Definitions of Managed Objects for the Resource Public Key Infrastructure (RPKI) to Router Protocol

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 Resource Public Key Infrastructure (RPKI) to Router Protocol.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6945.
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 [RFC6810].

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. 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 [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 memo specifies a MIB module that is compliant to the SMIv2, which is described in STD 58, RFC 2578 [RFC2578], STD 58, RFC 2579 [RFC2579], and STD 58, RFC 2580 [RFC2580].

3. Overview

The objects defined in this document are used to monitor the RPKI-Router Protocol [RFC6810]. The MIB module defined here 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.

The RPKI-Router Cache Server Table contains information about the state and current activity of connections with the RPKI-router cache servers. It also contains counters for the number of messages received and sent, plus the number of announcements, withdrawals, and active records. The RPKI-Router Cache Server Errors Table contains counters of occurrences of errors on the connections (if any). The RPKI-Router Prefix Origin Table contains IP prefixes with their minimum and maximum prefix lengths and the Origin Autonomous System (AS). This data is the collective set of information received from all RPKI cache servers that the router is connected with. The cache servers are running the RPKI-Router Protocol.

Two notifications have been defined to inform a Network Management Station (NMS) or operators about changes in the connection state of the connections listed in the RPKI-Router Cache Server (Connection) Table.

4. Definitions

The following MIB module imports definitions from [RFC2578], [RFC2579], [RFC2580], [RFC4001], and [RFC2287]. That means we have a normative reference to each of those documents.

The MIB module also has a normative reference to the RPKI-Router Protocol [RFC6810]. Furthermore, for background and informative information, the MIB module refers to [RFC1982], [RFC4252], [RFC5246], and [RFC5925].
RPKI-ROUTER-MIB DEFINITIONS ::= BEGIN

IMPORTS

MODULE-IDENTITY, OBJECT-TYPE, NOTIFICATION-TYPE,
Integer32, Unsigned32, mib-2, Gauge32, Counter32
FROM SNMPv2-SMI -- RFC 2578

InetAddressType, InetAddress, InetPortNumber,
InetAddressPrefixLength, InetAutonomousSystemNumber
FROM INET-ADDRESS-MIB -- RFC 4001

TEXTUAL-CONVENTION, TimeStamp
FROM SNMPv2-TC -- RFC 2579

MODULE-COMPLIANCE, OBJECT-GROUP, NOTIFICATION-GROUP
FROM SNMPv2-CONF -- RFC 2580

LongUtf8String FROM SYSAPPL-MIB -- RFC 2287

;

rpkiRtrMIB MODULE-IDENTITY
LAST-UPDATED "201305010000Z"
ORGANIZATION "IETF Secure Inter-Domain Routing (SIDR)
Working Group"

CONTACT-INFO "Working Group Email: sidr@ietf.org

Randy Bush
Internet Initiative Japan
5147 Crystal Springs
Bainbridge Island, WA  98110
USA
Email: randy@psg.com

Bert Wijnen
RIPE NCC
Schagen 33
3461 GL Linschoten
Netherlands
Email: bert@bwijnen.net

Keyur Patel
Cisco Systems
170 W. Tasman Drive
San Jose, CA  95134
USA
This MIB module contains management objects to support monitoring of the Resource Public Key Infrastructure (RPKI) protocol on routers.

Copyright (c) 2013 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 RFC 6945; see the RFC itself for full legal notices."

REVISION "201305010000Z"
DESCRIPTION "Initial version, published as RFC 6945."

::= { mib-2 218 }

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 used between a router (as a client) and a cache server."
The following types have been defined in RFC 6810:
ssh(1)    -  Section 7.1; see also RFC 4252.
tls(2)    -  Section 7.2; see also RFC 5246.
tcpMD5(3) -  Section 7.3; see also RFC 2385.
tcpAO(4)  -  Section 7.4; see also RFC 5925.
tcp(5)    -  Section 7.
ipsec(6)  -  Section 7; see also RFC 4301.
other(7)  -  none of the above."

