Authors: Chen, Ed.   L. Su
         China Mobile   China Mobile

the extensions of BGP-LS to carry security capabilities

Abstract

The goal is to collect the security capabilities of nodes, which will be one of the factors to form the routing topology, and use the routing programming capabilities to form a secure routing path.

The BGP-LS protocol is extended to carry the security capabilities of the node. The controller collects topology information, forms a topology path with security capabilities according to security requirements, and supports SRv6 path sending to execute node forwarding through programming.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The most important reason for using BGP-LS as the extended basic
protocol is that BGP-LS shields the differences of other routing
protocols, and the underlying routing protocol types do not need to
be considered when transmitting security capabilities.

RFC7752 standardized North-Bound Distribution of Link-State and
Traffic Engineering (TE) Information Using BGP, describes a
mechanism by which link-state and TE information can be collected
from networks and shared with external components using the BGP
routing protocol, using a new BGP Network Layer Reachability
Information (NLRI) encoding format.

BGP-LS is a new way to collect network topology. The topology
information discovered by the IGP protocol is summarized by the BGP
protocol and sent to the upper controller. With the powerful routing
and routing capabilities of the BGP protocol, there are three types
of BGP-LS routes, which are used to carry node, link and route
prefix information respectively. The three routes cooperate with
each other to complete the transmission of topology information. The
node routing function is to record the node information of the
topology, the link routing function is to record the link
information between two devices, and the address prefix routing

function is to record the network segment information that the node
can reach.

The state information NLRI collected by BGP-LS is described in TLV
(type/length/value triplet) format. Each link state described by
NLRI can identify a node, link or prefix. Therefore, three types of
NLRI are newly set in the standard, of which type 3 and 4 are used
to distinguish the prefix of IPv4 and IPv6. There are only two types
of NLRI attributes in the original BGP protocol: MP_ REACH_ NLRI,
attribute type 14; MP_ UNREACH_ NLRI, attribute type 15.

2. BGP-LS node type carries security capability

2.1. Collection model of security capabilities

```
                    +----------+
            +--------+Controller+-----------+
            |          +----------+         |
      BGP-LS(Node)                          |
            |                               |
XXXXXXXX|XXXXXXXXX                          |
X         |       X                         |
X    +-----+-+    X                 +-----+-+
X    |Router |    X                 |Router |
X    +----+--+    X                 +-+---+-+
X         |       X                   |   |
X         |       X          +------+  |
X         |       X          |       |
X    +----+----+  X      +---+----+  +--+-----+
X    |Security |  X      |Security|  |Security|
X    |Products |  X      |Products|  |Products|
X    +---------+  X      +--------+  +--------+
XXXXXXXXXXXXXXXXXX
```

Figure1: Router and attached security products are used as node units

2.2. New Node Attribute TLVs

The Local Node Descriptors TLV contains Node Descriptors for the
node anchoring the local end of the link. This is a mandatory TLV in
all three types of NLRIs (node, link, and prefix).

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|              Type             |             Length            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
//             Node Descriptor Sub-TLVs (variable)            //
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2: Local Node Descriptors TLV Format

Node attribute TLVs are the TLVs that may be encoded in the BGP-LS
attribute with a Node NLRI. The following Node Attribute TLVs are
defined:

TLV Code Point	Description	Length
263	Multi-Topology Identifier	variable
1024	Node Flag Bits	1
1025	Opaque Node Attribute	variable
1026	Node Name	variable
1027	IS-IS Area Identifier	variable
1028	IPv4 Router-ID of Local Node	4
1029	IPv6 Router-ID of Local Node	16

Table 3: Node Attribute TLVs

The security capability is transferred by adding the security
capability attribute to the attributes of the local node.

TLV Code Point	Description	Length
1030	Node Security Capability	variable

Table 4: New Node Attribute TLV

2.3. Usage of new attribute

When programming the routing path, take the security capability
requirement as one of the inputs. The description of the security
capability requirement can be structured or one-dimensional matrix,
which only needs to be consistent with the router's security
capability description; There are many routing rules. After
introducing security capability requirements, it is necessary to
dynamically adjust the security capability as the position of
routing rules according to the requirements. The main rule
strategies are: ① Select the routing node that meets the
security requirements as the forwarding node when the path is
reachable; ② Select the shortest path when all the safety
requirements are met; ③ When the same path length and security
requirements are met, select the path with small load for
forwarding.

