Draft Update: FC-BGP Protocol Specification

https://datatracker.ietf.org/doc/draft-sidrops-wang-fcbgp-protocol/00/

https://datatracker.ietf.org/doc/draft-wang-sidrops-fcbgp-protocol/01/

Zhuotao Liu

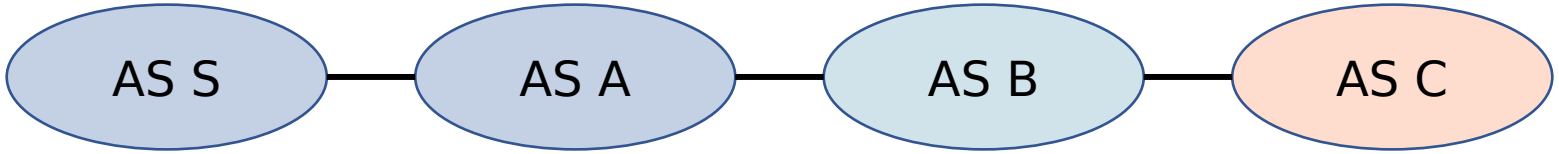
Authors: K. Xu, X. Wang, Z. Liu, Q. Li, J. Wu, and Y. Guo

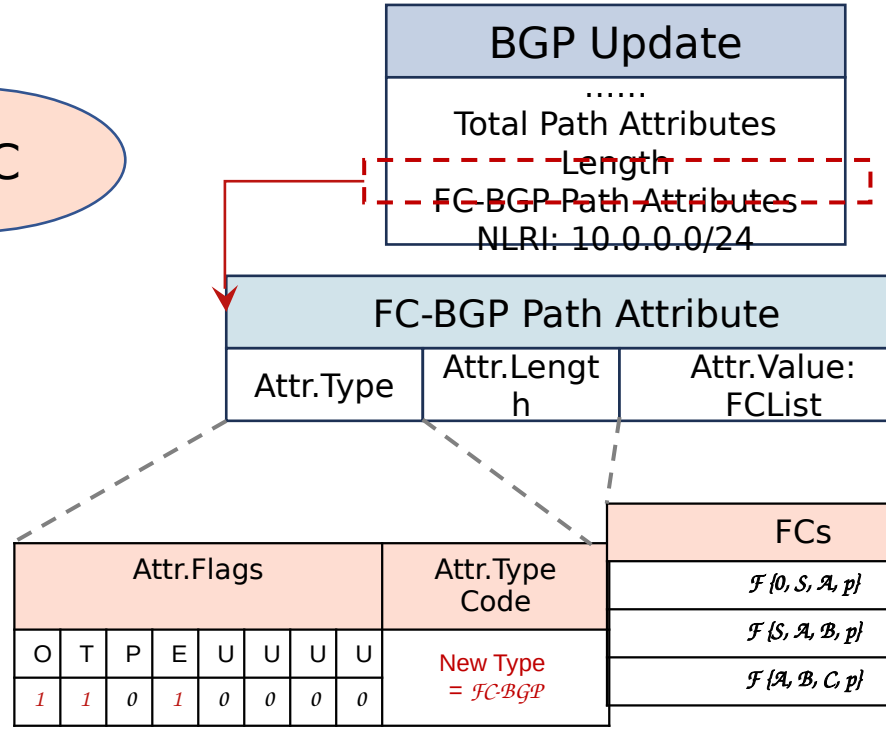
SIDROPS WG
IETF 120
July 2024

Outline of the Talk

- Recap on FC-BGP Basics
- Comments/Suggestions since IETF 119
- Main Changes from v-00 to v-01
- Implementation Status
- Next Steps

Recap on FC-BGP





Suppose AS B receives a BGP update P:$S \leftarrow A \leftarrow$ B, AS B uses the following Forwarding Commitment to publicly certify its routing intent over the next hop to AS C

$$\mathcal{F}_{\{A,B,C,\mathcal{P}\}} = \left\{ \mathcal{H}(A,B,C,\mathcal{P})_{\mathrm{Sig}_B} \,||\, \mathsf{A} \,||\, \mathsf{B} \,||\, \mathsf{C} \right\},$$

