

Network Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: May 3, 2012

R. Bush  
Internet Initiative Japan  
B. Wijnen  
RIPE NCC  
K. Patel  
Cisco Systems  
M. Baer  
SPARTA  
October 31, 2011

Definitions of Managed Objects for the RPKI-Router Protocol  
draft-ymbk-rpki-rtr-protocol-mib-02

## Abstract

This document defines a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. In particular, it describes objects used for monitoring the RPKI Router protocol.

## Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

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."

This Internet-Draft will expire on May 3, 2012.

## Copyright Notice

Copyright (c) 2011 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect

---

Internet-Draft    MIB Module for the RPKI-Router Protocol    October 2011

to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

<a href="#">1.</a>	<a href="#">Introduction . . . . .</a>	<a href="#">3</a>
<a href="#">1.1.</a>	<a href="#">Requirements Language . . . . .</a>	<a href="#">3</a>
<a href="#">2.</a>	<a href="#">Internet-Standard Management Framework . . . . .</a>	<a href="#">3</a>
<a href="#">3.</a>	<a href="#">Overview . . . . .</a>	<a href="#">3</a>
<a href="#">4.</a>	<a href="#">Definitions . . . . .</a>	<a href="#">4</a>
<a href="#">5.</a>	<a href="#">IANA Considerations . . . . .</a>	<a href="#">20</a>
<a href="#">6.</a>	<a href="#">Security Considerations . . . . .</a>	<a href="#">21</a>
<a href="#">7.</a>	<a href="#">References . . . . .</a>	<a href="#">21</a>
<a href="#">7.1.</a>	<a href="#">Normative References . . . . .</a>	<a href="#">21</a>
<a href="#">7.2.</a>	<a href="#">Informative References . . . . .</a>	<a href="#">22</a>
	<a href="#">Authors' Addresses . . . . .</a>	<a href="#">22</a>

---

Internet-Draft    MIB Module for the RPKI-Router Protocol    October 2011

## [1.](#) Introduction

This document defines a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. In particular, it defines objects used for monitoring the RPKI Router protocol [[I-D.ietf-sidr-rpki-rtr](#)].

### [1.1.](#) Requirements Language

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](#) [[RFC2119](#)].

## [2.](#) 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 \[RFC3410\]](#). 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 document specifies a MIB module that is compliant to the SMIV2, which is described in STD 58, [[RFC2578](#)], STD 58, [[RFC2579](#)] and STD 58, [[RFC2580](#)].

## [3.](#) Overview

The objects defined in this document are used to monitor the RPKI Router protocol [[I-D.ietf-sidr-rpki-rtr](#)]. The MIB module defined in this draft is broken into these tables: the RPKI Router Cache Server (connection) Table, the RPKI Router Cache Server Errors Table, and the RPKI Router Prefix Origin Table.



TEXTUAL-CONVENTION, TimeStamp  
FROM SNMPv2-TC -- [RFC2579](#)

MODULE-COMPLIANCE, OBJECT-GROUP, NOTIFICATION-GROUP  
FROM SNMPv2-CONF -- [RFC2580](#)

LongUtf8String FROM SYSAPPL-MIB -- [RFC2287](#)

;

rpkiRtrMIB MODULE-IDENTITY  
LAST-UPDATED "201110140000Z"  
ORGANIZATION "IETF Secure Inter-Domain Routing (SIDR)  
Working Group  
"  
CONTACT-INFO "Working Group Email: [sidr@ietf.org](mailto:sidr@ietf.org)  
  
Randy Bush

Bush, et al.

Expires May 3, 2012

[Page 4]

---

Internet-Draft MIB Module for the RPKI-Router Protocol October 2011

Internet Initiative Japan  
5147 Crystal Springs  
Bainbridge Island, Washington, 98110  
USA  
Email: [randy@psg.com](mailto:randy@psg.com)

Bert Wijnen  
RIPE NCC  
Schagen 33  
3461 GL Linschoten  
Netherlands  
Email: [bertietf@bwijnen.net](mailto:bertietf@bwijnen.net)

Keyur Patel  
Cisco Systems  
170 W. Tasman Drive  
San Jose, CA 95134  
USA  
Email: [keyupate@cisco.com](mailto:keyupate@cisco.com)

Michael Baer  
SPARTA

P.O. Box 72682  
Davis, CA 95617  
USA  
Email: michael.baer@sparta.com  
"

DESCRIPTION "This MIB module contains management objects to support monitoring of the Resource Public Key Infrastructure (RPKI) protocol on routers.

Copyright (c) 2011 IETF Trust and the persons identified as authors of the code. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, is permitted pursuant to, and subject to the license terms contained in, the Simplified BSD License set forth in [Section 4.c](#) of the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>).