REFERENCE  "The RPKI-Router Protocol, RFC 6810, Section 7"
SYNTAX     INTEGER {
            ssh(1),
            tls(2),
            tcpMD5(3),
            tcpAO(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 objects in this MIB module encountered a discontinuity.

For objects that use rpkiRtrDiscontinuityTimer to indicate discontinuity, only values received since the time indicated by rpkiRtrDiscontinuityTimer are comparable to each other. A manager should take the possibility of rollover into account when calculating difference values.

In principle, that should only happen if the SNMP agent or the instrumentation for this MIB module starts or restarts."
::= { rpkiRtrObjects 1 }
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. Implementers should be aware that if the rpkiRtrCacheServerRemoteAddress object exceeds 114 octets, the index values will exceed the 128 sub-identifier limit and cannot be accessed using SNMPv1, SNMPv2c, or SNMPv3."
INDEX        { rpkiRtrCacheServerRemoteAddressType,
               rpkiRtrCacheServerRemoteAddress,
               rpkiRtrCacheServerRemotePort
               }
::= { rpkiRtrCacheServerTable 1 }

RpkiRtrCacheServerTableEntry ::= SEQUENCE {
  rpkiRtrCacheServerRemoteAddressType     InetAddressType,
  rpkiRtrCacheServerRemoteAddress        InetAddress,
  rpkiRtrCacheServerRemotePort           InetPortNumber,
  rpkiRtrCacheServerLocalAddressType     InetAddressType,
  rpkiRtrCacheServerLocalAddress         InetAddress,
  rpkiRtrCacheServerLocalPort            InetPortNumber,
  rpkiRtrCacheServerPreference           Unsigned32,
  rpkiRtrCacheServerConnectionType       RpkiRtrConnectionType,
  rpkiRtrCacheServerConnectionStatus     INTEGER,
  rpkiRtrCacheServerDescription          LongUtf8String,
  rpkiRtrCacheServerMsgsReceived         Counter32,
  rpkiRtrCacheServerMsgsSent             Counter32,
  rpkiRtrCacheServerV4ActiveRecords      Gauge32,
  rpkiRtrCacheServerV4Announcements      Counter32,
  rpkiRtrCacheServerV4Withdrawals        Counter32,
  rpkiRtrCacheServerV6ActiveRecords      Gauge32,
  rpkiRtrCacheServerV6Announcements      Counter32,
  rpkiRtrCacheServerV6Withdrawals        Counter32,
  rpkiRtrCacheServerLatestSerial         Unsigned32,
}
rfcRtrCacheServerSessionID Unsigned32,
rfcRtrCacheServerRefreshTimer Unsigned32,
rfcRtrCacheServerTimeToRefresh Integer32,
rfcRtrCacheServerId Unsigned32
}

rfcRtrCacheServerRemoteAddressType OBJECT-TYPE
SYNTAX InetAddressType
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION "The network address type of the connection
to this RPKI cache server.

Note: Only IPv4, IPv6, and DNS support are required
for read-only compliance with RFC 6945."
::= { rfcRtrCacheServerTableEntry 1 }

rfcRtrCacheServerRemoteAddress OBJECT-TYPE
SYNTAX InetAddress
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
rfcRtrCacheServerRemoteAddressType.

This object matches the address type used within
the local router configuration. If the address is
of type dns (fqdn), then the router will resolve it
at the time it connects to the cache server."
::= { rfcRtrCacheServerTableEntry 2 }

rfcRtrCacheServerRemotePort 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."
::= { rfcRtrCacheServerTableEntry 3 }

rfcRtrCacheServerLocalAddressType OBJECT-TYPE
SYNTAX InetAddressType
MAX-ACCESS read-only
STATUS current
DESCRIPTION "The network address type of the connection
to this RPKI cache server."
Note: Only IPv4, IPv6, and DNS support are required for read-only compliance with RFC 6945.

::= { rpkiRtrCacheServerTableEntry 4 }

rpkiRtrCacheServerLocalAddress OBJECT-TYPE
SYNTAX       InetAddress
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 rpkiRtrCacheServerLocalAddressType.

