Secure Routing

Meiling Chen
China Mobile
3/14/2023

Requirements

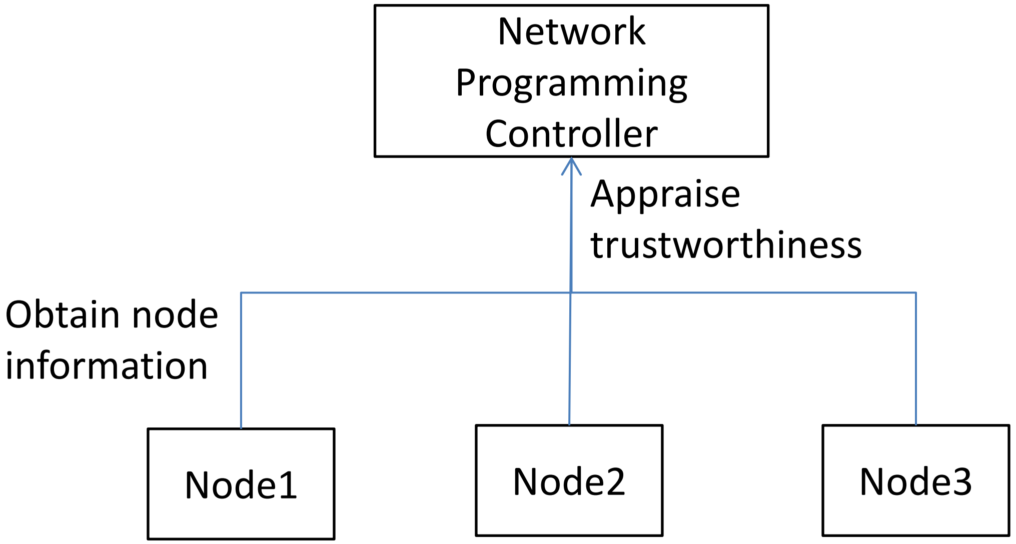
- Network connectivity is becoming increasingly widespread, application and industry integration are increasingly close, users have customized security requirements for network providers over connections, such as high security communication links, high security level routing devices, and customizable security services (DDoS, WAF and so on).
- Currently, IP protocol is only focus on the accessibility of the optimal transmission path, but lacks the ability to secure routing and service scheduling from the perspective of users and individual network providers. For example, power production systems used for power distribution require physical isolation; for telemedicine, low latency, high reliability, and anti DDoS are required.

Analysis of use cases

- Basic path security: from the perspective of node/link security status of network operators, secure routing for users.
- Differentiated security service: from the perspective of customized security services for users, users obtain secure routing and security services.