This version of this MIB module is part of RFCxxxx; see the RFC itself for full legal notices.  
"

REVISION "201110140000Z"

DESCRIPTION "Initial version, published as RFCxxxx."

-- Note to RFC Editor: pls fill in above (2 times) RFC

-- number for xxxx and delete these 2 lines.

::= { mib-2 XXX } -- XXX to be assigned by IANA

rpkiRtrNotifications OBJECT IDENTIFIER ::= { rpkiRtrMIB 0 }

rpkiRtrObjects OBJECT IDENTIFIER ::= { rpkiRtrMIB 1 }

rpkiRtrConformance OBJECT IDENTIFIER ::= { rpkiRtrMIB 2 }

-- =====  
-- Textual Conventions used in this MIB module  
-- =====

RpkiRtrConnectionType ::= TEXTUAL-CONVENTION

```

STATUS      current
DESCRIPTION "The connection type or transport security suite
            (transport plus security mecahnism) used between
            a router (as a client) and a cache server.

            The following types have been defined in RFCnnnn:
-- RFC Editor: pls fill out RFCnnnn number that will be or has
--              been assigned to draft-ietf-sidr-rpki-rtr-nn.txt
            ssh(1)    - sect 7.1, see also RFC4252.
            tls(2)    - sect 7.2, see also RFC5246.
            tcpMD5(3) - sect 7.3, see also RFC2385.
            tcpA0(4)  - sect 7.4, see also RFC5925.
            tcp(5)    - sect 7.
            ipsec(6)   - sect 7, see also RFC4301.
            other(7)  - non of the above
            "
REFERENCE    "The RPKI/Rtr Protocol, RFCnnnn - section 7"
-- RFC Editor: pls fill out RFCnnnn number that will be or has been
--              assigned to draft-ietf-sidr-rpki-rtr-nn.txt
SYNTAX      INTEGER {
                ssh(1),
                tls(2),
                tcpMD5(3),
                tcpA0(4),
                tcp(5),
                ipsec(6),
                other(7)
            }

-- =====
-- Scalar objects
-- =====
rpkiRtrDiscontinuityTimer OBJECT-TYPE

```

```

SYNTAX      TimeStamp
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION "This timer represents the timestamp (value
            of sysUpTime) at which time any of the
            Counter32 ojects in this MIB module
            encountered a discontinuity.

```

```

                In principle that should only happen if the
                SNMP agent or the instrumentation for this
                MIB module (re-)starts."
 ::= { rpkiRtrObjects 1 }

-- =====
-- RPKI Router Cache Server Connection Table
-- =====

rpkiRtrCacheServerTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF RpkiRtrCacheServerTableEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "This table lists the RPKI cache servers
                  known to this router/system."
    ::= { rpkiRtrObjects 2 }

rpkiRtrCacheServerTableEntry OBJECT-TYPE
    SYNTAX      RpkiRtrCacheServerTableEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "An entry in the rpkiRtrCacheServerTable.
                  It holds management attributes associated
                  with one connection to a RPKI cache server."
    INDEX       { rpkiRtrCacheServerAddressType,
                  rpkiRtrCacheServerRemoteAddress,
                  rpkiRtrCacheServerRemotePort
                }
    ::= { rpkiRtrCacheServerTable 1 }

RpkiRtrCacheServerTableEntry ::= SEQUENCE {
    rpkiRtrCacheServerAddressType      InetAddressType,
    rpkiRtrCacheServerRemoteAddress    InetAddress,
    rpkiRtrCacheServerRemotePort       InetPortNumber,
    rpkiRtrCacheServerLocalAddress     InetAddress,
    rpkiRtrCacheServerLocalPort        InetPortNumber,
    rpkiRtrCacheServerPreference       Unsigned32,
    rpkiRtrCacheServerConnectionType   RpkiRtrConnectionType,
    rpkiRtrCacheServerConnectionStatus INTEGER,
    rpkiRtrCacheServerDescription      LongUtf8String,

