

# Secure Routing

draft-chen-secure-routing-requirements-00

draft-chen-atomized-security-functions-00

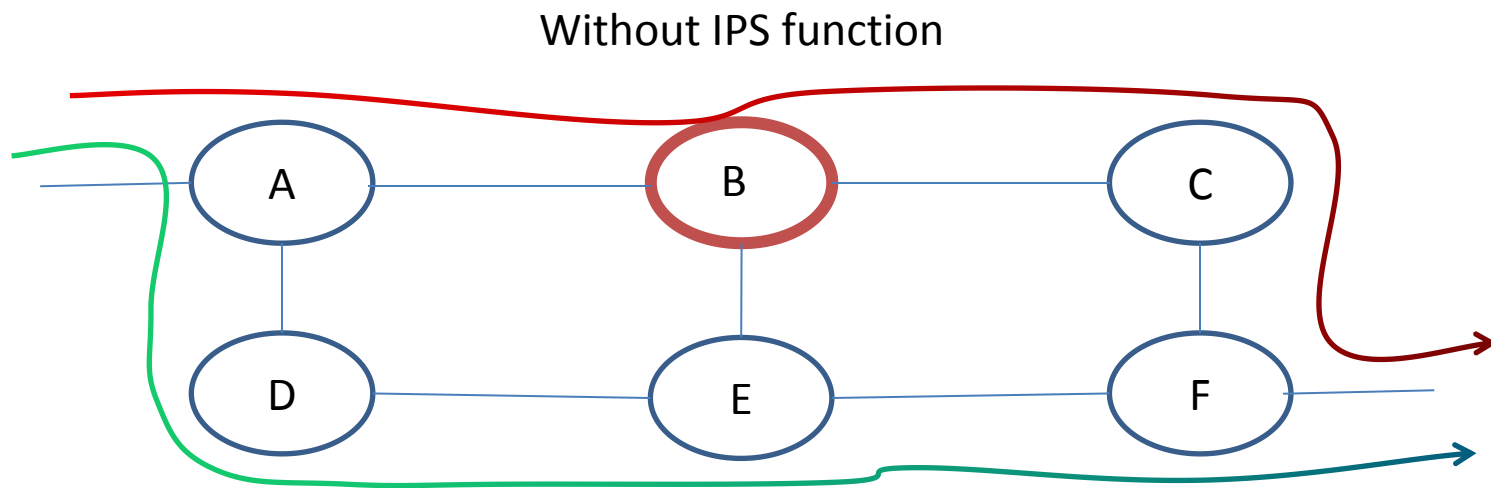
draft-chen-bgp-ls-security-capability-00

China Mobile

10/27/2022

# What does secure routing do?

- Provide security services for user link transmission



<Src A, Dst F> traffic flow with IPS security requirements should avoid Node B.