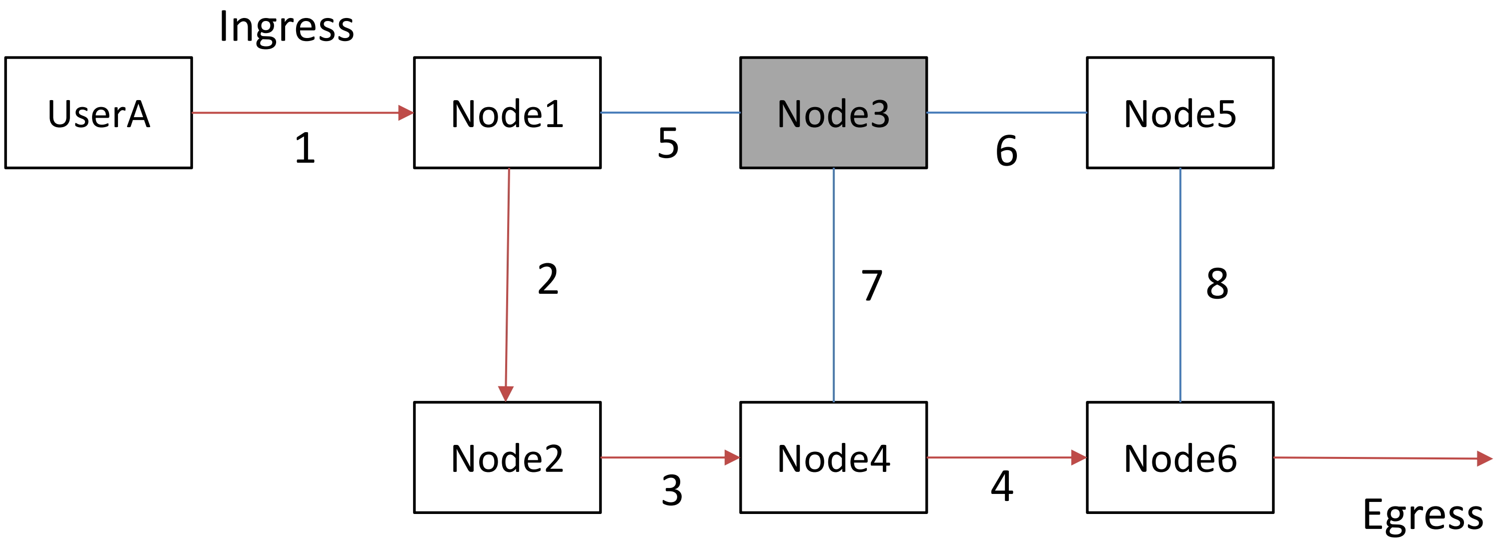
Use case1: basic path security

- Routing policy ensure transmission security based on network node security ppraisal;
- Function 1: Network programming controller obtain the information of nodes and appraise the trustworthiness.