```



```

rpkiRtrCacheServerMsgsSent          Counter32,
rpkiRtrCacheServerV4ActiveRecords   Gauge32,
rpkiRtrCacheServerV4Announcements   Counter32,
rpkiRtrCacheServerV4Withdrawals     Counter32,
rpkiRtrCacheServerV6ActiveRecords   Gauge32,
rpkiRtrCacheServerV6Announcements   Counter32,
rpkiRtrCacheServerV6Withdrawals     Counter32,
rpkiRtrCacheServerLatestSerial       Unsigned32,
rpkiRtrCacheServerNonce              Unsigned32,
rpkiRtrCacheServerRefreshTimer       Unsigned32,
rpkiRtrCacheServerTimeToRefresh      Integer32,
rpkiRtrCacheServerId                Unsigned32
}

rpkiRtrCacheServerAddressType OBJECT-TYPE
    SYNTAX      InetAddressType { ipv4(1), ipv6 (2) }
    MAX-ACCESS   not-accessible
    STATUS      current
    DESCRIPTION  "The network address type of the connection
                  to this RPKI cache server.

                  Only IPv4 and IPv6 are supported."
    ::= { rpkiRtrCacheServerTableEntry 1 }

rpkiRtrCacheServerRemoteAddress OBJECT-TYPE
    SYNTAX      InetAddress (SIZE(4|16))
    MAX-ACCESS   not-accessible
    STATUS      current
    DESCRIPTION  "The remote network address for this connection
                  to this RPKI cache server.

                  The format of the address is defined by the
                  value of the corresponding instance of
                  rpkiRtrCacheServerAddressType."
    ::= { rpkiRtrCacheServerTableEntry 2 }

rpkiRtrCacheServerRemotePort OBJECT-TYPE
    SYNTAX      InetPortNumber (1..65535)
    MAX-ACCESS   not-accessible
    STATUS      current
    DESCRIPTION  "The remote port number for this connection
                  to this RPKI cache server."
    ::= { rpkiRtrCacheServerTableEntry 3 }

rpkiRtrCacheServerLocalAddress OBJECT-TYPE
    SYNTAX      InetAddress (SIZE(4|16))
    MAX-ACCESS   read-only

```

```
STATUS          current
DESCRIPTION "The local network address for this connection
            to this RPKI cache server.

            The format of the address is defined by the
            value of the corresponding instance of
            rpkiRtrCacheServerAddressType."
::= { rpkiRtrCacheServerTableEntry 4 }

rpkiRtrCacheServerLocalPort OBJECT-TYPE
SYNTAX          InetPortNumber (1..65535)
MAX-ACCESS      read-only
STATUS          current
DESCRIPTION "The local port number for this connection
            to this RPKI cache server."
::= { rpkiRtrCacheServerTableEntry 5 }

rpkiRtrCacheServerPreference OBJECT-TYPE
SYNTAX          Unsigned32 (0..255)
MAX-ACCESS      read-only
STATUS          current
DESCRIPTION "The routers' preference for this
            RPKI cache server.

            A lower value means more preferred. If two
            entries have the same preference, then the
            order is arbitrary.

            If no order is specified in the configuration
            then this value is set to 255."
REFERENCE       "The RPKI/Rtr Protocol, RFCnnnn - section 8."
-- RFC-Editor: pls update RFCnnnn with the actual RFC number
--              assigned to draft-ietf-sidr-rpki-rtr-nn.txt
::= { rpkiRtrCacheServerTableEntry 6 }

rpkiRtrCacheServerConnectionType OBJECT-TYPE
SYNTAX          RpkiRtrConnectionType
MAX-ACCESS      read-only
STATUS          current
DESCRIPTION "The connection type or transport security suite
            in use for this RPKI cache server."
::= { rpkiRtrCacheServerTableEntry 7 }

rpkiRtrCacheServerConnectionStatus OBJECT-TYPE
SYNTAX          INTEGER { up(1), down(2) }
MAX-ACCESS      read-only
```

STATUS current  
DESCRIPTION "The connection status for this entry"

(connection to this RPKI cache server)."  
::= { rpkIRtrCacheServerTableEntry 8 }

rpkiRtrCacheServerDescription OBJECT-TYPE  
SYNTAX LongUtf8String  
MAX-ACCESS read-only  
STATUS current  
DESCRIPTION "Free form description/information for this  
connection to this RPKI cache server."  
::= { rpkIRtrCacheServerTableEntry 9 }

rpkiRtrCacheServerMsgsReceived OBJECT-TYPE  
SYNTAX Counter32  
MAX-ACCESS read-only  
STATUS current  
DESCRIPTION "Number of messages received from this  
RPKI cache server via this connection.  
  
Discontinuities are indicated by the value  
of rpkIRtrDiscontinuityTimer."  
::= { rpkIRtrCacheServerTableEntry 10 }

rpkiRtrCacheServerMsgsSent OBJECT-TYPE  
SYNTAX Counter32  
MAX-ACCESS read-only  
STATUS current  
DESCRIPTION "Number of messages sent to this  
RPKI cache server via this connection.  
  
Discontinuities are indicated by the value  
of rpkIRtrDiscontinuityTimer."  
::= { rpkIRtrCacheServerTableEntry 11 }

rpkiRtrCacheServerV4ActiveRecords OBJECT-TYPE  
SYNTAX Gauge32  
MAX-ACCESS read-only  
STATUS current  
DESCRIPTION "Number of active IPv4 records received from  
this RPKI cache server via this connection."