(i) FC-BGP adopts a per-pathlet validation scheme for validating BGP updates, instead of the per-path validation scheme used in BPGsec, which has two benefits

1) Same security guarantees as BGPsec in full-deployment, but with much lower path validation overhead in dynamic networks, like the Internet
2) (Strictly) more security benefits than BGPsec in case of partial

Comments/Suggestions since IETF 119

- The draft is somewhat light, lacking necessary materials
- Showing FC-BGP is equivalently secure as BGPsec.
- The impacts to FIB or RIB size, memory consumption and convergence time, etc.
- Should not modify the priority of route selection.
- Where do you implement FC-BGP?
- Clarify certificate and keys for signature signing and what happens when keys refreshed.
- Add considerations of AS Confederation and transparent Route Server
- Comparability: co-existence of FC-BGP with BGP/BGPsec.
- Security Consideration about insertion of ASN 0
- Focusing on only the control plane security

Key Changes from v-00 to v-01

1. We removing the data-plane related content in this version
2. In Sec.1, we add **the key differentiator of FC-BGP** (stressing the partial deployment scenario), describe explicitly that FC-BGP **depends on RPKI,** and cite RPKI's RFCs.
3. In Sec. 2, we explicitly states that negotiating **new capability is unnecessary.**
4. In Sec.4 and Sec.5, we add additional **the protocol descriptions regarding** sending/receiving BGP-UPDATE messages, including AS Confederation, ISP Router Server, etc.
5. In Sec.6, Sec.7, and Sec.8, we further add more **operational considerations, security considerations, and IANA considerations**.

Change No.1: Key Differentiaor with BGPsec

- Text in this v-01

1. Introduction

……

FC-BGP and BGPsec offer different levels of security benefits in the case of partial deployment, even though they achieve the same security benefits when fully deployed.

……

In contrast to BGPsec, FC-BGP treats **partial deployability** as a first-class citizen. It adopts a pathlet-driven authentication paradigm, in which the authenticity of an AS-path can be incrementally built based on authenticated pathlets. This design ensures that downstream FC-BGP-aware ASes can use the authenticated pathlets provided by upstream upgraded ASes, even if the full AS-path traverses legacy ASes that do not support FC-BGP.

……

Change No. 2: RPKI / BGPsec Certificate/Key

- FC-BGP relies on RPKI. It uses BGPsec keys to sign/verify FCs.
- Text in this v-01

  Similar to BGPsec, FC-BGP relies on RPKI to **perform route origin validation** [RFC6483].

  ……

  This certificate is associated with its AS number. The **router key generation** here follows [RFC8208] and [RFC8635].

  ……

  it MUST match the **AS number in the Subject field of the RPKI router certificate** that will be used to verify the FC segment constructed by this FC-BGP speaker (see Section 3.1.1 of [RFC8209] and [RFC6487])

  ……

  FC-BGP only supports one **algorithm suite** in this document as **BGPsec Algorithm** defined in [RFC8208].

Change No.3: Processing BGP UPDATE

- Sending
  - Text in this v-01

4. FC-BGP UPDATE Messages
   4.1. Generation
   4.2. Propagation
   4.3. Processing Instructions for AS Confederation Members

……

- Receiving
  - Text in this v-01

5. Processing a Received FC-BGP UPDATE Message
   5.1. Overview
   5.2. Validation
      5.2.1. Validation Algorithm

Change No.4: Route Selection

- We do not modify the priority of BGP route selection in FC-BGP. Instead, we leave route section to local policy.
- Text in this v-01

6.4. BGP Route Selection

While FC-BGP does modify the BGP route selection result, it is not the primary intention of FC-BGP to modify the BGP route selection process itself. Instead, FC-BGP focuses on providing an additional layer of validation and verification for BGP UPDATE messages.

