

Network Working Group  
Internet Draft  
Expiration Date: August 2001

J. Haas  
NextHop  
S. Hares  
NextHop  
22 February 2001

Definitions of Managed Objects  
for the Fourth Version of Border Gateway Protocol (BGP-4)  
- Extensions for Optional parameters

[draft-jhaas-bgp4-mib-opt-00.txt](#)

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC 2026](#).

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>.

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

Copyright Notice

Copyright (C) The Internet Society (1999). All Rights Reserved.

Abstract

This memo is an extension to the BGP-4 MIB to support the Optional Parameters attributes for Authentication [RFC1771 4.2a] and BGP-4 Capabilities Advertisement [[RFC2842](#)]. Additionally, this MIB provides a registration point for BGP-4 Capabilities defined protocols.

Internet Draft

[draft-jhaas-bgp4-mib-opt-00.txt](#)

Februrary 2001

This BGP MIB provides management information relating to these optional functions in BGP-4.

Distribution of this memo is unlimited. Please forward comments to [idr@merit.net](mailto:idr@merit.net).

## 1. Introduction

This memo defines a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. In particular, it describes the optional managed objects used for managing Authentication and Optional Capabilities for the Border Gateway Protocol Version 4.

The BGP-4 Authentication Optional Parameter attribute is defined in [RFC 1771, section 4.2a](#).

The BGP-4 Capabilities Advertisement extension is defined in [RFC 2842](#).

Please refer to the RFCs for the definition of these protocols.

## 2. Overview

These objects are used to control and manage a optional functions in the BGP-4 protocol. This optional MIB is considered an extension to the current BGP-4 MIB. The OID numbering begins at the end of the Current BGP-4 MIB.

This optional MIB is made up of the following objects:

- i. `bgpAuthenticationTable { bgp 9 1 }`

Specifies the Authentication data exchanged between BGP-4 peers.

- ii. `bgpCapabilitySupportAvailable { bgp 9 2 }`

Specifies whether or not the BGP-4 Capabilities Advertisement RFC is supported.

iii. `bgpSupportedCapabilities { bgp 9 3 }`

Specifies a bit vector of what BGP-4 Capabilities are supported by this implementation.

iv. `bgpPeerCapabilitiesTable { bgp 9 4 }`

A table of capabilities advertised to and received from a BGP-4 peer.

v. `bgpProtocolExtensions { bgp 9 5 }`

Provides a registration point for additional MIBs for BGP-4 protocol extensions which use BGP-4 Capabilities Advertisement.

### 3. Definitions

BGP4-OPT-PARAMETERS-MIB DEFINITIONS ::= BEGIN

#### IMPORTS

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

bgpPeerRemoteAddr FROM BGP-MIB

TruthValue, AutonomousType FROM SNMPv2-TC

MODULE-COMPLIANCE, OBJECT-GROUP, NOTIFICATION-GROUP  
FROM SNMPv2-CONF;

bgp4OptParametersMIB MODULE-IDENTITY  
LAST-UPDATED "200102230000Z"  
ORGANIZATION "IETF IDR Working Group"  
CONTACT-INFO

"E-Mail: idr@merit.net

Editor: Susan Hares  
517 W. William Street  
Ann Arbor, MI 48103-4943  
Tel: +1 734 936 2095  
Fax: +1 734 615-3241  
E-mail: skh@nexthop.com

Authors: Jeffrey Haas  
NextHop Technologies  
517 W. William Street  
Ann Arbor, MI 48103-4943  
Tel: +1 734 936 2095  
Fax: +1 734 615-3241  
E-mail: jhaas@nexthop.com"

Haas

[Page 3]

Internet Draft

[draft-jhaas-bgp4-mib-opt-00.txt](#)

Februrary 2001

#### DESCRIPTION

"The extension of the MIB module for BGP-4 for optional parameters."

REVISION "200102230000Z"

#### DESCRIPTION

"Initial proposal.

Definition of MIB extension for the following optional exetnsions to BGP-4"

#### REFERENCE

"[RFC 1771](#) - Border Gateway Protocol, Version 4

[RFC 2385](#) - TCP MD5 Authentication

[RFC 2842](#) - Capabilities Advertisement with BGP-4"