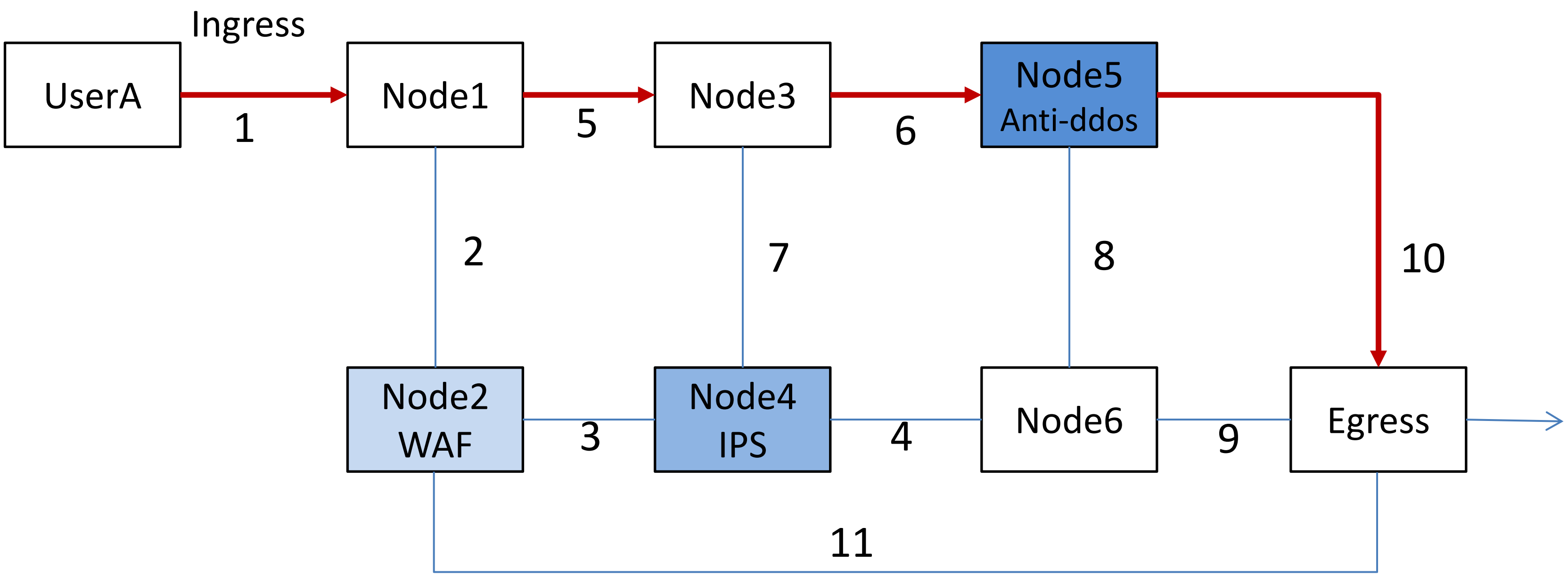
Use case1: basic path security

- Function 2: Routing policy is based on the trustworthiness of nodes, ensure link forwarding security.
- for example Node3 with poor trustworthiness, important users will avoid Node3 for routing policy. Figure describes userA's link forwarding process avoids Node3,select path<1,2,3,4>.