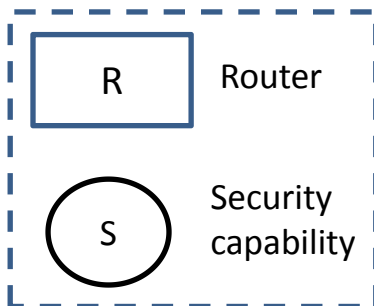
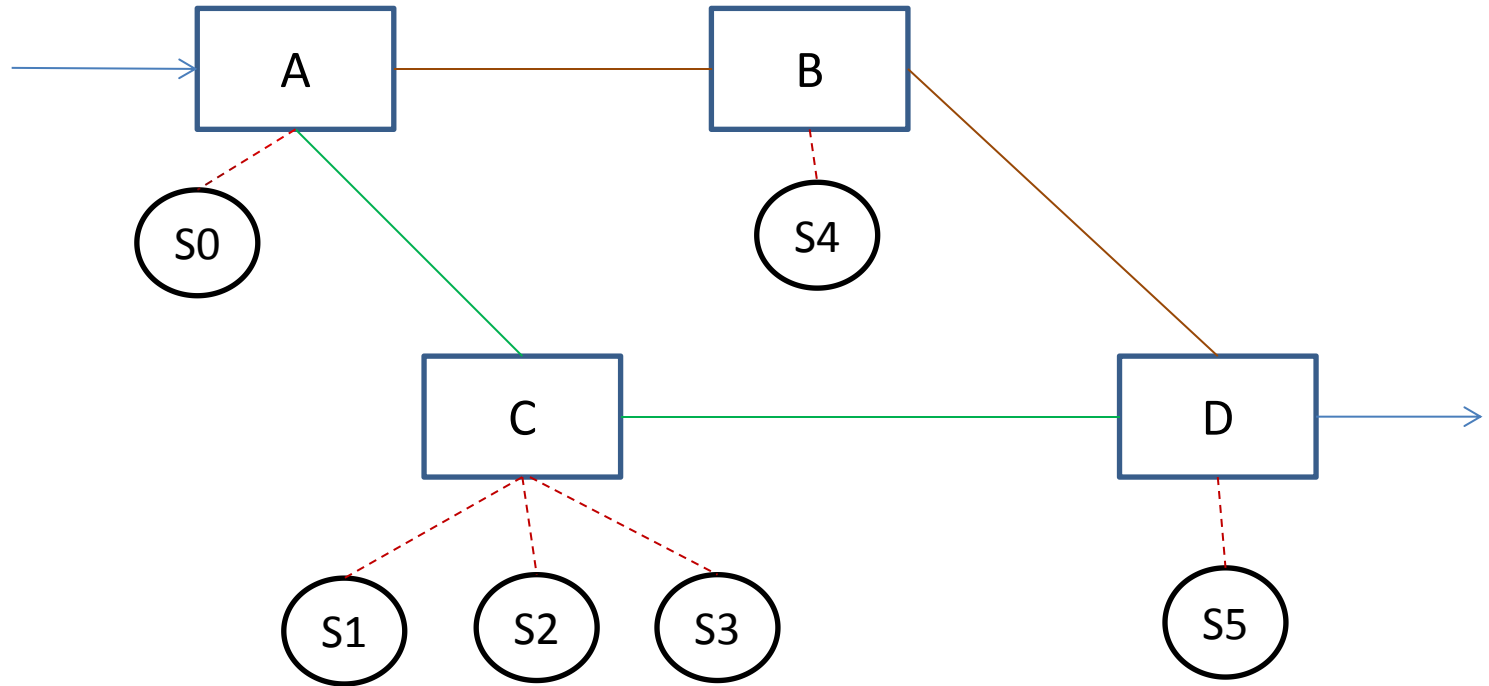
# Why secure routing is required?

- To network operators:
  1. provide users with differentiated security capabilities/services.
  2. Network defense, reduce malicious users' attacks on the network.
- To users: select the network path according to the business security requirements.

# Why can't the existing technology do Secure Routing

- The management and use of existing security devices are separated from the IP network;
- Network routing strategy is independent of security;

# Secure routing Model



# What security capabilities are provided

- Anti-DDoS
- IPS
- IDS
- ...

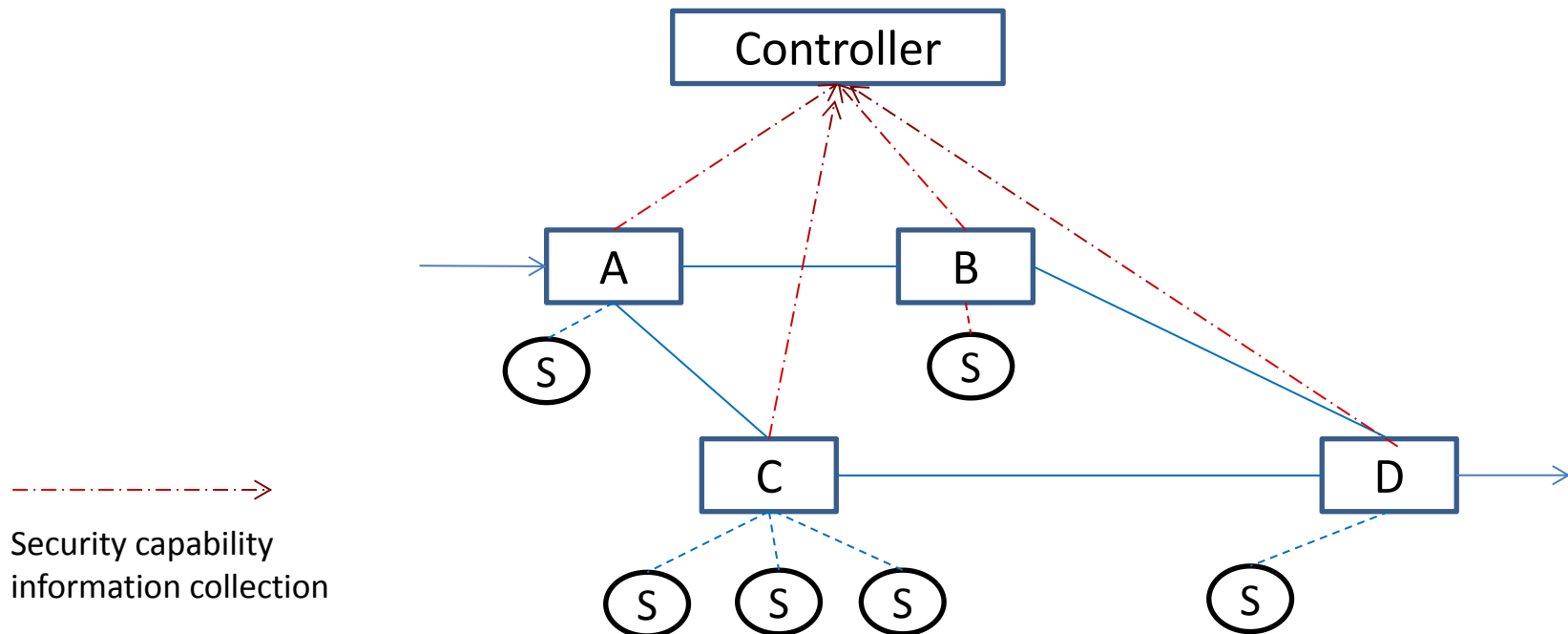
According to the IPDRR model to classify the capabilities of existing security products into 23 security capability categories.

