IP MIB for IP Fast-Reroute

draft-ietf-rtgwg-ipfrr-ip-mib-02

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

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

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

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

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

This Internet-Draft will expire on August 23, 2012.

Abstract

This draft defines a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. In particular, it describes managed objects relevant for IP routes using IP Fast-Reroute [RFC5714].
Table of Contents

1. Introduction ............................................. 3
   1.1. The SNMP Management Framework ....................... 3
2. Brief Description of MIB Objects ............................ 4
   2.1. ipFrrProtectStats Group .............................. 4
   2.2. ipFrrAltTable ....................................... 4
   2.3. ipFrrNoAltTable ..................................... 4
3. IP Fast-Reroute MIB Module Definitions ...................... 5
4. Security Considerations .................................... 16
5. References ................................................. 16
Authors’ Addresses ........................................... 18
Full Copyright Statements ..................................... 19
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 the managed objects used for IP routes and interfaces in relation to IP Fast-Reroute. This document uses terminology from [RFC5714] and [RFC5286].

Current work is underway to define mechanisms for determining alternate paths for traffic to use when the original path becomes unavailable due to a local failure. The alternate next-hops can be computed in the context of any IGP.

There are certain configuration attributes for IP Fast-Reroute that should be configured to enable IP Fast Reroute in the context of the IGP. These configuration attributes of IP Fast-Reroute are not covered by this MIB module. Examples include whether IP Fast-Reroute is enabled on a network region (i.e. an OSPF area or IS-IS level) and the desired local hold-down timer [RFC5286], whose proper value is dependent upon the size of the network region.

It is possible for traffic other than IP to depend upon and use the alternate next-hops computed by IP Fast-Reroute. An example would be MPLS traffic whose path is configured via LDP [RFC5036]. The additional details (for example, outgoing MPLS label) pertaining to alternate next-hops that are required by such traffic are not covered by this MIB module.

An IP route may be reachable via multiple primary next-hops which provide equal-cost paths. Where IP Fast-Reroute is enabled, each primary next-hop will be protected by one or more alternate next-hops. Such an alternate next-hop may itself be a primary next-hop.

1.1. The SNMP 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].
2. Brief Description of MIB Objects

This MIB module consists of five global objects, organized into the ipFrrProtectStats group, and two tables.

2.1. ipFrrProtectStats Group

The global objects in this group provide summary information related to protection for all IP routes. The information available includes counts of all routes, of all protected routes, of all unprotected routes, of all routes which are protected against a link failure, and of all routes which are protected against a node failure.

2.2. ipFrrAltTable

The ipFrrAltTable extends the inetCidrRouteTable[RFC4292] to provide information about each alternate next-hop associated with a primary next-hop used by a route. Statically configured alternate next-hops associated with primary next-hops can be created.

2.3. ipFrrNoAltTable

The ipFrrNoAltTable extends the inetCidrRouteTable[RFC4292] to provide information about the routes which do not have an alternate next-hop associated with any of the route’s primary next-hop. The entry provides an explanation for the lack of protection.
3. IP Fast-Reroute MIB Module Definitions

IPFRR-MIB DEFINITIONS ::= BEGIN

IMPORTS
  MODULE-IDENTITY,
  OBJECT-TYPE,
  Gauge32,
  Integer32             FROM SNMPv2-SMI          -- [RFC2578]
  RowStatus
  FROM SNMPv2-TC           -- [RFC2579]
  MODULE-COMPLIANCE,
  OBJECT-GROUP
  FROM SNMPv2-CONF         -- [RFC2580]
  InetAddressType,
  InetAddress
  FROM INET-ADDRESS-MIB    -- [RFC4001]
  InterfaceIndex
  FROM IF-MIB              -- [RFC2863]
  ip
  FROM IP-MIB              -- [RFC4293]
  inetCidrRouteDestType,
  inetCidrRouteDest,
  inetCidrRoutePfxLen,
  inetCidrRoutePolicy,
  inetCidrRouteNextHopType,
  inetCidrRouteNextHop
  FROM IP-FORWARD-MIB
  -- [RFC4292]