3. BGP-LS Link type carries security capability

3.1. Collection model of security capabilities

```
                  +----------+
         +--------+Controller+-----------+
         |        +----------+           |
         |                               |
         |                               |
xxxxxxxxxxxxxxxxxxx                       |
x           |     x                       |
x    +-----+-+    x  BGP-LS(Link)    +-----+-+
x    |Router |----x------------------|Router |
x    +----+--+    x                  +-+---+-+
x         |       x                    |   |
x         |       x             +------+   |
x         |       x             |          |
x    +----+----+  x         +---+----+  +--+-----+
x    |Security |  x         |Security|  |Security|
x    |Products |  x         |Products|  |Products|
x    +---------+  x         +--------+  +--------+
xxxxxxxxxxxxxxxxxxx
```
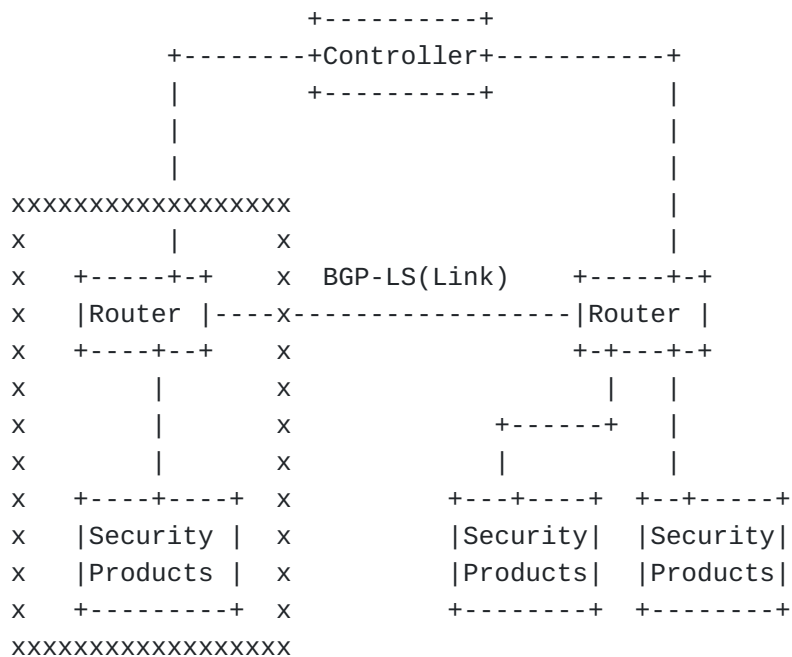
Figure 5: The peer node transmits the security capability through the li

The router and its attached security products are the basic units.
When collecting status information, only some nodes can directly
transmit the node status information to the controller through the
BGP-LS protocol. Other nodes that do not directly transmit the node
information need to transmit the node information to the direct node
to achieve the transmission of security capability information.
Therefore, for non direct nodes, It is required to report its own

security capability information through the BGP-LS link state data
packet.

3.2. New Link Attribute TLVs

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+
|  Protocol-ID  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Identifier                           |
|                           (64 bits)                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
//              Local Node Descriptors (variable)             //
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
//             Remote Node Descriptors (variable)            //
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
//                 Link Descriptors (variable)               //
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
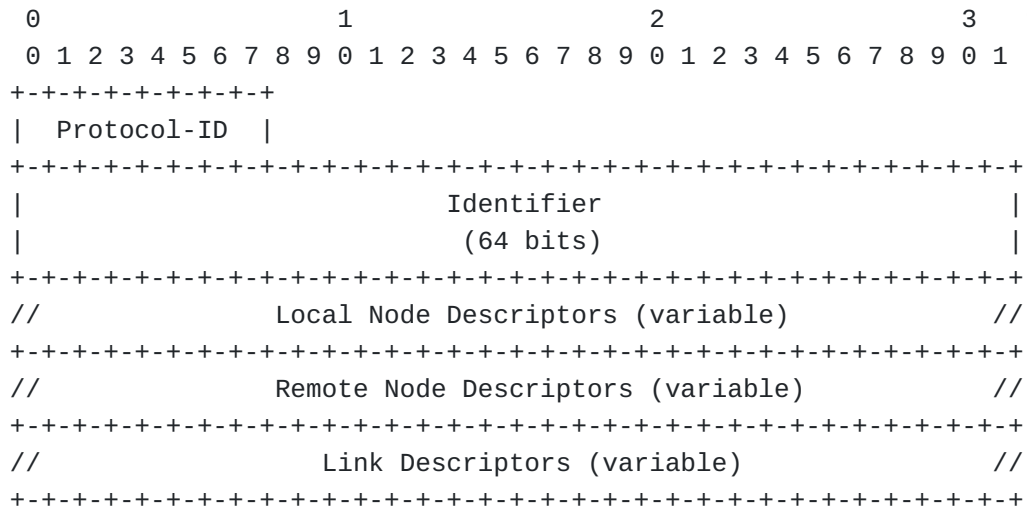
Figure 6: The Link NLRI Format