::= { bgp 9 }

```
-- bgpAuthenticationTable      { bgp4OptParametersMIB 1 }
-- bgpCapabilitySupportAvailable { bgp4OptParametersMIB 2 }
-- bgpSupportedCapabilities     { bgp4OptParametersMIB 3 }
-- bgpPeerCapabilitiesTable     { bgp4OptParametersMIB 4 }
-- bgpProtocolExtensions       { bgp4OptParametersMIB 5 }
```

bgpAuthenticationTable OBJECT-TYPE

SYNTAX SEQUENCE OF BgpAuthenticationPeerEntry

MAX-ACCESS not-accessible

STATUS current  
DESCRIPTION  
    "The BGP-4 Authentication Table contains information  
    about BGP Authentication Options on a per-peer basis."  
REFERENCE  
    "[RFC 1771](#) - Border Gateway Protocol, Version 4"  
::= { bgp4OptParametersMIB 1 }

bgpAuthenticationPeerEntry OBJECT-TYPE  
SYNTAX BgpAuthenticationPeerEntry  
MAX-ACCESS not-accessible  
STATUS current  
DESCRIPTION  
    "Information about Authentication on a per-peer basis."  
INDEX {  
    bgpPeerRemoteAddr,  
    bgpAuthenticationDirection  
}  
::= { bgpAuthenticationTable 1 }

bgpAuthenticationEntry OBJECT-TYPE  
SYNTAX BgpAuthenticationEntry  
MAX-ACCESS not-accessible

STATUS current  
DESCRIPTION  
    "Information about BGP-4 Authentication."  
::= { bgpAuthenticationPeerEntry 2 }

BgpAuthenticationEntry ::= SEQUENCE {  
    bgpAuthenticationDirection Integer32  
    bgpAuthenticationCode Integer32  
    bgpAuthenticationDataLength Integer32  
    bgpAuthenticationDataContents OCTET STRING  
}

bgpAuthenticationDirection OBJECT-TYPE  
SYNTAX Integer32 {  
    sent (1) -- Authorization is being sent  
    received (2) -- Authorization is being received  
}  
MAX-ACCESS not-accessible

STATUS current  
DESCRIPTION  
"This variable indicates whether authentication information is either being sent by the BGP speaker or has been received by the BGP speaker. It also serves as the index into the table of authentication information for the direction of authentication."  
::= { bgpAuthenticationEntry 1 }

bgpAuthenticationCode OBJECT-TYPE  
SYNTAX Integer32 (-1 | 0..255)  
MAX-ACCESS read-write  
STATUS current  
DESCRIPTION  
"This is the AuthenticationCode used.  
This value is set to -1 if Authentication is not present."  
REFERENCE  
"[RFC 1771](#), sec. 4.2.a"  
::= { bgpAuthenticationEntry 2 }

bgpAuthenticationDataLength OBJECT-TYPE  
SYNTAX Integer32 (-1 | 0..252)  
MAX-ACCESS read-write  
STATUS current  
DESCRIPTION  
"This value is derived from the optional parameter length minus one (the size of bgpAuthenticationCode). This value may be no

larger than 252 due to overhead. This value is set to -1 if Authentication is not present."  
::= { bgpAuthenticationEntry 3 }

bgpAuthenticationDataContents OBJECT-TYPE  
SYNTAX OCTET STRING (SIZE (1..252))  
MAX-ACCESS read-write  
STATUS current  
DESCRIPTION  
"This is the Authentication payload. The semantics of this variable are interpreted

according to the authentication code."  
 ::= { bgpAuthenticationEntry 4 }

bgpCapabilitySupportAvailable OBJECT-TYPE

SYNTAX TruthValue  
MAX-ACCESS read-write  
STATUS current  
DESCRIPTION  
"This variable determines whether BGP-4  
capabilities are supported in this  
implementation. This variable may be set to  
false to disable capability support."  
 ::= { bgp4OptParametersMIB 2 }

bgpSupportedCapabilities OBJECT-TYPE

SYNTAX OCTET STRING (SIZE(0..32)) -- 256 bit vector  
MAX-ACCESS read-only  
STATUS current  
DESCRIPTION  
"Vector of BGP-4 capabilities that are  
supported in this implementation. Capabilities  
are identified via the string of bits within  
this object. The first octet contains bits  
0 to 7, the second octet contains bits 8 to 15  
and so on. If a bit, i, is present and set,  
then the capability (i+1) is supported.  
  
When capabilities are not supported, all bits  
must be zero."  
 ::= { bgp4OptParametersMIB 3 }

bgpPeerCapabilitiesTable OBJECT-TYPE

SYNTAX SEQUENCE OF BgpPeerCapabilitiesEntry  
MAX-ACCESS not-accessible  
STATUS current  
DESCRIPTION  
"This table contains contains the capabilities

that are supported for a given peer."  
 ::= { bgp4OptParametersMIB 4 }

BgpPeerCapabilitiesEntry ::= SEQUENCE {

```

    bgpPeerCapabilitiesAnnounced
        OCTET STRING,
    bgpPeerCapabilitiesReceived
        OCTET STRING
}

bgpPeerCapabilitiesEntry OBJECT-TYPE
    SYNTAX      BgpPeerCapabilitiesEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "These entries are keyed by a BGP-4 peer's remote
        address and port combination over which the
        peering session has been established."
    AUGMENTS { bgpPeerTable }
    ::= { bgpPeerCapabilitiesTable 2 }

bgpPeerCapabilitiesAnnounced OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE (0..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "This bit vector identifies which capabilities
        have been announced to a BGP-4 speaker.

        Capabilities are identified via the string of
        bits within this object.  The first octet
        contains bits 0 to 7, the second octet contains
        bits 8 to 15 and so on.  If a bit, i, is present
        and set, then the capability (i+1) is supported.

        When capabilities are not supported, all bits
        must be zero."
    ::= { bgpPeerCapabilitiesEntry 1 }

bgpPeerCapabilitiesReceived OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE (0..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "This bit vector identifies which capabilities have
        been announced by the remote BGP-4 speaker."