::= { rpkiRtrCacheServerTableEntry 12 }

rpkiRtrCacheServerV4Announcements OBJECT-TYPE

SYNTAX Counter32

MAX-ACCESS read-only

STATUS current

DESCRIPTION "The number of IPv4 records announced by the  
RPKI cache Server via this connection."

Discontinuities are indicated by the value  
of rpkiRtrDiscontinuityTimer."

::= { rpkiRtrCacheServerTableEntry 13 }

rpkiRtrCacheServerV4Withdrawals OBJECT-TYPE

SYNTAX Counter32

MAX-ACCESS read-only

STATUS current

DESCRIPTION "The number of IPv4 records withdrawn by the  
RPKI cache Server via this connection."

Discontinuities are indicated by the value  
of rpkiRtrDiscontinuityTimer."

::= { rpkiRtrCacheServerTableEntry 14 }

rpkiRtrCacheServerV6ActiveRecords OBJECT-TYPE

SYNTAX Gauge32

MAX-ACCESS read-only

STATUS current

DESCRIPTION "Number of active IPv6 records received from  
this RPKI cache server via this connection."

::= { rpkiRtrCacheServerTableEntry 15 }

rpkiRtrCacheServerV6Announcements OBJECT-TYPE

SYNTAX Counter32

MAX-ACCESS read-only

STATUS current

DESCRIPTION "The number of IPv6 records announced by the  
RPKI cache Server via this connection."

Discontinuities are indicated by the value  
of rpkiRtrDiscontinuityTimer."

```
::= { rpkiRtrCacheServerTableEntry 16 }
```

```
rpkiRtrCacheServerV6Withdrawals OBJECT-TYPE
```

```
SYNTAX Counter32
```

```
MAX-ACCESS read-only
```

```
STATUS current
```

```
DESCRIPTION "The number of IPv6 records withdrawn by the  
RPKI cache Server via this connection.
```

```
Discontinuities are indicated by the value  
of rpkiRtrDiscontinuityTimer."
```

```
::= { rpkiRtrCacheServerTableEntry 17 }
```

```
rpkiRtrCacheServerLatestSerial OBJECT-TYPE
```

```
SYNTAX Unsigned32
```

```
MAX-ACCESS read-only
```

```
STATUS current
```

```
DESCRIPTION "The latest serial number of data received from  
this RPKI server on this connection.
```

```
Note: this value wraps back to zero when it  
reaches its maximum value."
```

```
REFERENCE "RFCnnnn section 2 and RFC1982"
```

```
-- RFC-Editor: please fill out nnnn with the RFC number assigned  
-- to draft-ietf-sidr-rpki-rtr-nn.txt
```

```
::= { rpkiRtrCacheServerTableEntry 18 }
```

```
rpkiRtrCacheServerNonce OBJECT-TYPE
```

```
SYNTAX Unsigned32 (0..65535)
```

```
MAX-ACCESS read-only
```

```
STATUS current
```

```
DESCRIPTION "The nonce associated with the RPKI cache server  
at the other end of this connection."
```

```
REFERENCE "RFCnnnn section 2"
```

```
::= { rpkiRtrCacheServerTableEntry 19 }
```

```
rpkiRtrCacheServerRefreshTimer OBJECT-TYPE
```

```
SYNTAX Unsigned32 (60..7200)
```

```
UNITS "seconds"
```

```
MAX-ACCESS read-only
```

```
STATUS current
```

DESCRIPTION "The number of seconds configured for the refresh timer for this connection to this RPKI cache server."

::= { rpkiRtrCacheServerTableEntry 20 }

rpkiRtrCacheServerTimeToRefresh OBJECT-TYPE

SYNTAX Integer32

UNITS "seconds"

MAX-ACCESS read-only

STATUS current

DESCRIPTION "The number of seconds remaining before a new refresh is performed via a Serial Query to this cache server over this connection."

A negative value means that the refresh time has passed this many seconds and the refresh has not yet been completed.

Upon a completed refresh (i.e. a successful rnd complete esponse to a Serial Query) the value of this attribute will be re-initialized with the value of the corresponding rpkiRtrCacheServerRefreshTimer attribute."

::= { rpkiRtrCacheServerTableEntry 21 }

rpkiRtrCacheServerId OBJECT-TYPE

SYNTAX Unsigned32 (1..4294967295)

MAX-ACCESS read-only

STATUS current

DESCRIPTION "The unique ID for this connection."

An implementation must make sure this ID is unique within this table. It is this ID that can be used to find entries in the rpkiRtrPrefixOriginTable that were created by announcements received on this connection from this cache server."