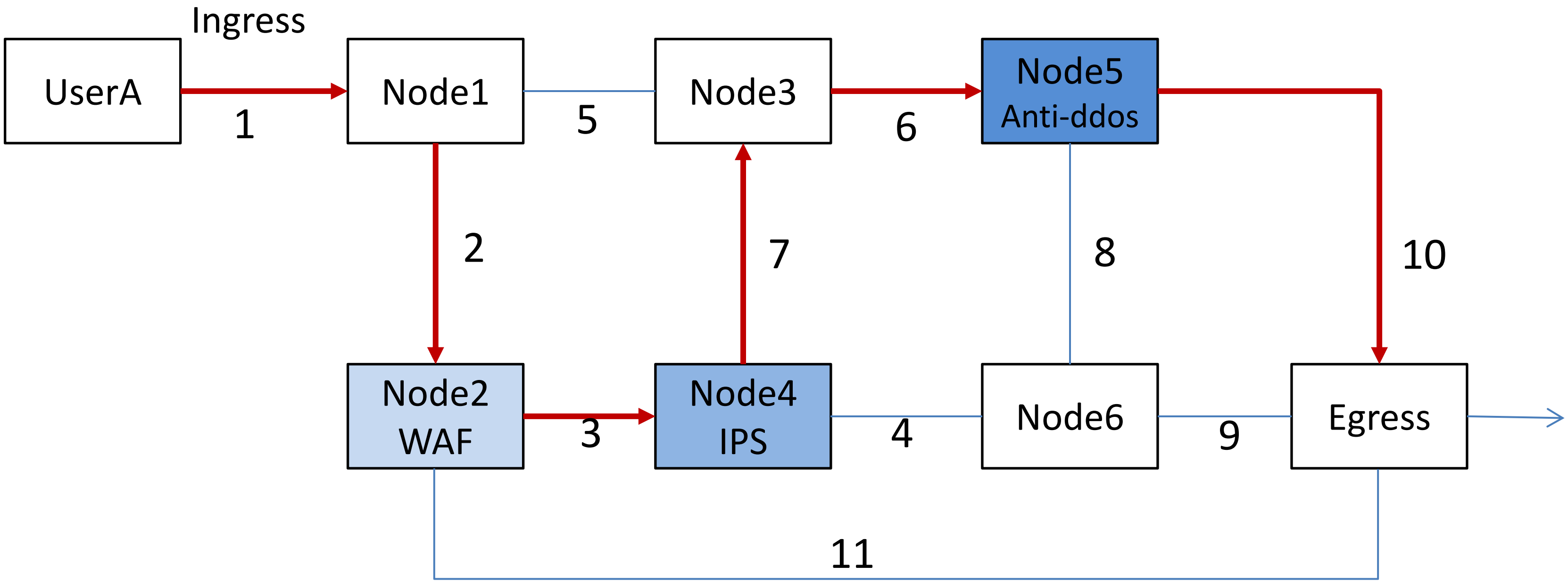
Use case2: Differentiated security service

- For customers with specific security requirements, ISPs need to transmit data at the security level expected by customers.
- Example1: When userA needs Anti-ddos services, the secure routing must pass   through Node5, Figure4-1 shows the path<1,5,6,10> selected for UserA   which require anti-ddos service.