This object matches the address type used within the local router configuration. If the address is of type dns (fqdn), then the router will resolve it at the time it connects to the cache server."

::= { rpkiRtrCacheServerTableEntry 5 }

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 6 }

rpkiRtrCacheServerPreference OBJECT-TYPE
SYNTAX       Unsigned32
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.

In two cases, the maximum value for an Unsigned32 object should be returned for this object:
- If no order is specified in the RPKI-Router configuration.
- If a preference value is configured that is larger than the max value for an Unsigned32 object."

REFERENCE    "The RPKI-Router Protocol, RFC 6810, Section 8."
DEFVAL { 4294967295 }
::= { rpkiRtrCacheServerTableEntry 7 }

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 8 }

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 9 }

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 10 }

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 11 }

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 12 }
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 13 }

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 14 }

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 15 }

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 16 }

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 17 }
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 18 }

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 "RFC 1982 and RFC 6810, Section 2"
::= { rpkiRtrCacheServerTableEntry 19 }

rpkiRtrCacheServerSessionID OBJECT-TYPE
SYNTAX Unsigned32 (0..65535)
MAX-ACCESS read-only
STATUS current
DESCRIPTION "The Session ID associated with the RPKI cache
server at the other end of this connection."
REFERENCE "RFC 6810, Section 2"
::= { rpkiRtrCacheServerTableEntry 20 }

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."
REFERENCE "RFC 6810, Sections 6.1 and 8"
::= { rpkiRtrCacheServerTableEntry 21 }

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. It will stop decrementing at the maximum negative value.

Upon a completed refresh (i.e., a successful and complete response to a Serial Query) the value of this attribute will be reinitialized with the value of the corresponding rpkiRtrCacheServerRefreshTimer attribute."

REFERENCE "RFC 6810, Section 8"
::= { rpkiRtrCacheServerTableEntry 22 }

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."

REFERENCE "RFC 6810, Section 4"
::= { rpkiRtrCacheServerTableEntry 23 }

-- ==============================================================
-- 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 error codes that were received on the specified connection to a specific cache server."

REFERENCE "RFC 6810, Section 10"

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  
-- ==============================================================

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 Autonomous  
System Number (ASN) as received by announcements  
via the RPKI-Router 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.  If a cache server  
is removed from the local configuration, any table  
rows associated with that server (indicated by  
rpkiRtrPrefixOriginCacheServerId) are also removed  
from this table.

Implementers should be aware that if the  
rpkiRtrPrefixOriginAddress object exceeds 111  
octets, the index values will exceed the 128
sub-identifier limit and cannot be accessed using
SNMPv1, SNMPv2c, or SNMPv3."

INDEX
{ rpkiRtrPrefixOriginAddressType,
rpkiRtrPrefixOriginAddress,
rpkiRtrPrefixOriginMinLength,
rpkiRtrPrefixOriginMaxLength,
rpkiRtrPrefixOriginASN,
rpkiRtrPrefixOriginCacheServerId }
::= { rpkiRtrPrefixOriginTable 1 }

RpkiRtrPrefixOriginTableEntry ::= SEQUENCE {
  rpkiRtrPrefixOriginAddressType    InetAddressType,
rpkiRtrPrefixOriginAddress        InetAddress,
rpkiRtrPrefixOriginMinLength      InetAddressPrefixLength,
rpkiRtrPrefixOriginMaxLength      InetAddressPrefixLength,
rpkiRtrPrefixOriginASN            InetAutonomousSystemNumber,
rpkiRtrPrefixOriginCacheServerId  Unsigned32
}

rpkiRtrPrefixOriginAddressType OBJECT-TYPE
SYNTAX     InetAddressType
MAX-ACCESS not-accessible
STATUS     current
DESCRIPTION "The network address type for this prefix.