::= { rpkiRtrCacheServerTableEntry 22 }

-- =====  
-- Errors Table  
-- =====

```

rpkiRtrCacheServerErrorsTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF RpkiRtrCacheServerErrorsTableEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "This table provides statistics on errors per
                  RPKI peer connection. These can be used for
                  debugging."
    ::= { rpkiRtrObjects 3 }

```

```

rpkiRtrCacheServerErrorsTableEntry OBJECT-TYPE
    SYNTAX      RpkiRtrCacheServerErrorsTableEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "An entry in the rpkiCacheServerErrorTable. It holds
                  management objects associated with errors that
                  were detected for the specified connection to
                  a specific cache server."
    AUGMENTS     { rpkiRtrCacheServerTableEntry }
    ::= { rpkiRtrCacheServerErrorsTable 1 }

```

```

RpkiRtrCacheServerErrorsTableEntry ::= SEQUENCE {
    rpkiRtrCacheServerErrorsCorruptData      Counter32,
    rpkiRtrCacheServerErrorsInternalError    Counter32,
    rpkiRtrCacheServerErrorsNoData           Counter32,
    rpkiRtrCacheServerErrorsInvalidRequest   Counter32,
    rpkiRtrCacheServerErrorsUnsupportedVersion Counter32,
    rpkiRtrCacheServerErrorsUnsupportedPdu   Counter32,
    rpkiRtrCacheServerErrorsWithdrawalUnknown Counter32,
    rpkiRtrCacheServerErrorsDuplicateAnnounce Counter32
}

```

```

}

```

```

rpkiRtrCacheServerErrorsCorruptData OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "The number of 'Corrupt Data' errors received
                  from the RPKI cache server at the other end
                  of this connection.

```

Discontinuities are indicated by the value

of rpkIRtrDiscontinuityTimer."  
 ::= { rpkIRtrCacheServerErrorsTableEntry 1 }

rpkiRtrCacheServerErrorsInternalError OBJECT-TYPE

SYNTAX Counter32  
MAX-ACCESS read-only  
STATUS current  
DESCRIPTION "The number of 'Internal Error' errors received  
from the RPKI cache server at the other end  
of this connection.

Discontinuities are indicated by the value  
of rpkIRtrDiscontinuityTimer."

::= { rpkIRtrCacheServerErrorsTableEntry 2 }

rpkiRtrCacheServerErrorsNoData OBJECT-TYPE

SYNTAX Counter32  
MAX-ACCESS read-only  
STATUS current  
DESCRIPTION "The number of 'No Data Available' errors received  
from the RPKI cache server at the other end  
of this connection.

Discontinuities are indicated by the value  
of rpkIRtrDiscontinuityTimer."

::= { rpkIRtrCacheServerErrorsTableEntry 3 }

rpkiRtrCacheServerErrorsInvalidRequest OBJECT-TYPE

SYNTAX Counter32  
MAX-ACCESS read-only  
STATUS current  
DESCRIPTION "The number of 'Invalid Request' errors received  
from the RPKI cache server at the other end  
of this connection.

Discontinuities are indicated by the value  
of rpkIRtrDiscontinuityTimer."

::= { rpkIRtrCacheServerErrorsTableEntry 4 }

rpkiRtrCacheServerErrorsUnsupportedVersion OBJECT-TYPE

SYNTAX Counter32



MAX-ACCESS read-only  
STATUS current  
DESCRIPTION "The number of 'Unsupported Protocol Version' errors received from the RPKI cache server at the other end of this connection.

Discontinuities are indicated by the value of rpkIRtrDiscontinuityTimer."

::= { rpkIRtrCacheServerErrorsTableEntry 5 }

rpkiRtrCacheServerErrorsUnsupportedPdu OBJECT-TYPE

SYNTAX Counter32  
MAX-ACCESS read-only  
STATUS current  
DESCRIPTION "The number of 'Unsupported PDU Type' errors received from the RPKI cache server at the other end of this connection.

Discontinuities are indicated by the value of rpkIRtrDiscontinuityTimer."

::= { rpkIRtrCacheServerErrorsTableEntry 6 }

rpkiRtrCacheServerErrorsWithdrawalUnknown OBJECT-TYPE

SYNTAX Counter32  
MAX-ACCESS read-only  
STATUS current  
DESCRIPTION "The number of 'Withdrawal of Unknown Record' errors received from the RPKI cache server at the other end of this connection.

Discontinuities are indicated by the value of rpkIRtrDiscontinuityTimer."

::= { rpkIRtrCacheServerErrorsTableEntry 7 }

rpkiRtrCacheServerErrorsDuplicateAnnounce OBJECT-TYPE

SYNTAX Counter32  
MAX-ACCESS read-only  
STATUS current  
DESCRIPTION "The number of 'Duplicate Announcement Received' errors received from the RPKI cache server at the other end of this connection.