Use case2: Differentiated security service

- Example2: When userA needs IPS, WAF and Anti-ddos services, the secure routing must pass through Node4, Node2 and Node5, Figure4-4 shows the path<1,2,3,7,6,10> selected for UserA which require IPS, WAF and Anti-ddos services.

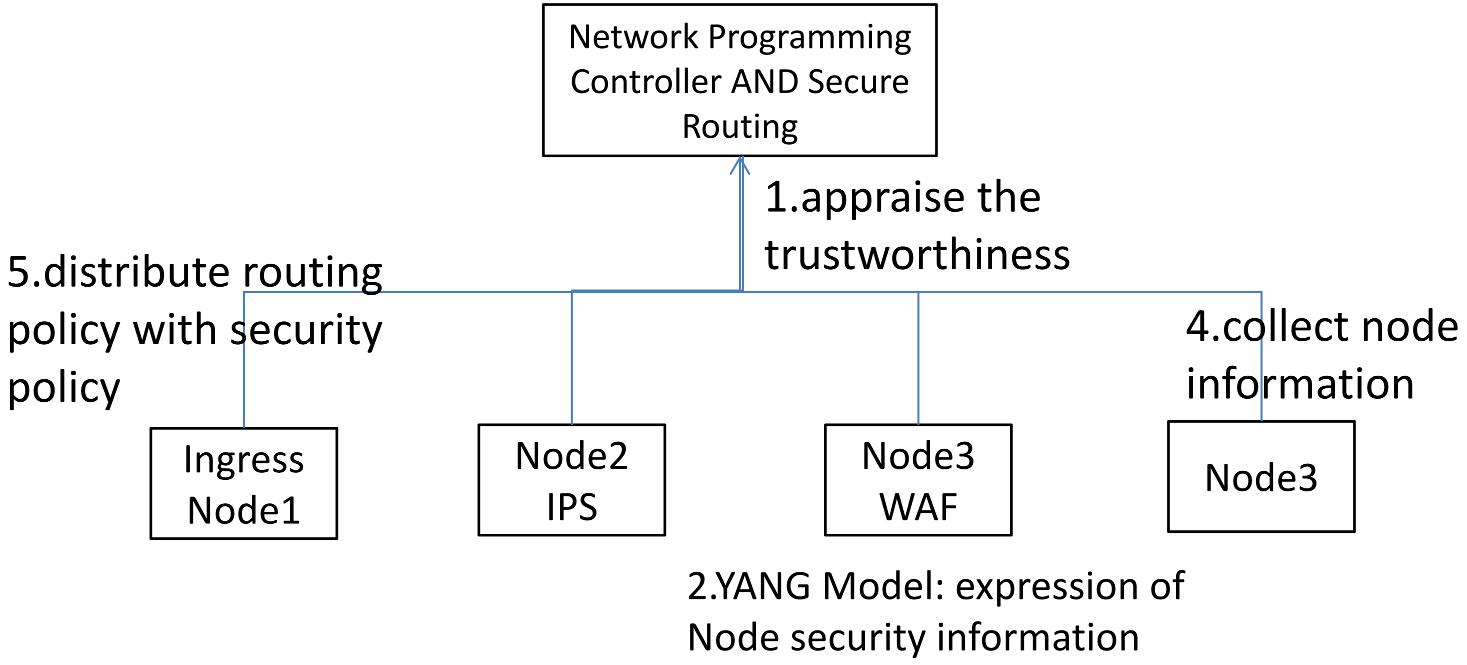


Target of secure routing

- Secure routing is to converge security and routing ,ensure the secure data transmission.
- The purpose is to add security factor in the routing process.
- Secure routing is a distributed security service.
- The scope is transmission process security, while end-to-end security and application layer security are out of scope.

functions required to implement secure routing.

