter(see [RFC3611 Section 4.7](#))."

::= { rtcpXrVoipEntry 8 }

rtcpXrVoipBurstLossDensity OBJECT-TYPE

SYNTAX INTEGER

ACCESS read-only

STATUS mandatory

DESCRIPTION

"Density of loss and discarded packets during burst periods.
(see [RFC3611 Section 4.7](#))"

::= { rtcpXrVoipEntry 9 }

rtcpXrVoipBurstLenMs OBJECT-TYPE

SYNTAX INTEGER

ACCESS read-only

STATUS mandatory

DESCRIPTION

"Average length of bursts in milliseconds (see [RFC3611 Section 4.7](#))."

::= { rtcpXrVoipEntry 10 }

rtcpXrVoipGapLossDensity OBJECT-TYPE

ACCESS read-only
STATUS mandatory
DESCRIPTION
 "Density of loss and discarded packets during gap periods
 (see [RFC3611 Section 4.7](#))."
::= { rtcpXrVoipEntry 11 }

rtcpXrVoipGapLenMs OBJECT-TYPE
SYNTAX INTEGER
ACCESS read-only
STATUS mandatory
DESCRIPTION
 "Average length of gaps in milliseconds (see [RFC3611 Section 4.7](#))."
::= { rtcpXrVoipEntry 12 }

rtcpXrVoipAverageOneWayDelay OBJECT-TYPE
SYNTAX INTEGER
ACCESS read-only
STATUS mandatory
DESCRIPTION
 "Average (symmetric) one way RTCP delay on call. A value of zero may
 indicate that this value has not yet been determined.
 (see [RFC3611 Section 4.7](#))."
::= { rtcpXrVoipEntry 13 }

rtcpXrVoipEndSystemDelay OBJECT-TYPE
SYNTAX INTEGER
ACCESS read-only
STATUS mandatory
DESCRIPTION
 "Average end system delay on call. A value of zero may
 indicate that this value has not yet been determined
 (see [RFC3611 Section 4.7](#))."
::= { rtcpXrVoipEntry 14 }

rtcpXrVoipNoiseLeveldBm OBJECT-TYPE
SYNTAX INTEGER
ACCESS read-only
STATUS mandatory
DESCRIPTION
 "Measured received silent period noise level in dBm
 (see [RFC3611 Section 4.7](#))."
::= { rtcpXrVoipEntry 15 }

rtcpXrVoipSignalLeveldBm OBJECT-TYPE
SYNTAX INTEGER
ACCESS read-only
STATUS mandatory
DESCRIPTION
 "Measured received signal level during talkspurts in dBm
 (see [RFC3611 Section 4.7](#))."
::= { rtcpXrVoipEntry 16 }

Clark

Expires January 2005

[Page 8]

rtcpXrVoipLocalRERLdB OBJECT-TYPE

SYNTAX INTEGER

ACCESS read-only

STATUS mandatory

DESCRIPTION

"Residual Echo Return Loss measured at this endpoint
(see [RFC3611 Section 4.7](#))."

::= { rtcpXrVoipEntry 17 }

rtcpXrVoipConversationalRCQ OBJECT-TYPE

SYNTAX INTEGER

ACCESS read-only

STATUS mandatory

DESCRIPTION

"Conversational quality R factor for this call
(see [RFC3611 Section 4.7](#))."

::= { rtcpXrVoipEntry 18 }

rtcpXrVoipListeningMOSLQ OBJECT-TYPE

SYNTAX INTEGER

ACCESS read-only

STATUS mandatory

DESCRIPTION

"Estimated listening quality MOS for this call
(see [RFC3611 Section 4.7](#))."

::= { rtcpXrVoipEntry 19 }

rtcpXrVoipConversationalMOSCQ OBJECT-TYPE

SYNTAX INTEGER

ACCESS read-only

STATUS mandatory

DESCRIPTION

"Estimated conversational quality MOS for this call
(see [RFC3611 Section 4.7](#))."

::= { rtcpXrVoipEntry 20 }

rtcpXrVoipPlcType OBJECT-TYPE

SYNTAX INTEGER { disabled(1),
enhanced(2),
standard(3),
unspecified (4)}

ACCESS read-only

STATUS mandatory

DESCRIPTION

"Defines type of packet loss concealment used on this call
(see [RFC3611 Section 4.7](#))."