Discontinuities are indicated by the value of rpkIRtrDiscontinuityTimer."

```
::= { rpkiRtrCacheServerErrorsTableEntry 8 }
```

```
-- =====
-- The rpkiRtrPrefixOriginTable (was referred to as ROATable in an
-- earlier version of this table)
-- =====
```

```
rpkiRtrPrefixOriginTable OBJECT-TYPE
```

```
SYNTAX          SEQUENCE OF RpkiRtrPrefixOriginTableEntry
MAX-ACCESS      not-accessible
STATUS          current
DESCRIPTION     "This table lists the prefixes that were
                  announced by RPKI cache servers to this system.
                  That is the prefixes and their Origin ASN
                  as recieved by announcements via the
                  rpki-rtr protocol."
```

```
::= { rpkiRtrObjects 4 }
```

```
rpkiRtrPrefixOriginTableEntry OBJECT-TYPE
```

```
SYNTAX          RpkiRtrPrefixOriginTableEntry
MAX-ACCESS      not-accessible
STATUS          current
DESCRIPTION     "An entry in the rpkiRtrPrefixOriginTable.
                  This represents one announced prefix."
```

```
INDEX          { rpkiRtrPrefixOriginAddressType,
                  rpkiRtrPrefixOriginAddress,
                  rpkiRtrPrefixOriginMinLength
                }
```

```
::= { rpkiRtrPrefixOriginTable 1 }
```

```
RpkiRtrPrefixOriginTableEntry ::= SEQUENCE {
```

```
  rpkiRtrPrefixOriginAddressType      InetAddressType,
  rpkiRtrPrefixOriginAddress          InetAddress,
  rpkiRtrPrefixOriginMinLength        InetAddressPrefixLength,
  rpkiRtrPrefixOriginMaxLength        InetAddressPrefixLength,
  rpkiRtrPrefixOriginASN              InetAutonomousSystemNumber,
  rpkiRtrPrefixOriginCacheServerId    Unsigned32
```

```
}
```

```
rpkiRtrPrefixOriginAddressType OBJECT-TYPE
```

```
SYNTAX          InetAddressType { ipv4(1), ipv6(2) }
MAX-ACCESS      not-accessible
STATUS          current
DESCRIPTION     "The network Address Type for this prefix.
```

```
                  Only IPv4 and IPv6 are supported."
```

```
::= { rpkiRtrPrefixOriginTableEntry 1 }
```

---

Internet-Draft    MIB Module for the RPKI-Router Protocol    October 2011

rpkiRtrPrefixOriginAddress OBJECT-TYPE

SYNTAX            InetAddress (SIZE(4|16))  
MAX-ACCESS       not-accessible  
STATUS            current  
DESCRIPTION "The network Address for this prefix.

The format of the address is defined by the  
value of the corresponding instance of  
rpkiRtrCacheServerAddressType."

::= { rpkiRtrPrefixOriginTableEntry 2 }

rpkiRtrPrefixOriginMinLength OBJECT-TYPE

SYNTAX            InetAddressPrefixLength  
MAX-ACCESS       not-accessible  
STATUS            current  
DESCRIPTION "The minimum prefix length allowed for this prefix."  
::= { rpkiRtrPrefixOriginTableEntry 3 }

rpkiRtrPrefixOriginMaxLength OBJECT-TYPE

SYNTAX            InetAddressPrefixLength  
MAX-ACCESS       read-only  
STATUS            current  
DESCRIPTION "The maximum prefix length allowed for this prefix.

Note, this value must be greater or equal to the  
value of rpkiRtrPrefixOriginMinLength."

::= { rpkiRtrPrefixOriginTableEntry 4 }

rpkiRtrPrefixOriginASN OBJECT-TYPE

SYNTAX            InetAutonomousSystemNumber  
MAX-ACCESS       read-only  
STATUS            current  
DESCRIPTION "The ASN that is authorized to announce the  
prefix or sub-prefixes covered by this entry."  
::= { rpkiRtrPrefixOriginTableEntry 5 }

rpkiRtrPrefixOriginCacheServerId OBJECT-TYPE

SYNTAX            Unsigned32 (1..4294967295)  
MAX-ACCESS       read-only  
STATUS            current

DESCRIPTION "The unique ID of the connection to the cache  
server from which this announcement was received.  
That connection is identified/found by a matching  
value in attribute rpkiRtrCacheServerId."  
::= { rpkiRtrPrefixOriginTableEntry 6 }

-- =====  
-- Notifications

Bush, et al.

Expires May 3, 2012

[Page 17]

---

Internet-Draft    MIB Module for the RPKI-Router Protocol    October 2011

-- =====

rpkiRtrCacheServerConnectionStateChange NOTIFICATION-TYPE  
OBJECTS        { rpkiRtrCacheServerConnectionStatus,  
                  rpkiRtrCacheServerLatestSerial,  
                  rpkiRtrCacheServerNonce  
                  }  
STATUS         current  
DESCRIPTION "This notification signals a change in the status  
            of an rpkiRtrCacheServerConnection.  
  