1. Static node security, by appraising the trustworthiness(doing);
2. Expression of node security capability, by YANG Model(to do);
3. Type of security functions: reorganize and define the security functions supported by existing network devices(doing);
4. Protocol for collecting node security capabilities, such as adding new parameters to BGP-LS(doing);
5. A protocol for distributing security policy configuration, such as by SRv6(to do);


Network Programming Controller AND Secure Routing
1.appraise the trustworthiness
5.distribute routing policy with security policy
4.collect node information
Ingress Node1
Node2 IPS
Node3 WAF
Node3
2.YANG Model: expression of Node security information

4 related drafts

1. **draft-chen-secure-routing-use-cases-02**

   https://datatracker.ietf.org/doc/html/draft-chen-secure-routing-use-cases-02

2. **draft-chen-secure-routing-requirements-01**

   https://datatracker.ietf.org/doc/html/draft-chen-secure-routing-requirements-01

3. **draft-chen-atomized-security-functions-00**

   https://datatracker.ietf.org/doc/html/draft-chen-atomized-security-functions-00

4. **draft-chen-bgp-ls-security-capability-00**

   https://datatracker.ietf.org/doc/html/draft-chen-idr-bgp-ls-security-capability-00

Next To Do

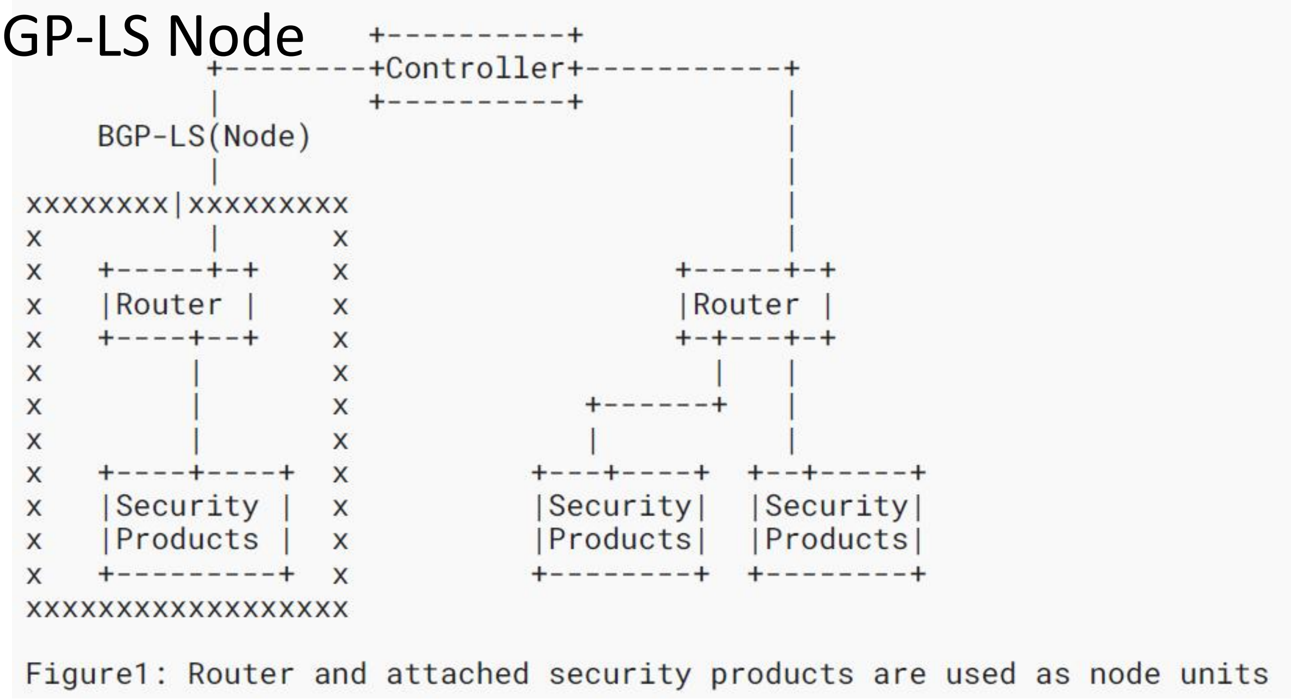
- Want to know how many people are interested in this?
- Put forward a protocol for distributing security policy configuration.

