Network Working Group
Internet-Draft
Intended status: Informational
Expires: February 15, 2021

D. Abraitis
Hostinger

August 14, 2020

Version Capability for BGP
draft-abraitis-bgp-version-capability-06

Abstract

In this document, we introduce a new BGP capability that allows the advertisement of a BGP speaker's routing daemon version.

This BGP capability is an optional advertisement. Implementations are not required to advertise the version nor to process received advertisements.

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 https://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 February 15, 2021.

Copyright Notice

Table of Contents

1. Introduction

In modern data center designs, we tend to have conventional routers participating in the routing process. And the fleet of routers has different versions of routing daemon. This means that knowing which versions of the routing daemons are running the various routers in the network can be a crucial factor in quickly identifying the root cause of any protocol or network problems.

This BGP capability is an optional advertisement. Implementations are not required to advertise the version nor to process received advertisements.

Information about the version of the routing daemon could also be exchanged in protocols such as LLDP and CDP. However, in containerized environments, it is very hard and not recommended to exchange this information between background processes. Therefore, and to help minimize operational costs, it is helpful to exchange the routing daemon information between BGP peers directly.

2. Specification of Requirements

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 BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Version Capability

Capabilities advertisements with BGP are defined in [RFC5492]. They utilize the BGP Capabilities Optional Parameter that contains one or more triples <Capability Code, Capability Length, Capability Value>. This document defines a new BGP capability, the Version Capability, with Capability Code TBD and Capability Length and Capability Value as described below.

The inclusion of the Version Capability is OPTIONAL. If an implementation supports the inclusion of the capability, the implementation MUST include a configuration switch to enable or disable its use, and that switch MUST be off by default.

The Version Capability is intended principally more to non-production environments where more visibility is needed for troubleshooting purposes. It is NOT RECOMMENDED for use outside single Autonomous System domain or Autonomous System Confederations, except you have a topology with a number of routers each with a separate Autonomous Number.

An implementation that does not recognize or support the Version Capability but which receives one MUST respond as described in [RFC5492] by ignoring the option. An implementation that wishes to complain that its neighbor does not support the Version Capability MAY use the 'Unsupported Capability' Error Subcode of a Notification message as described in [RFC5492].

The triple for the Version Capability is as follows:

Capability Code

TBD by IANA

Capability Length

The Capability Length for the Version Capability MUST be greater than zero. A value of zero SHALL be treated as an encoding error and the entire triple MUST be ignored.

The Capability Length SHOULD be no greater than 64. This is the limit to allow other capabilities as much space as they require.

Capability Value

The Capability Value field is encoded in UTF-8 [RFC3629]. It is unstructured data and can be formatted in any way that the implementor decides.

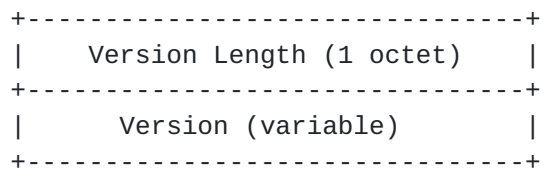

Figure 1

Version Length:

The number of characters in the Version

Version:

The Version encoded via UTF-8

3.1. Capabilities Length Overflow

As defined in [RFC5492] the total length of capabilities that can be carried by the BGP Capabilities Optional Parameter is 255 bytes. If an implementation is constructing a BGP Capabilities Optional Parameter and its length exceeds 255 bytes, it is RECOMMENDED to exclude the Version Capability. An implementation may optimally achieve this by making the Version Capability the last capability triple to add to the Parameter, and only adding it if there is sufficient space to do so.

4. Operation

The Version Capability MUST only be used for displaying the version of a BGP speaker's router daemon to make troubleshooting easier.

Consider a group of routers each with a number of upstream nodes, and suppose that each router has a different operating system and different routing daemon at a different version installed. Assuming that a specific feature is not working or that there is a bug which has not been fixed in a particular version of the code, knowledge of the routing daemon versions would allow an operator to quickly identify the pattern of which versions are affected.

Enabling (i.e., turning on) this capability requires bouncing all existing BGP sessions and the feature MUST be explicitly configured before an implementation advertizes the Version Capability.

4.1. Example Usage

Below is an example of implementation in [FRRouting] how it looks like with version advertised by a BGP sender:

```
:~# vtysh -c 'show ip bgp summary failed'
...
Neighbor EstdCnt DropCnt ResetTime Reason
ens192         3       3  00:00:35 Waiting for peer OPEN (n/a)
ens224         3       3  00:01:12 Waiting for NHT (FRRouting 7.2)
eth0           3       3  00:00:14 Neighbor deleted (FRRouting 7.3)
...
```

Figure 2

```
:~# vtysh -c 'show ip bgp neighbors 198.51.100.1 json' \
> | jq '."198.51.100.1".neighborCapabilities.versions'
{
  "advertisedVersion": "FRRouting 7.2-dev-MyOwnFRRVersion",
  "receivedVersion": "FRRouting 7.2-dev-MyOwnFRRVersion-gc68bb14"
}
```

Figure 3

5. IANA Considerations

IANA maintains the "Border Gateway Protocol (BGP) Parameters" registry with a subregistry called "Capabilities Codes". IANA is requested to assign a capability number from the First Come First Served range for the Version Capability in this document as follows:

Value	Description	Reference
TBD	Version Capability	[This.I-D]

Table 1: Version Capability

6. Security Considerations

The Version Capability should be treated as sensitive information: it could be easier for an attacker to exploit the system if they know the specific version of a BGP speaker. This information could be gathered by inspecting BGP OPEN messages that carry the Version Capability defined in this document. Using encryption to protect the information exchanged in BGP sessions SHOULD, therefore, be carefully

considered when this feature is enabled. Suitable encryption can be achieved by protecting the BGP session using TLS [RFC5246].

Furthermore, knowledge of which versions of code is running on a given router and from which vendor it comes may facilitate a number of social-engineering attacks. This further adds to the desire to protect this information through encryption.

Modifying the information advertised by a router might lead to attacks including bogus software upgrades and also might mask the causes of faults in the network. This can be mitigated by protecting the BGP session using TLS.

Many BGP implementations leave TCP port 179 open in order to be able to establish sessions with new neighbors. This could lead to an attack where a rogue BGP implementation attempts to open a session and learns the version information from the responding peer.

The Version Capability MUST be configurable with a vendor-specific knob to be able to enable or disable the capability. The vendor might implement to disable this capability per neighbor.

It would be safe to enable this for iBGP or inside the same tenant where you have full control and the BGP speaker is behind the exit points.

This capability is NOT RECOMMENDED for eBGP use.

Sensitive information leaks can be minimized by using the [RFC5082] mechanism or firewalls to filter out TCP 179 port from untrusted networks. This capability can be disabled per neighbor, thus the sensitive information can't be disclosed to untrusted neighbors.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC3629] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, DOI 10.17487/RFC3629, November 2003, <https://www.rfc-editor.org/info/rfc3629>.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <https://www.rfc-editor.org/info/rfc5246>.

7.2. Informative References

[FRRouting] Abraitis, D., "FRRouting - BGP Version Capability", 2019, <https://github.com/ton31337/frr/commit/4c566878fd1a7df9f8c84ee03f419c0b00ae444b>.

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, DOI 10.17487/RFC3552, July 2003, <https://www.rfc-editor.org/info/rfc3552>.

Author's Address

Donatas Abraitis
Hostinger
Jonavos g. 60C
Kaunas 44192
LT

Phone: +370 614 18958
Email: donatas.abraitis@hostinger.com