TLV Code Point	Description	IS-IS TLV /Sub-TLV
1028	IPv4 Router-ID of Local Node	134/---
1029	IPv6 Router-ID of Local Node	140/---
1030	IPv4 Router-ID of Remote Node	134/---
1031	IPv6 Router-ID of Remote Node	140/---
1088	Administrative group (color)	22/3
1089	Maximum link bandwidth	22/9
1090	Max. reservable link bandwidth	22/10
1091	Unreserved bandwidth	22/11
1092	TE Default Metric	22/18
1093	Link Protection Type	22/20
1094	MPLS Protocol Mask	---
1095	IGP Metric	---
1096	Shared Risk Link Group	---
1097	Opaque Link Attribute	---
1098	Link Name	---

Table 7: Link Attribute TLVs

The new attribute describes the link security capability and transmits the link security capability information through this attribute.

TLV Code Point	Description	IS-IS TLV /Sub-TLV
1099	Link security info	---

Table 8: New Link Attribute TLVs

3.3. Useage of new attribute

```
+------+              +------+
|  A   |              |  B   |
+---+--+              +--+---+
    |SCicg A          |
    +--------------->|
    |         SCing B |
    <----------------+
    |SCing <A,B>      |
    +--------------->
    |                |
```
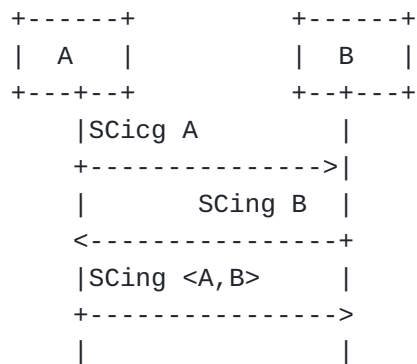
Figure 9: Assosiation security capability interaction

The Assosiation security capability depends on the security
capability enabled by the node. As a node directly connected to the
controller, node B first interacts with the enabled security
capability information of the opposite end in a two-way manner, and
then the opposite end initiates the transmission of the assosiation
security capability information.

The decision of assosiation security capability can be divided into
two situations: one is under the same security domain, and the other
is under different security domains. 1. The decision rules for link
security capabilities under different security domains are as
follows: SCing represents the enabled security capabilities of a
node. Example: SCing A=[1,0,0,1,0,......]，SCing
B=[1,1,0,1,0,......]，SCing Assosiation<A,B> = SCing A &&
SCing B

When the link passes through more than two nodes, it is necessary to
logically and operate the security capabilities of all nodes in the
path to obtain the link security capabilities.

   1. The decision rules of assosiation security capability in the
      same security domain are as follows: SCing indicates the
      security capability of a node that has been enabled. Example:
      SCing A=[1,0,0,1,0,......]，SCing
      B=[1,1,0,1,0,......]，SCing Assosiation<A,B> = SCing A ||
      SCing B

When the link passes through more than two nodes, it is necessary to
logically or operate the security capabilities of all nodes in the
path to obtain the link security capabilities.

4. BGP-LS Prefix type carries security capability

4.1. Collection model of security capabilities

```
     +----------+                    +----------+
     +Controller+                    +Controller+
     +----------+                    +----------+
          |                               |
          | AS 100                        |
xxxxxxxxxxxxxxxxxx                        |AS 200
x         |       x                xxxxxxx|xxxxxxxx
x    +-----+-+    x  BGP-LS(Prefix) x +-----+-+   x
x    |RouterA|----x-----------------x--|RouterE|   x
x    +----+--+    x                   x +-+---+-+   x
x         |       x         xxxxxxxxxx  |   |       x
x         |       x         x    +------+   |       x
x         |       x         x    |          |       x
x    +----+--+    x         x +---+--+  +--+---+    x
x    |Router |    x         x |Router|--|Router|    x
x    +-------+    x         x +------+  +------+    x
xxxxxxxxxxxxxxxxxx          xxxxxxxxxxxxxxxxxxxxxxxxxx
```
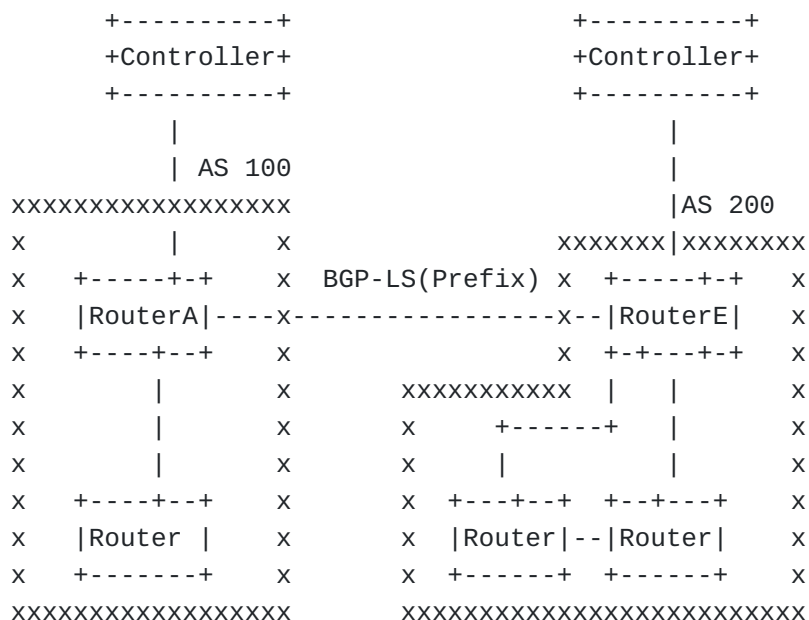
Figure 10: Security capability is transferred between ASs through Prefix