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

- <https://datatracker.ietf.org/doc/draft-chen-atomized-security-functions/>

# What to do for Secure Routing

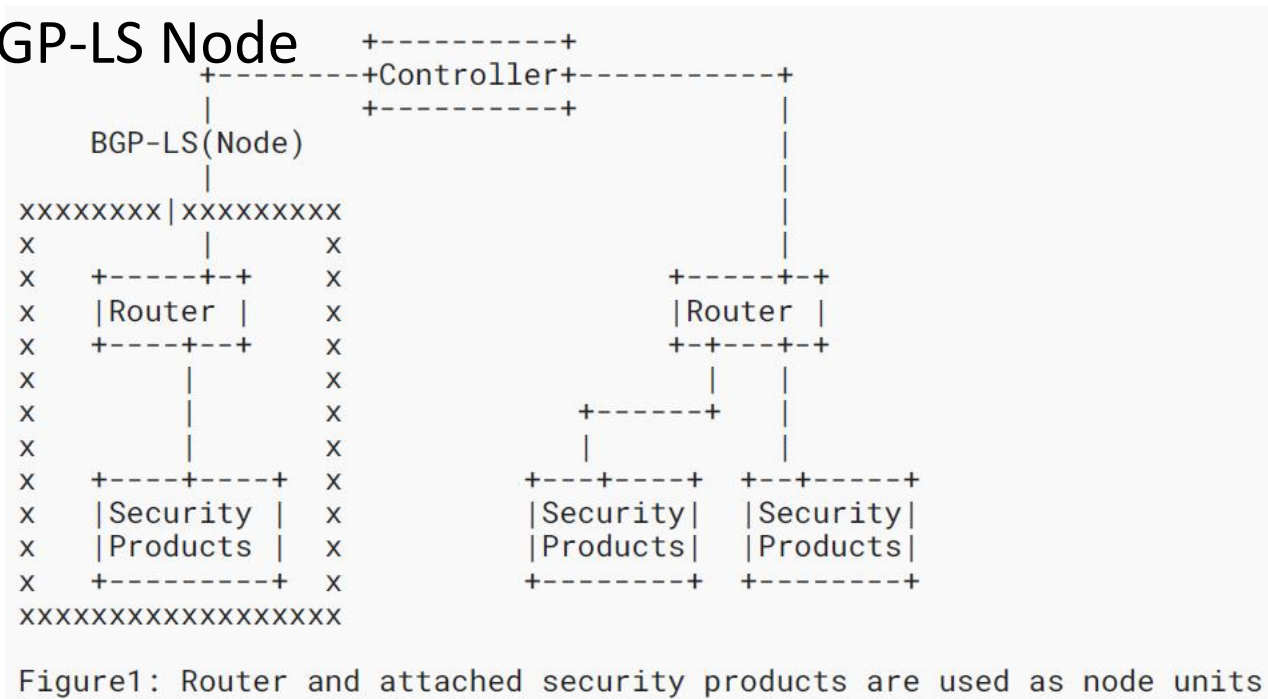
- Get the node's security capability
- Form routing path according to user security requirements
- Issue the routing path, which is implemented through routing programming