 ;

ipFrrMIB MODULE-IDENTITY
LAST-UPDATED "201203131200Z" -- Mar 13, 2012
ORGANIZATION "draft-ietf-ipfrr-ip-mib-02.txt"
CONTACT-INFO
  
    A S Kiran Koushik
    Cisco Systems Inc.
    EMail: kkoushik@cisco.com

    John W Flick
    Hewlett Packard Company
    EMail: john.flick@hp.com

    Alia Atlas
    Juniper Networks
    Email: akatlas@juniper.net

A S Kiran Koushik
Cisco Systems Inc.
EMail: kkoushik@cisco.com

John W Flick
Hewlett Packard Company
EMail: john.flick@hp.com

Alia Atlas
Juniper Networks
Email: akatlas@juniper.net
DESCRIPTION

"IP MIB module for management of IP Fast-Reroute.

Copyright (C) The Internet Society (date).
This version of this MIB module is part of
draft-ietf-rtgwg-ipfrr-ip-mib-00.txt"
REVISION      "201203131200Z" -- Mar 13, 2012
DESCRIPTION
"Editorial changes. Added new type to ipFrrAltType."
REVISION      "200502181200Z" -- February 18, 2005
DESCRIPTION
"Add Set operations on ipFrrAltTable"
REVISION      "200502131200Z" -- February 13, 2005
DESCRIPTION
"Initial version."
::= {  ip ZZZ } -- To be assigned by IANA
-- RFC Ed.: replace 999 with actual RFC number
-- & remove this note

-- Top level components of this MIB module.

ipFrrMIBObjects OBJECT IDENTIFIER ::= { ipFrrMIB 1 }

ipFrrProtectStats OBJECT IDENTIFIER ::= { ipFrrMIBObjects 1 }

-- the IP FRR MIB-Group

-- A collection of objects providing summarized information
-- about the protection availability and type of alternate paths
-- provided by IP Fast-Reroute mechanisms.

ipFrrTotalRoutes   OBJECT-TYPE
SYNTAX     Gauge32
MAX-ACCESS read-only
STATUS     current
DESCRIPTION
"The number of valid routes known by this entity."
::= { ipFrrProtectStats 1 }

ipFrrUnprotectedRoutes   OBJECT-TYPE
SYNTAX     Gauge32
MAX-ACCESS read-only
STATUS     current
DESCRIPTION
"The number of valid routes known by this entity

which do not have an alternate next-hop associated with any primary next-hop.

::= { ipFrrProtectStats 2 }

ipFrrProtectedRoutes OBJECT-TYPE
SYNTAX Gauge32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The number of routes known by this entity which have at least one alternate next-hop."
::= { ipFrrProtectStats 3 }

ipFrrLinkProtectedRoutes OBJECT-TYPE
SYNTAX Gauge32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The number of routes known by this entity for which all alternate next-hops provide link protection for their associated primary next-hops."
::= { ipFrrProtectStats 4 }

ipFrrNodeProtectedRoutes OBJECT-TYPE
SYNTAX Gauge32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The number of routes known by this entity for which all alternate next-hops provide node protection for their associated primary next-hops."
::= { ipFrrProtectStats 5 }

-- the IP FRR Alternate MIB-Group
--
-- The ipFrrAltTable extends the inetCidrRouteTable to indicate
-- the alternate next-hop(s) associated with each primary
-- next-hop. The additional indices (ipFrrAltNextHopType and
-- ipFrrAltNextHop ) allow for multiple alternate paths for a
-- given primary next-hop.

ipFrrAltTable OBJECT-TYPE
SYNTAX SEQUENCE OF IpFrrAltEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
"This entity’s IP Fast Reroute Alternates table."
::= { ipFrrMIBObjects 2 }

ipFrrAltEntry OBJECT-TYPE
SYNTAX IpFrrAltEntry
MAX-ACCESS not-accessible
An entry containing information on a particular route, one of its particular (primary) next-hops and one of the associated alternate next-hops.