   The router and its attached security products are the basic units.
   When collecting the status information, only some nodes can directly
   transmit the node status information to the controller through the
   BGP-LS protocol. Other nodes that do not directly transmit the node
   information need to transmit the node information to the directly
   connected node to achieve the transmission of security capability
   information. In the figure, nodes A and E are direct connected
   nodes, which are connected to their respective controllers. Nodes A
   and E are responsible for collecting the security capabilities of
   other nodes in their respective fields.

4.2. New Link Attribute TLVs

   The IPv4 and IPv6 Prefix NLRIs (NLRI Type = 3 and Type = 4) use the
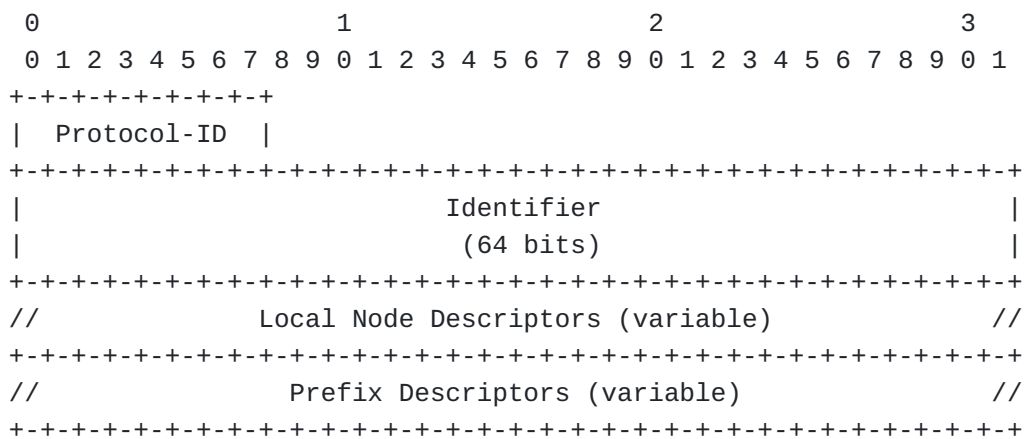   same format, as shown in the following figure.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+
|  Protocol-ID  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Identifier                           |
|                          (64 bits)                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
//              Local Node Descriptors (variable)             //
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
//                 Prefix Descriptors (variable)             //
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

          Figure 11: The IPv4/IPv6 Topology Prefix NLRI Format

TLV Code Point	Description	Length
1152	IGP Flags	1
1153	IGP Route Tag	4*n
1154	IGP Extended Route Tag	8*n
1155	Prefix Metric	4
1156	OSPF Forwarding Address	4
1157	Opaque Prefix Attribute	variable

          Table 12: Prefix Attribute TLVs

An AS has at least one super direct connection node, which has the
security capability information of all nodes under the AS. By adding
new attributes to Prefix, the security capabilities of the entire AS
can be transferred.

TLV Code Point	Description	Length
1158	AS security capabilities	variable

AS Security capabilities means the security capability information
of all nodes under the AS, that is, the security capability
information of all nodes is spliced, such as {[IP address (A)+node
security capability], [IP address (B)+node security capability]...}.

4.3. Usage of new attribute

5. IANA Considerations

   This memo includes no request to IANA.

6. Security Considerations

   TBD

Authors' Addresses

   Meiling Chen (editor)
   China Mobile
   BeiJing
   China

   Email: chenmeiling@chinamobile.com

   Li Su
   China Mobile
   BeiJing
   China

   Email: suli@chinamobile.com