# 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





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

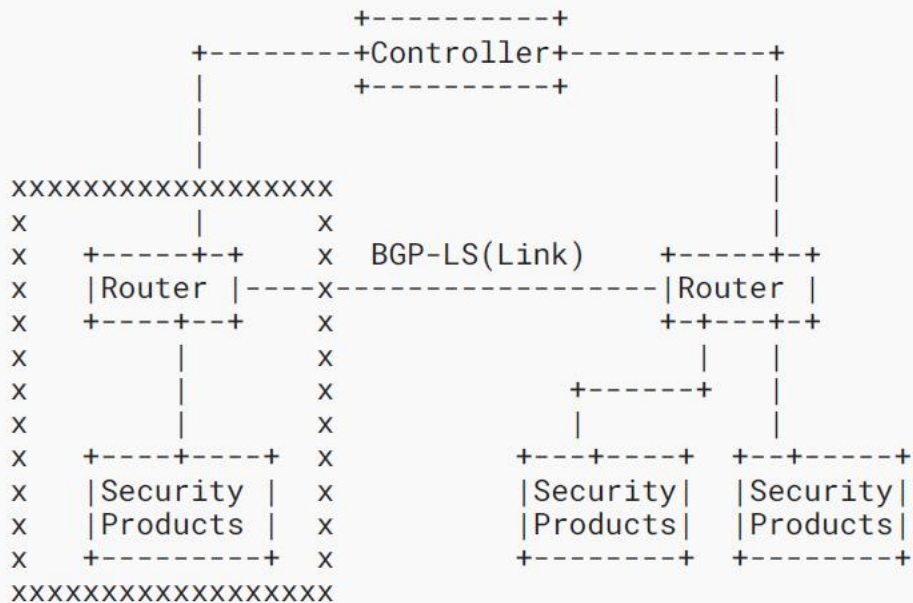
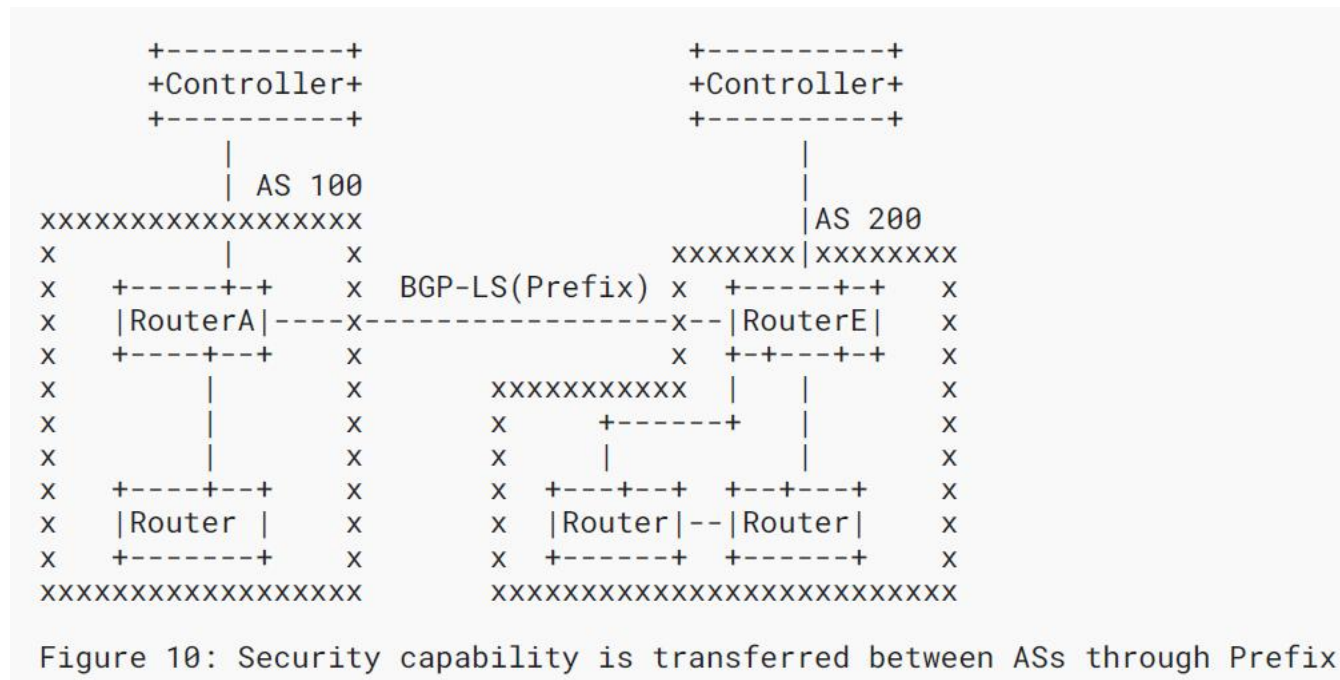