Appendix

How to get node's security capabilities

- Extended BGP-LS(RFC7752) protocol to carry the security capabilities of the node.

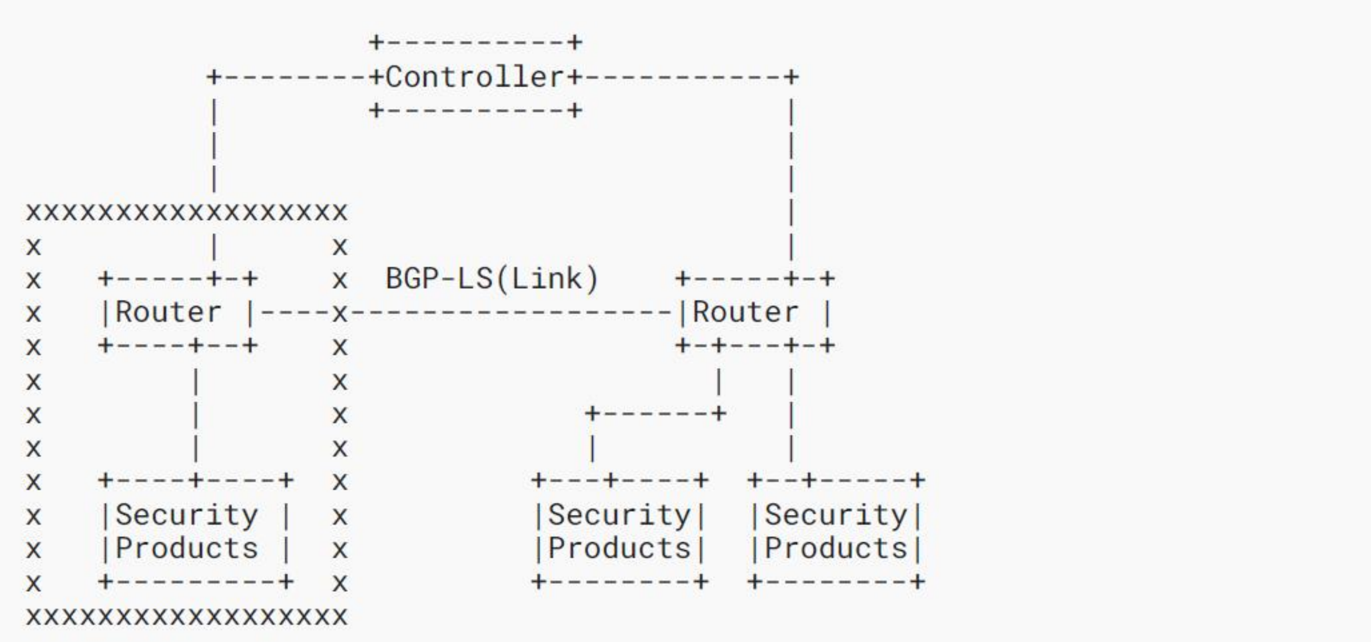
1. Carrying the security capability of the local node through the BGP-LS Node



```
                   +----------+
          +--------+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

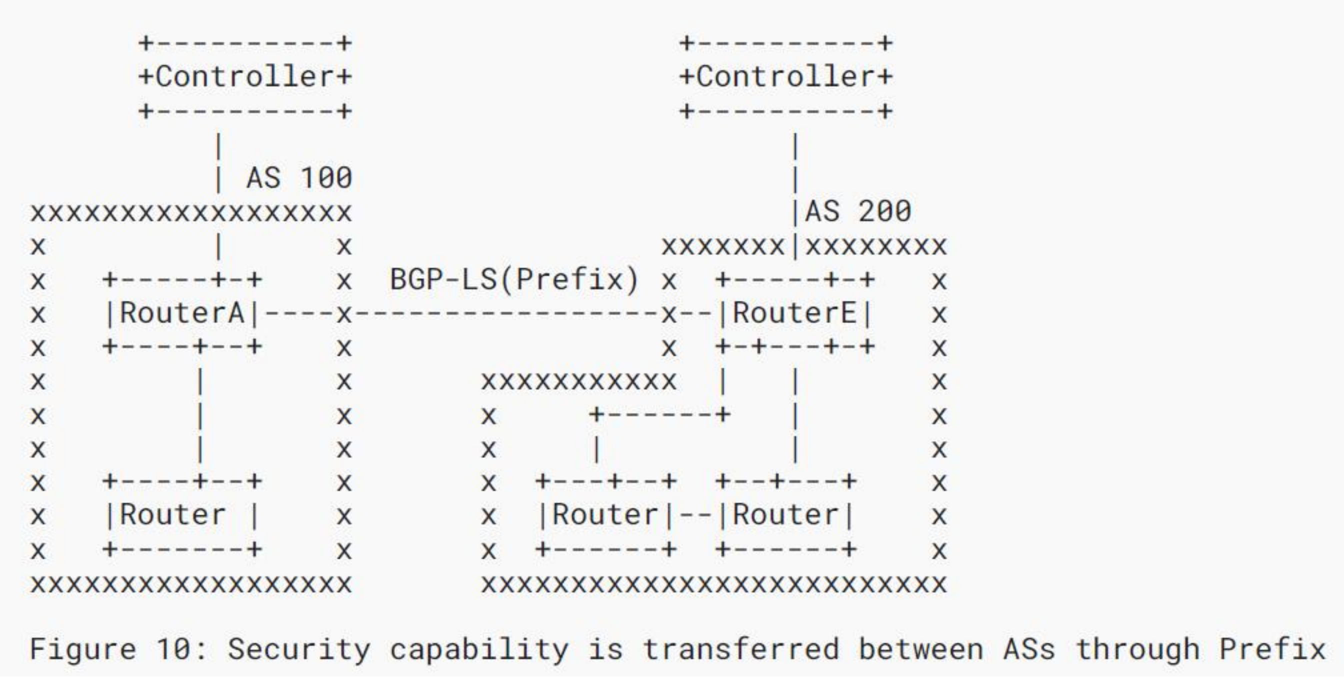
2. Carrying the security capability of the remote node through the BGP-LS Link