```



Capabilities are identified via the string of bits within this object. The first octet contains bits 0 to 7, the second octet contains bits 8 to 15 and so on. If a bit, *i*, is present and set, then the capability (*i*+1) is supported.

When capabilities are not supported, all bits must be zero."

::= { bgpPeerCapabilitiesEntry 2 }

bgpProtocolExtensions OBJECT-TYPE

SYNTAX AutonomousType

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"Registration point for MIB Modules for BGP Protocol Extensions.

The Capabilities Advertisement RFC delineates IANA registered capability code numbers, 0-127 and private use capability code numbers, 128-255.

The first sub-identifier will be the enterprise number of the registering entity. This is used to remove the ambiguity of the private use portion of the capability code assignments. For IANA registered capability codes 0-127, the first sub-identifier will be 0.

The second sub-identifier will be the capability code for the advertised capability.

For example, the MPBGP-MIB would be assigned as { bgpProtocolStandardExtensions 0 1 } since it has been assigned capability code number 1 and is an IETF assigned (IANA registered) capability extension."

REFERENCE

"[RFC 2842](#) - Capabilities Advertisement with BGP-4"

::= { bgp4OptParametersMIB 5 }

END

#### 4. Intellectual Property

The IETF takes no position regarding the validity or scope of any

Internet Draft

[draft-jhaas-bgp4-mib-opt-00.txt](#)

Februrary 2001

intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in [BCP-11](#). Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

## 5. Acknowledgements

The authors wish to thank Matt Richardson and Shane Wright of NextHop for helpful feedback during the design of this document. The authors wish to particularly thank Bert Wijnen of Lucent for all the help in the MIB layout.

## 6. References

- [1] Rekhter, Y., Li, T., "A Border Gateway Protocol 4 (BGP-4)", [RFC 1771](#), March 1995.
- [2] Chandra, R., Scudder, T., "Capabilities Advertisement with BGP-4", [RFC 2842](#), May 2000.
- [3] Case, J., McCloghrie, K., Rose, M., and S. Waldbusser, "Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)", [RFC 1903](#), SNMP Research, Inc., Cisco Systems, Inc., Dover Beach Consulting, Inc., International Network Services, January 1996.
- [3] Blumenthal, U., and B. Wijnen, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)", [RFC 2274](#), IBM T. J. Watson Research, January 1998.
- [4] Wijnen, B., Presuhn, R., and K. McCloghrie, "View-based

## 7. Security Considerations

There are a number of management objects defined in this MIB that have a MAX-ACCESS clause of read-write:

- +o bgpAuthenticationCode
- +o bgpAuthenticationDataType
- +o bgpAuthenticationDataContents
- +o bgpCapabilitySupportAvailable

These objects should be considered sensitive or vulnerable in most network environments. The support for SET operations in a non-secure environment without proper protection can have a negative effect on network operations. Incorrect configuration of these parameters may cause BGP peer connections to terminate early or to send more routes under a flapping condition.

There are a number of managed objects in this MIB that may be considered to contain sensitive information in the operation of a network. For example, a BGP peer's local and remote addresses may be sensitive for ISPs who want to keep interface addresses on routers confidential to prevent router addresses used for a denial of service attack or spoofing.

Therefore, it may be important in some environments to control read access to these objects and possibly to even encrypt the values of these object when sending them over the network via SNMP. Not all versions of SNMP provide features for such a secure environment. SNMPv1 by itself is not a secure environment. 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.

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 2274](#) [3] and the View-based Access Control Model [RFC 2275](#) [4] 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.

Haas

[Page 10]

---

Internet Draft

[draft-jhaas-bgp4-mib-opt-00.txt](#)

Februrary 2001

## 8. Authors Address

Jeffrey Haas  
NextHop Technologies  
517 Williams  
Ann Arbor, MI 48103-4943  
Phone: +1 734 936 2095  
Fax: +1 734 615-3241  
Email: [jhaas@nexthop.com](mailto:jhaas@nexthop.com)

Susan Hares  
NextHop Technologies  
517 Williams  
Ann Arbor, MI 48103-4943  
Phone: +1 734 936 2095  
Fax: +1 734 615-3241  
Email: [skh@nexthop.com](mailto:skh@nexthop.com)