Figure 5: The peer node transmits the security capability through the link

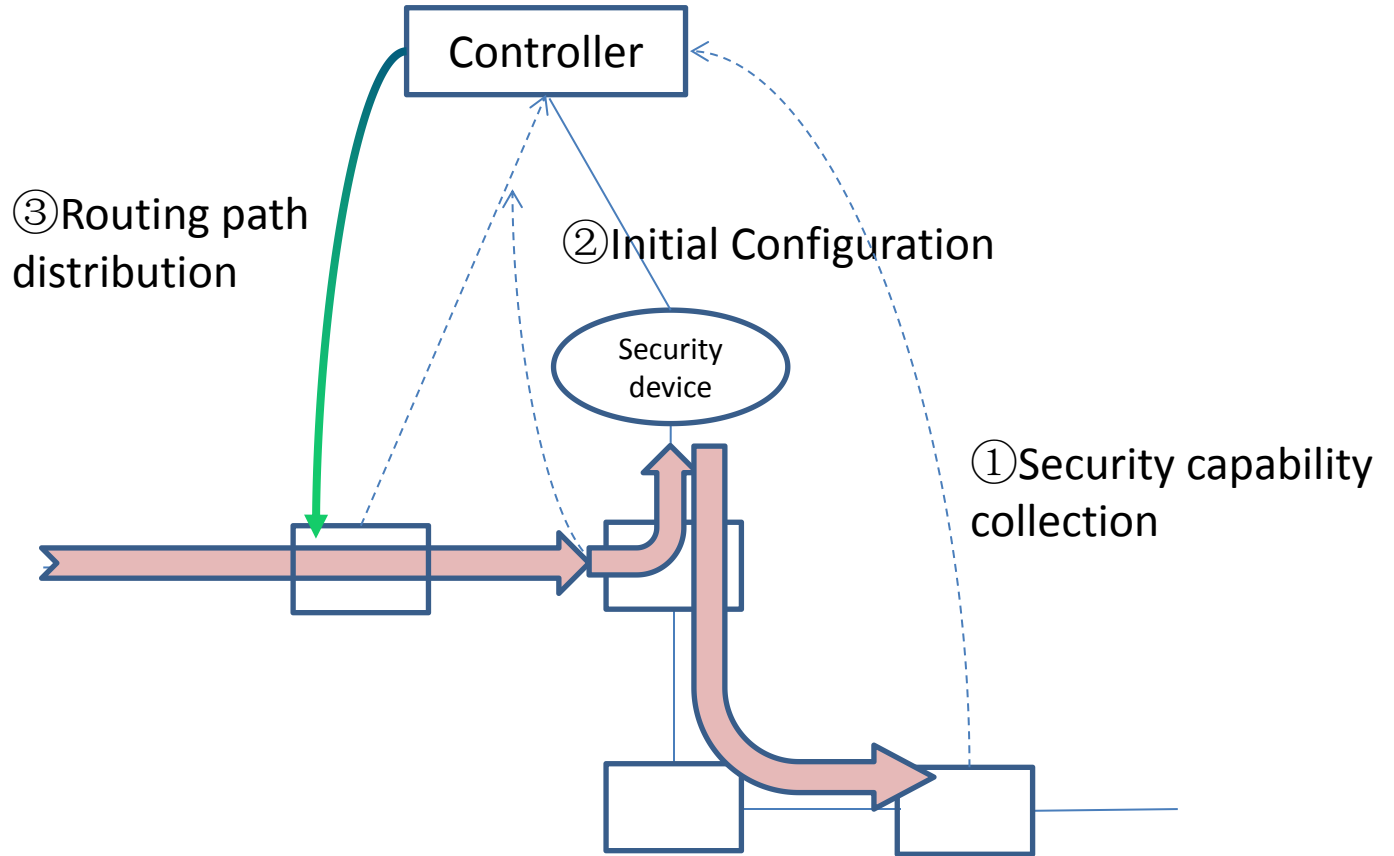
### 3. Carrying the security capability of the AS through the BGP-LS Prefix



draft-chen-bgp-ls-security-capability-00

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

# Interfaces



----->  
Security capability  
collection interface

→  
Traffic flow

# Next To Do

- This topic needs more discussion,
- No suitable WG in the Security Area?
- Apply for a special email list to discuss? Such as how to use these security capabilities except form secure routing path?
- How to timely and efficient schedule the use of security functions?