```
                   +----------+
          +--------+Controller+-----------+
          |        +----------+           |
          |                               |
          |                               |
xxxxxxxxxxxxxxxxxx                        |
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          +--------+  +--------+
xxxxxxxxxxxxxxxxxx
```

Figure 5: The peer node transmits the security capability through the link

3. Carrying the security capability of the AS through the BGP-LS Prefix

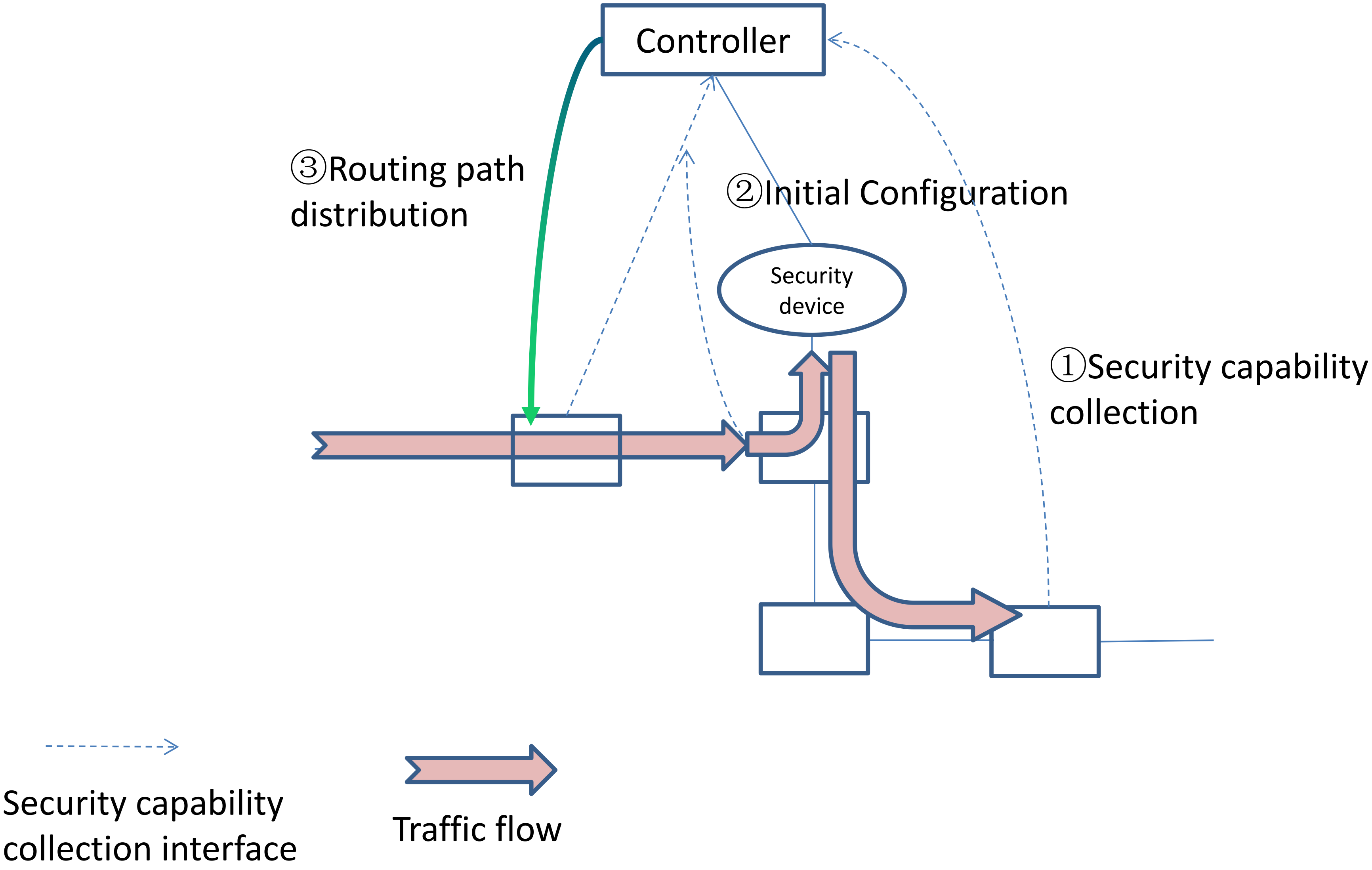


```
      +----------+                  +----------+
      +Controller+                  +Controller+
      +----------+                  +----------+
          |                               |
          | AS 100                        |
xxxxxxxxxxxxxxxxxx                        |AS 200
x         |      x                 xxxxxxx|xxxxxxxx
x   +-----+-+    x  BGP-LS(Prefix) x  +-----+-+   x
x   |RouterA|----x-----------------x--|RouterE|   x
x   +----+--+    x                 x  +-+---+-+   x
x        |       x       xxxxxxxxxxx  |   |       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

draft-chen-bgp-ls-security-capability-00
https://datatracker.ietf.org/doc/draft-chen-bgp-ls-security-capability/

Interfaces



Controller

③Routing path distribution

②Initial Configuration

Security device

①Security capability collection

Security capability collection interface

Traffic flow