Note: Only IPv4 and IPv6 support are required for read-only compliance with RFC 6945."
::= { rpkiRtrPrefixOriginTableEntry 1 }

rpkiRtrPrefixOriginAddress OBJECT-TYPE
SYNTAX     InetAddress
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 rpkiRtrPrefixOriginAddressType."
::= { 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   not-accessible
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 (0..4294967295)
MAX-ACCESS   not-accessible
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
-- ==================================================

rpkiRtrCacheServerConnectionStateChange NOTIFICATION-TYPE
OBJECTS     { rpkiRtrCacheServerConnectionStatus,
             rpkiRtrCacheServerLatestSerial,
             rpkiRtrCacheServerSessionID }
STATUS      current
DESCRIPTION "This notification signals a change in the status
of an rpkiRtrCacheServerConnection.
The management agent MUST throttle the generation of
consecutive rpkiRtrCacheServerConnectionStateChange
notifications such that there is at least a 5 second
gap between them.
If more than one notification has occurred locally
during that time, the most recent notification is
sent at the end of the 5 second gap and the others are discarded.

::= {(rpkiRtrNotifications 1)

rpkiRtrCacheServerConnectionToGoStale NOTIFICATION-TYPE
OBJECTS { rpkiRtrCacheServerV4ActiveRecords, rpkiRtrCacheServerV6ActiveRecords, rpkiRtrCacheServerLatestSerial, rpkiRtrCacheServerSessionID, 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 ::= {rpkiRtrConformance 2}
rpkiRtrRFC6945ReadOnlyCompliance 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.

There are a number of INDEX objects that cannot be represented in the form of OBJECT clauses in SMIV2, but for which there are compliance requirements. Those requirements and similar requirements for related objects are expressed
below, in pseudo-OBJECT clause form, in this description:

-- OBJECT rpkiRtrCacheServerRemoteAddressType
-- SYNTAX InetAddressType { ipv4(1), ipv6(2), dns(16) }
-- DESCRIPTION
-- The MIB requires support for the IPv4, IPv6, and DNS
-- InetAddressTypes for this object.

-- OBJECT rpkiRtrCacheServerLocalAddressType
-- SYNTAX InetAddressType { ipv4(1), ipv6(2), dns(16) }
-- DESCRIPTION
-- The MIB requires support for the IPv4, IPv6, and DNS
-- InetAddressTypes for this object.

-- OBJECT rpkiRtrPrefixOriginAddressType
-- SYNTAX InetAddressType { ipv4(1), ipv6(2) }
-- DESCRIPTION
-- The MIB requires support for the IPv4, and IPv6
-- InetAddressTypes for this object.

"
rpkiRtrCacheServerV6ActiveRecords,
rpkiRtrCacheServerV6Announcements,
rpkiRtrCacheServerV6Withdrawals,
rpkiRtrCacheServerLatestSerial,
rpkiRtrCacheServerSessionID,
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
{
  rpkiRtrPrefixOriginCacheServerId
}

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

IANA has assigned the MIB module in this document the following
OBJECT IDENTIFIER within the SMI Numbers registry.

<table>
<thead>
<tr>
<th>Descriptor</th>
<th>OBJECT IDENTIFIER value</th>
</tr>
</thead>
<tbody>
<tr>
<td>rpkiRtrMIB</td>
<td>{ mib-2 218 }</td>
</tr>
</tbody>
</table>

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 set up 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),
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.

Implementations MUST provide the security features described by the
SNMPv3 framework (see [RFC3410]), including full support for
authentication and privacy via the User-based Security Model (USM)
[RFC3414] with the AES cipher algorithm [RFC3826]. Implementations
MAY also provide support for the Transport Security Model (TSM) [RFC5591] in combination with a secure transport such as SSH [RFC5592] or TLS/DTLS [RFC6353].

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


7.2. Informative References


Authors’ Addresses

Randy Bush
Internet Initiative Japan
5147 Crystal Springs
Bainbridge Island, WA 98110
US
EMail: randy@psg.com

Bert Wijnen
RIPE NCC
Schagen 33
3461 GL Linschoten
Netherlands
EMail: bertietf@bwijnen.net

Keyur Patel
Cisco Systems
170 W. Tasman Drive
San Jose, CA 95134
USA
EMail: keyupate@cisco.com

Michael Baer
SPARTA
P.O. Box 72682
Davis, CA 95617
USA
EMail: baerm@tislabs.com