Implementers need to be aware that if the total number of elements (octets or sub-identifiers) in inetCidrRouteDest, inetCidrRoutePolicy, inetCidrRouteNextHop, and ipFrrAltNextHop exceeds 107 then OIDs of column instances in this table will have more than 128 sub-identifiers and cannot be accessed using SNMPv1, SNMPv2c, or SNMPv3.

INDEX { inetCidrRouteDestType, inetCidrRouteDest, inetCidrRoutePfxLen, inetCidrRoutePolicy, inetCidrRouteNextHopType, inetCidrRouteNextHop, ipFrrAltNextHopType, ipFrrAltNextHop }

::= { ipFrrAltTable 1 }

IpFrrAltEntry ::= SEQUENCE {
  ipFrrAltNextHopType              InetAddressType,
  ipFrrAltNextHop                  InetAddress,
  ipFrrAltIfIndex                  InterfaceIndex,
  ipFrrAltType                     INTEGER,
  ipFrrAltProtectionAvailable      BITS,
  ipFrrAltMetric1                  Integer32,
  ipFrrAltStatus                   RowStatus
}

ipFrrAltNextHopType OBJECT-TYPE
SYNTAX     InetAddressType
MAX-ACCESS not-accessible
STATUS     current
DESCRIPTION
"The type of the ipFrrNextHop address, as defined in the InetAddress MIB.

Only those address types that may appear in an actual routing table are allowed as values of this object."

REFERENCE "RFC 4001"

 ::= { ipFrrAltEntry 1 }
ipFrrAltNextHop OBJECT-TYPE
SYNTAX     InetAddress
MAX-ACCESS not-accessible
STATUS     current
DESCRIPTION
"The address of the next system along the alternate
route.

The type of this address is determined by the value
of the ipFrrAltNextHopType."
::= { ipFrrAltEntry 2 }

ipFrrAltIfIndex OBJECT-TYPE
SYNTAX     InterfaceIndex
MAX-ACCESS read-create
STATUS     current
DESCRIPTION
"The ifIndex value which identifies the local
interface through which the next hop of this
alternate route should be reached."
::= { ipFrrAltEntry 3 }

ipFrrAltType OBJECT-TYPE
SYNTAX     INTEGER {
   other      (1), -- type not defined
   equalCost  (2), -- primary path
   loopFree   (3), -- loop free alternate
   MRT        (4)  -- Maximally Redundant Trees
}
MAX-ACCESS read-create
STATUS     current
DESCRIPTION
"The type of alternate which is provided by the
alternate next-hop. The supported types are as
follows:

equalCost : The alternate next-hop is another
primary next-hop.

loopFree : The shortest route to the destination
IP address from the alternate next-hop
does not traverse this system. See
draft-ietf-rtgwg-ipfrr-spec-base-04.
other : The mechanism by which the alternate next-hop can be used is not specified.

MRT : Maximally Redundant Trees, where each destination has two MRTs associated with it. These two trees are referred as blue and red MRTs. See draft-ietf-rtgwg-mrt-frr-architecture-00.

::= { ipFrrAltEntry 4 }

ipFrrAltProtectionAvailable OBJECT-TYPE
SYNTAX     BITS {
          nodeProtect(0),
          linkProtect(1),
          unknownProtection(2)
        }
MAX-ACCESS read-create
STATUS     current
DESCRIPTION
"This object specifies the scope of protection for which this alternate next-hop can provide failure protection. The alternate next-hop should provide one or more of node-protection and link-protection. If the protection provided by the alternate next-hop is unknown, then only unknownProtection should be specified. Specifying unknownProtection with any other type of protection is not supported. "

::= { ipFrrAltEntry 5 }

ipFrrAltMetric1 OBJECT-TYPE
SYNTAX     Integer32
MAX-ACCESS read-create
STATUS     current
DESCRIPTION
"This is the primary routing metric for this alternate path to the destination IP address. If the alternate path metric is unknown, the value should be set to -1."