            The SNMP agent MUST throttle the generation of  
            consecutive rpkiRtrCacheServerConnectionStateChange  
            notifications such that there is at least a  
            5 second gap between them.  
            "  
::= { rpkiRtrNotifications 1 }

rpkiRtrCacheServerConnectionToGoStale NOTIFICATION-TYPE  
OBJECTS        { rpkiRtrCacheServerV4ActiveRecords,  
                  rpkiRtrCacheServerV6ActiveRecords,  
                  rpkiRtrCacheServerLatestSerial,  
                  rpkiRtrCacheServerNonce,  
                  rpkiRtrCacheServerRefreshTimer,  
                  rpkiRtrCacheServerTimeToRefresh  
                  }  
STATUS         current  
DESCRIPTION "This notification signals that an RPKI cache  
            server connection is about to go stale.  
            It is suggested that this notification is  
            generated when the value of the  
            rpkiRtrCacheServerTimeToRefresh attribute  
            goes below 60 seconds.

The SNMP agent MUST throttle the generation of consecutive rpkIRtrCacheServerConnectionToGoStale notifications such that there is at least a 5 second gap between them.

"

::= { rpkIRtrNotifications 2 }

-- =====  
-- Module Compliance information  
-- =====

rpkIRtrCompliances OBJECT IDENTIFIER ::= {rpkIRtrConformance 1}  
rpkIRtrGroups OBJECT IDENTIFIER ::=

Bush, et al.

Expires May 3, 2012

[Page 18]

---

Internet-Draft MIB Module for the RPKI-Router Protocol October 2011

{rpkIRtrConformance 2}

rpkIRtrReadOnlyCompliance MODULE-COMPLIANCE  
STATUS current  
DESCRIPTION "The compliance statement for the rpkIRtrMIB module. There are only read-only objects in this MIB module, so the 'ReadOnly' in the name of this compliance statement is there only for clarity and truth in advertising.  
"

MODULE -- This module

MANDATORY-GROUPS { rpkIRtrCacheServerGroup,  
rpkIRtrPrefixOriginGroup,  
rpkIRtrNotificationsGroup  
}

GROUP rpkIRtrCacheServerErrorsGroup

DESCRIPTION "Implementation of this group is optional and would be useful for debugging."

::= { rpkIRtrCompliances 1 }

rpkIRtrCacheServerGroup OBJECT-GROUP

OBJECTS { rpkIRtrDiscontinuityTimer,  
rpkIRtrCacheServerLocalAddress,  
rpkIRtrCacheServerLocalPort,  
rpkIRtrCacheServerPreference,  
rpkIRtrCacheServerConnectionType,

```

rpkiRtrCacheServerConnectionStatus,
rpkiRtrCacheServerDescription,
rpkiRtrCacheServerMsgsReceived,
rpkiRtrCacheServerMsgsSent,
rpkiRtrCacheServerV4ActiveRecords,
rpkiRtrCacheServerV4Announcements,
rpkiRtrCacheServerV4Withdrawals,
rpkiRtrCacheServerV6ActiveRecords,
rpkiRtrCacheServerV6Announcements,
rpkiRtrCacheServerV6Withdrawals,
rpkiRtrCacheServerLatestSerial,
rpkiRtrCacheServerNonce,
rpkiRtrCacheServerRefreshTimer,
rpkiRtrCacheServerTimeToRefresh,
rpkiRtrCacheServerId
}
STATUS current
DESCRIPTION "The collection of objects to monitor the RPKI peer
connections."
::= { rpkiRtrGroups 1 }

```

rpkiRtrCacheServerErrorsGroup OBJECT-GROUP

```

OBJECTS { rpkiRtrCacheServerErrorsCorruptData,
rpkiRtrCacheServerErrorsInternalError,
rpkiRtrCacheServerErrorsNoData,
rpkiRtrCacheServerErrorsInvalidRequest,
rpkiRtrCacheServerErrorsUnsupportedVersion,
rpkiRtrCacheServerErrorsUnsupportedPdu,
rpkiRtrCacheServerErrorsWithdrawalUnknown,
rpkiRtrCacheServerErrorsDuplicateAnnounce
}
STATUS current
DESCRIPTION "The collection of objects that may help in
debugging the communication between rpki
clients and cache servers."
::= { rpkiRtrGroups 2 }

```

rpkiRtrPrefixOriginGroup OBJECT-GROUP

```

OBJECTS { rpkiRtrPrefixOriginMaxLength,
rpkiRtrPrefixOriginASN,
rpkiRtrPrefixOriginCacheServerId