::= { rtcpXrVoipEntry 21 }

rtcpXrVoipJitterBufferAdaptationMode OBJECT-TYPE

SYNTAX INTEGER { reserved (1),
nonAdaptive (2),
adaptive (3),

Clark

Expires January 2005

[Page 9]

```

        unknown (4) }
ACCESS read-only
STATUS mandatory
DESCRIPTION
    "Defines if jitter buffer is in fixed or adaptive mode
    (see RFC3611 Section 4.7)."
```

rtcpXrVoipEntry 22 }

```
rtcpXrVoipJitterBufferAdaptationRate OBJECT-TYPE
    SYNTAX INTEGER
    ACCESS read-only
    STATUS mandatory
    DESCRIPTION
        "Estimated adaptation rate of jitter buffer
        (see RFC3611 Section 4.7)."
```

rtcpXrVoipEntry 23 }

```
rtcpXrVoipJitterBufferAverageDelay OBJECT-TYPE
    SYNTAX INTEGER
    ACCESS read-only
    STATUS mandatory
    DESCRIPTION
        "Average size of jitter buffer in mS
        (see RFC3611 Section 4.7)."
```

rtcpXrVoipEntry 24 }

```
rtcpXrVoipJitterBufferMaximumDelay OBJECT-TYPE
    SYNTAX INTEGER
    ACCESS read-only
    STATUS mandatory
    DESCRIPTION
        "Maximum delay through jitter buffer at current size in mS
        (see RFC3611 Section 4.7)."
```

rtcpXrVoipEntry 25 }

```
rtcpXrVoipJitterBufferSize OBJECT-TYPE
    SYNTAX INTEGER
    ACCESS read-only
    STATUS mandatory
    DESCRIPTION
        "Absolute maximum size jitter buffer can reach in mS
        (see RFC3611 Section 4.7)."
```

rtcpXrVoipEntry 26 }

END

4. Security Considerations

In most cases, MIBs are not themselves security risks; if SNMP security is operating as intended, the use of a MIB to view information about a system, or to change some parameter at the system, is a tool, not a threat.

None of the read-only objects in this MIB reports a password, though some SDES [[RFC3550](#)] items such as the CNAME [[RFC3550](#)], the canonical name, may be deemed sensitive depending on the security policies of a particular enterprise. If access to these objects is not limited by an appropriate access control policy, these objects can provide an attacker with information about a system's configuration and the services that that system is providing. Some enterprises view their network and system configurations, as well as information about usage and performance, as corporate assets; such enterprises may wish to restrict SNMP access to most of the objects in the MIB.

Confidentiality of RTP and RTCP data packets is defined in [section 9](#) of the RTP specification [[RFC3550](#)]. Encryption may be performed on RTP packets, RTCP packets, or both. Encryption of RTCP packets may pose a problem for third-party monitors though "For RTCP, it is allowed to split a compound RTCP packet into two lower-layer packets, one to be encrypted and one to be sent in the clear. For example, SDES information might be encrypted while reception reports were sent in the clear to accommodate third-party monitors [[RFC3550](#)]."

SNMPv1 by itself is not a secure environment. Even if the network itself is secure (for example by using IPSec), 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.

5. Acknowledgements

6. 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

Clark

Expires January 2005

[Page 11]

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.

7. References

- [RFC3550] Shulzrinne, H., Casner, S., Frederick, R. and V. Jacobson, "RTP: A Transport Protocol for real-time applications," [RFC 3550](#), July 2003.
- [RFC3611] Friedman, T., Caceres, R., Clark, A., "RTP Control Protocol Reporting Extensions (RTCP XR)," [RFC 3611](#), [October/November] 2003
- [RFC2571] Harrington, D., Presuhn, R. and B. Wijnen, "An Architecture for Describing SNMP Management Frameworks", [RFC 2571](#), December 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] Rose, M., "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](#), December 1999.
- [RFC2579] McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M. and S. Waldbusser, "Textual Conventions for SMIv2", STD 58, [RFC 2579](#), December 1999.
- [RFC2580] McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M. and S. Waldbusser, "Conformance Statements for SMIv2", STD 58, [RFC 2580](#), December 1999.
- [RFC1157] Case, J., Fedor, M., Schoffstall, M. and J. Davin, "Simple Network Management Protocol", STD 15, [RFC 1157](#),

May 1990.

Clark

Expires January 2005

[Page 12]

- [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](#), December 1999.
- [RFC2574] Blumenthal, U. and B. Wijnen, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)", [RFC 2574](#), December 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](#), December 1999.
- [RFC2575] Wijnen, B., Presuhn, R. and K. McCloghrie, "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)", [RFC 2575](#), December 1999.
- [RFC2570] Case, J., Mundy, R., Partain, D. and B. Stewart, "Introduction to Version 3 of the Internet-standard Network Management Framework", [RFC 2570](#), December 1999.

Clark

Expires January 2005

[Page 13]

8. Authors' Addresses

Alan Clark
Telchemy Incorporated
3360 Martins Farm Road, Ste 200
Suwanee, Georgia 30024
U.S.A.

Email: alan@telchemy.com

Amy Pendleton
Nortel Networks
2380 Performance Drive
Richardson, Texas 75081
U.S.A.

Email: aspen@nortelnetworks.com

9. Full Copyright Statement

Copyright (C) The Internet Society (2004). This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Clark

Expires January 2005

[Page 14]