::= { ipFrrAltEntry 6 }

ipFrrAltStatus OBJECT-TYPE
SYNTAX     RowStatus
MAX-ACCESS read-create
STATUS     current
DESCRIPTION
"The row status variable, used according to row installation and removal conventions."

::= { ipFrrAltEntry 7 }
The ipFrrNoAltTable extends the inetCidrRouteTable to indicate which routes are unprotected and the reason why. The indices do not include the primary next-hop because the lack of protection is for the route. This allows easy access to the set of unprotected routes that would be affected by a local failure of their primary next-hop.

ipFrrNoAltTable OBJECT-TYPE
SYNTAX SEQUENCE OF IpFrrNoAltEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION "This entity’s IP Fast Reroute Unprotected Routes table."
 ::= { ipFrrMIBObjects 3 }

ipFrrNoAltEntry OBJECT-TYPE
SYNTAX IpFrrNoAltEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION "An entry containing the reason why a route does not have an alternate next-hop. The existence of an entry for a route indicates that there is no alternate next-hop."
INDEX { inetCidrRouteDestType, inetCidrRouteDest, inetCidrRoutePfxLen }
 ::= { ipFrrNoAltTable 1 }

IpFrrNoAltEntry ::= SEQUENCE {
   ipFrrNoAltCause INTEGER
}

ipFrrNoAltCause OBJECT-TYPE
SYNTAX INTEGER {
   ipFrrUnavailable (1), -- No valid alternate(s)
   localAddress (2), -- local/internal address
   ipFrrDisabled (3), -- Protection not enabled
   other (4) -- unknown or other cause
}
MAX-ACCESS read-only
STATUS current
"For valid routes without an alternate next-hop, this object enumerates the reason why no protection is available. The possibilities are as follows.

ipFrrUnavailable : The supported IP Fast-Reroute mechanisms could not find a safe alternate next-hop.

localAddress : The route represents a local address. This system is the destination so no alternate path is possible or necessary.

ipFrrDisabled : Finding of alternate next-hops is operationally disabled.

other : The reason is unknown or different from those specifically enumerated possible causes."

::= { ipFrrNoAltEntry 1 }

-- conformance information

ipFrrMIBConformance
  OBJECT IDENTIFIER ::= { ipFrrMIB 2 }

ipFrrMIBCompliances
  OBJECT IDENTIFIER ::= { ipFrrMIBConformance 1 }

ipFrrMIBGroups
  OBJECT IDENTIFIER ::= { ipFrrMIBConformance 2 }

-- compliance statements

ipFrrMIBCompliance MODULE-COMPLIANCE
  STATUS  deprecated
  DESCRIPTION
"Minimum requirements to state conformity to this MIB. Supporting only IP v4 addresses. This is deprecated in favor of ipFrrMIBinetCompliance

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, expressed in OBJECT clause form in this description:

OBJECT inetCidrRouteDestType
SYNTAX InetAddressType { ipv4(1), ipv4z(3) }
MIN-ACCESS read-only
DESCRIPTION
A (deprecated) complying implementation at this level is required to support IPv4 addresses only. This compliance level is defined so an implementation only needs to support the addresses it actually supports on the device.

OBJECT inetCidrRouteNextHopType
SYNTAX InetAddressType { ipv4(1), ipv4z(3) }
MIN-ACCESS read-only
DESCRIPTION
A (deprecated) complying implementation at this level is required to support IPv4 addresses only. This compliance level is defined so an implementation only needs to support the addresses it actually supports on the device.

OBJECT ipFrrAltNextHopType
SYNTAX InetAddressType { ipv4(1), ipv4z(3) }
MIN-ACCESS read-only
DESCRIPTION
A (deprecated) complying implementation at this level is required to support IPv4 addresses only. This compliance level is defined so an implementation only needs to support the addresses it actually supports on the device.
WRITE-SYNTAX INTEGER { createAndGo(4), destroy(6) }
DESCRIPTION
"Support for createAndWait and notInService is not required."