However, the handling of FC-BGP validation states, as well as the integration of FC-BGP with the BGP route selection, **is indeed a matter of local policy.** FC-BGP implementations SHOULD provide mechanisms that allow operators to define and configure their own local policies on a **per-session basis.**

……

Change No.5: AS Confederation

- The leftmost bit of the Flags field: Confed_Segment flag (Flags-CS)
- Text in this v-01

3. FC Path Attribute

……

The leftmost bit of the Flags field in Figure 2 is the **Confed_Segment flag (Flags-CS).** The Flags-CS flag is **set to 1** to indicate that the FC-BGP speaker that constructed this FC segment is sending the UPDATE message to a peer AS within the same AS confederation [RFC5065]. (That is, a sequence of consecutive Confed_Segment flags are set in an FC-BGP UPDATE message whenever, in a non-FC-BGP UPDATE message, an AS_PATH segment of type AS_CONFED_SEQUENCE occurs.) In all other cases, the Flags-CS flag is **set to 0**.

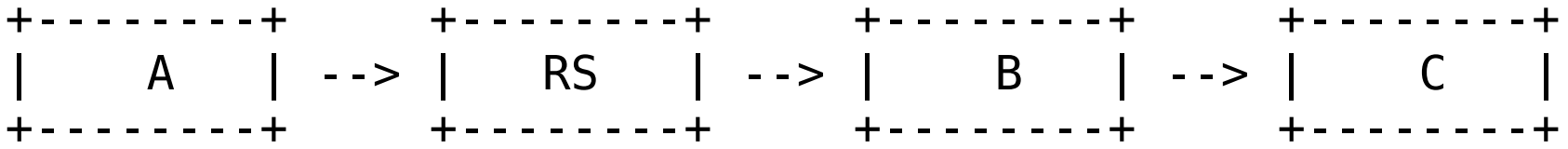
……

4.3. Processing Instructions for AS Confederation Members

……

Change No.6: Route Server

- The second leftmost bit (i.e., the second highest) of the Flags field is the Route_Server flag (Flags-RS).
- Text in [4.1. Generation; 5.2.1. Validation Algorithm; 7. Security Considerations]



RS inserts ASN into AS path.

1. FC(0, A, RS) by AS A
2. FC(A, RS, B) by RS
3. FC(RS, B, C) by AS B

RS acts like a typical FC-BGP-enabled AS.

RS does not insert ASN into AS path.

1. RS populates its FC segment into FCList.
   1. FC(0, A, RS) by AS A
   2. FC(A, RS, B, **Flags-RS**) by RS
   3. FC(RS, B, C) by AS B
2. RS fails to populate FC segment.
   1. FC(0, A, RS) by AS A
   2. FC(RS, B, C) by AS B

A typical partial deployment case

Change No. 7: Inserting ASN 0

- Text in this v-01

7.3.1. Three AS Numbers

……

In the context of BGP [RFC4271], to detect an AS routing loop, it scans the full AS path (as specified in the AS_PATH attribute) and checks that the autonomous system number of the local system does not appear in the AS path. As outlined in [RFC7607], Autonomous System 0 was listed in the IANA Autonomous System Number Registry as "Reserved - May be used to identify non-routed networks". So, **there should be no AS 0 in the AS_PATH attribute of the BGP UPDATE message**. **Therefore, AS 0 could be used to populate the PASN field when no previous AS hops in the AS path.**

Implementation Status

- FRR: based on FRR 9.0.1
  - FC Path Attribute
    - SIG = ECDSA(SHA256(PASN, CASN, NASN, Address, Prefixlen))
    - Sign FC with ECDSA-SHA256 when sending BGP UPDATE
    - FC Verification when receiving BGP UPDATE
  - Keys: Loading from files
  - TODO:
    - AS Confederation, Route Server, AS Path Prepending, etc.
    - RPKI Keys
- Dev. and Test Env.
  - OS: Ubuntu 22.04
  - OpenSSL 3.0.2
- H3C: commercial release, in testing
  - Device: CR19000 Series
  - FC Path Attribute
    - SIG = ECDSA(SHA256(PASN, CASN, NASN, Address, Prefixlen))
    - Sign FC with ECDSA-SHA256 when sending BGP UPDATE
    - FC Verification when receiving BGP UPDATE
  - Keys: Generates within the router

Next Steps

- We are looking forward to WG Adoption.

Questions? Feedback?

Comments are welcomed.

https://datatracker.ietf.org/doc/draft-wang-sidrops-fcbgp-protocol/01/

Please email feedback to

draft-wang-sidrops-fcbgp-protocol@ietf.org

or, open issues at

https://github.com/FCBGP/fcbgp-protocol