```

```

    }
    STATUS      current
    DESCRIPTION "The collection of objects that represent
                the prefix(es) and their validated origin
                ASes."
    ::= { rpkiRtrGroups 3 }

rpkiRtrNotificationsGroup NOTIFICATION-GROUP
    NOTIFICATIONS { rpkiRtrCacheServerConnectionStateChange,
                    rpkiRtrCacheServerConnectionToGoStale
                    }
    STATUS      current
    DESCRIPTION "The set of notifications to alert an NMS of change
                in connections to RPKI cache servers."
    ::= { rpkiRtrGroups 4 }

END

```

## 5. IANA Considerations

The MIB module in this document will required an IANA assigned OBJECT IDENTIFIER within the SMI Numbers registry. For example, replacing XXX below:

Descriptor	OBJECT IDENTIFIER value
-----	-----

Bush, et al.

Expires May 3, 2012

[Page 20]

---

Internet-Draft    MIB Module for the RPKI-Router Protocol    October 2011

```
rpkiRouter                    { mib-2 XXX }
```

## 6. Security Considerations

There are no management objects defined in this MIB module that have a MAX-ACCESS clause of read-write and/or read-create. So, if this MIB module is implemented correctly, then there is no risk that an intruder can alter or create any management objects of this MIB module via direct SNMP SET operations.

Most of the readable objects in this MIB module (i.e., objects with a

MAX-ACCESS other than not-accessible) may be considered sensitive or vulnerable in some network environments. They are vulnerable in the sense that when an intruder sees the information in this MIB module, then it might help him/her to setup a an attack on the router or cache server. It is thus important to control even GET and/or NOTIFY access to these objects and possibly to even encrypt the values of these objects when sending them over the network via SNMP.

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.

## [7.](#) References

### [7.1.](#) Normative References

[I-D.ietf-sidr-rpki-rtr]

Bush, R. and R. Austein, "The RPKI/Router Protocol",  
[draft-ietf-sidr-rpki-rtr-18](#) (work in progress),  
October 2011.

Bush, et al.

Expires May 3, 2012

[Page 21]

---

Internet-Draft    MIB Module for the RPKI-Router Protocol    October 2011

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.

[RFC2287] Krupczak, C. and J. Saperia, "Definitions of System-Level Managed Objects for Applications", [RFC 2287](#),



February 1998.

- [RFC2578] McCloghrie, K., Perkins, D., and J. Schoenwaelder, "Structure of Management Information Version 2 (SMIv2)", STD 58, [RFC 2578](#), April 1999.
- [RFC2579] McCloghrie, K., Perkins, D., and J. Schoenwaelder, "Textual Conventions for SMIv2", STD 58, [RFC 2579](#), April 1999.
- [RFC2580] McCloghrie, K., Perkins, D., and J. Schoenwaelder, "Conformance Statements for SMIv2", STD 58, [RFC 2580](#), April 1999.
- [RFC3410] Case, J., Mundy, R., Partain, D., and B. Stewart, "Introduction and Applicability Statements for Internet-Standard Management Framework", [RFC 3410](#), December 2002.
- [RFC4001] Daniele, M., Haberman, B., Routhier, S., and J. Schoenwaelder, "Textual Conventions for Internet Network Addresses", [RFC 4001](#), February 2005.

## [7.2.](#) Informative References

- [RFC1982] Elz, R. and R. Bush, "Serial Number Arithmetic", [RFC 1982](#), August 1996.
- [RFC2385] Heffernan, A., "Protection of BGP Sessions via the TCP MD5 Signature Option", [RFC 2385](#), August 1998.
- [RFC4252] Ylonen, T. and C. Lonvick, "The Secure Shell (SSH) Authentication Protocol", [RFC 4252](#), January 2006.
- [RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", [RFC 5246](#), August 2008.
- [RFC5925] Touch, J., Mankin, A., and R. Bonica, "The TCP Authentication Option", [RFC 5925](#), June 2010.

## Authors' Addresses

Randy Bush  
Internet Initiative Japan  
5147 Crystal Springs  
Bainbridge Island, Washington 98110  
US

Phone: +1 206 780 0431 x1

Email: [randy@psg.com](mailto:randy@psg.com)

Bert Wijnen  
RIPE NCC  
Schagen 33  
3461 GL Linschoten  
Netherlands

Email: [bertietf@bwijnen.net](mailto:bertietf@bwijnen.net)

Keyur Patel  
Cisco Systems  
170 W. Tasman Drive  
San Jose, CA 95134  
USA

Email: [keyupate@cisco.com](mailto:keyupate@cisco.com)

Michael Baer  
SPARTA  
P.O. Box 72682  
Davis, CA 95617  
USA

Email: [michael.baer@sparta.com](mailto:michael.baer@sparta.com)