::= { ipFrrMIBCompliances 2 }

ipFrrReadOnlyCompliance MODULE-COMPLIANCE
  STATUS current
  DESCRIPTION
"When this MIB is implemented without support for read-create (i.e. in read-only mode), then that implementation can claim read-only compliance. In that case, ipFrrAlt group can be monitored but cannot be configured with this MIB."

MODULE
MANDATORY-GROUPS { ipFrrBasicGroup }

OBJECT ipFrrAltIfIndex
MIN-ACCESS read-only
DESCRIPTION
"Write access is not required."

OBJECT ipFrrAltType
MIN-ACCESS read-only
DESCRIPTION
"Write access is not required."

OBJECT ipFrrAltProtectionAvailable
MIN-ACCESS read-only
DESCRIPTION
"Write access is not required."

OBJECT ipFrrAltMetric1
MIN-ACCESS read-only
DESCRIPTION
"Write access is not required."

OBJECT ipFrrAltStatus
MIN-ACCESS read-only
DESCRIPTION
"Write access is not required."

::= { ipFrrMIBCompliances 3 }

-- units of conformance
ipFrrBasicGroup OBJECT-GROUP
  OBJECTS {ipFrrTotalRoutes,
ipFrrUnprotectedRoutes,
ipFrrProtectedRoutes,
ipFrrLinkProtectedRoutes,
ipFrrNodeProtectedRoutes,
ipFrrAltIfIndex,
ipFrrAltType,
ipFrrAltProtectionAvailable,
ipFrrAltMetric1,
ipFrrAltStatus,
ipFrrNoAltCause}

} STATUS current
DESCRIPTION
  "The entire collection of objects defined in
  this MIB for management of IP Fast Reroute ."
::= { ipFrrMIBGroups 1 }

END
4. Security Considerations

There are a number of management objects defined in this MIB module with a MAX-ACCESS clause of read-write and/or read-create. Such objects may be considered sensitive or vulnerable in some network environments. The support for SET operations in a non-secure environment without proper protection can have a negative effect on network operations. The ipFrrAltTable contains routing and forwarding information that is critical to the operation of the network in the event of a local failure. Allowing unauthenticated write access to this table can compromise the validity of the alternate forwarding information.

Some 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. It is thus important to control even GET access to these objects and possibly to even encrypt the values of these objects when sending them over the network via SNMP.

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 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 them.

5. References

5.1 Normative References
5.2 Informative References


6.  IANA Considerations

The MIB module in this document uses the following IANA-assigned
OBJECT IDENTIFIER value recorded in the SMI Numbers registry.

The IANA is requested to assign \{ ip ZZZ \} to the
IPFRR-MIB MIB module specified in this document.

Editor’s Note (to be removed prior to publication): the IANA is
requested to assign a value for "ZZZ" under
the ip subtree and to record the assignments in the SMI Numbers
registry. When the assignments have been made, the RFC Editor is
asked to replace "ZZZ" (here and in the MIB
modules) with the assigned value and to remove this note.

Authors’ Addresses

Alia Atlas
Juniper Networks
10 Technology Park Drive
Westford, MA  01886
USA

Email: akatlas@juniper.net

A S Kiran Koushik (Ed.)
Cisco Systems Inc.
12515 Research Blvd, Bldg 4,
Austin, TX 78759
USA

Email: kkoushik@cisco.com

John Flick (Ed.)
Hewlett-Packard Company
8000 Foothills Blvd.
Roseville, CA 95747-5557
USA
Email: john.flick@hp.com
Acknowledgements

The authors would like to acknowledge contributions made by Bill Anderson and Don Fedyk and thank them.

Full Copyright Statement

Copyright (c) 2012 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 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.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Acknowledgment

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