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

Meiling Chen
China Mobile
7/24/2023

Existed Problems for security services

- China mobile has many regions (in hundreds), each regions is responsible for purchasing and deploying the security equipment independently.
  - lack the visibility across multiple regions.
  - Difficult to coordinate globally.
- To satisfiy security requirement for end-to-end services, it is necessary to know the capabilities of all security devices in all the regions.
  - Offline coodination is difficult as each region deployment status is dynamic.
- It is important to have interoperatble solution because:
  - we purchase equipment from many vendors.
  - with standard, we can easily enforce vendors to provide the exposure function during our evaluation process.

Security functions capabilities exposure

- **Combination of security and network:**
  - From the perspective of Carriers/ISPs, to integrate security service into the network service provided to the users.
  - From the perspective of users, the security service may include security functions like firewalls, IPS, anti-ddos, etc.

- To implement security functions capabilities exposure at the protocol level, some extensions of the existing protocols are needed, including:
  - Collect security information from nodes;
  - Distribute security policy via protocols, such as SRv6.

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, add a new Node Attribute.

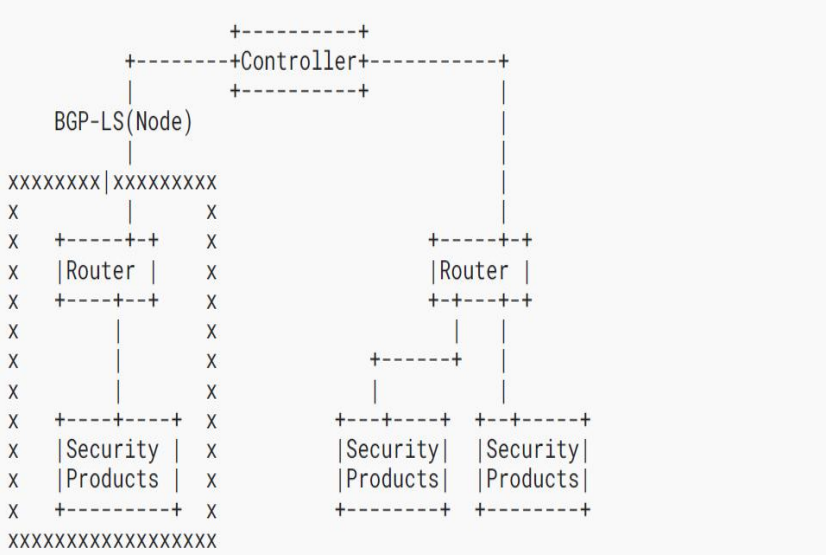


Figure1: Router and attached security products are used as node units

TLV Code Point	Description	Length
1030	Node Security Capability	variable

Table 4: New Node Attribute TLV

2. Carrying the security capability of the remote node through the BGP-LS Link, add a new Link Attribute.

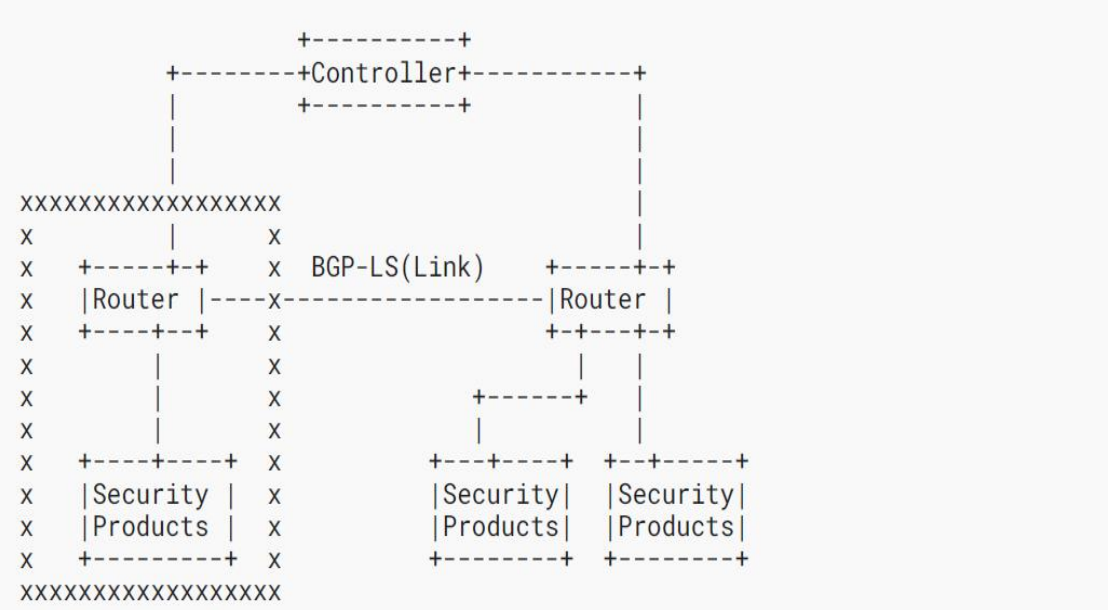


Figure 5: The peer node transmits the security capability through the link

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

Table 8: New Link Attribute TLVs

3. Carrying the security capability of the AS through the BGP-LS Prefix, add a New Prefix Attribute.

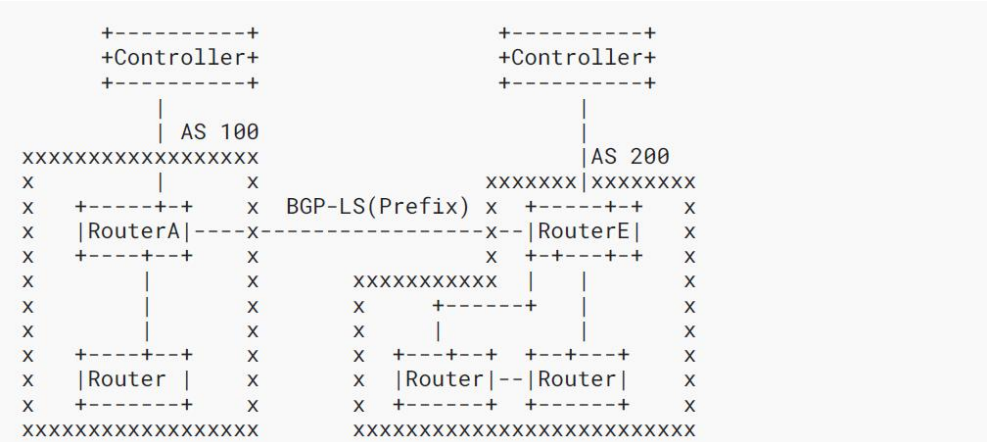


Figure 10: Security capability is transferred between ASs through Prefix

TLV Code Point	Description	Length
1158	AS security capabilities	variable

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

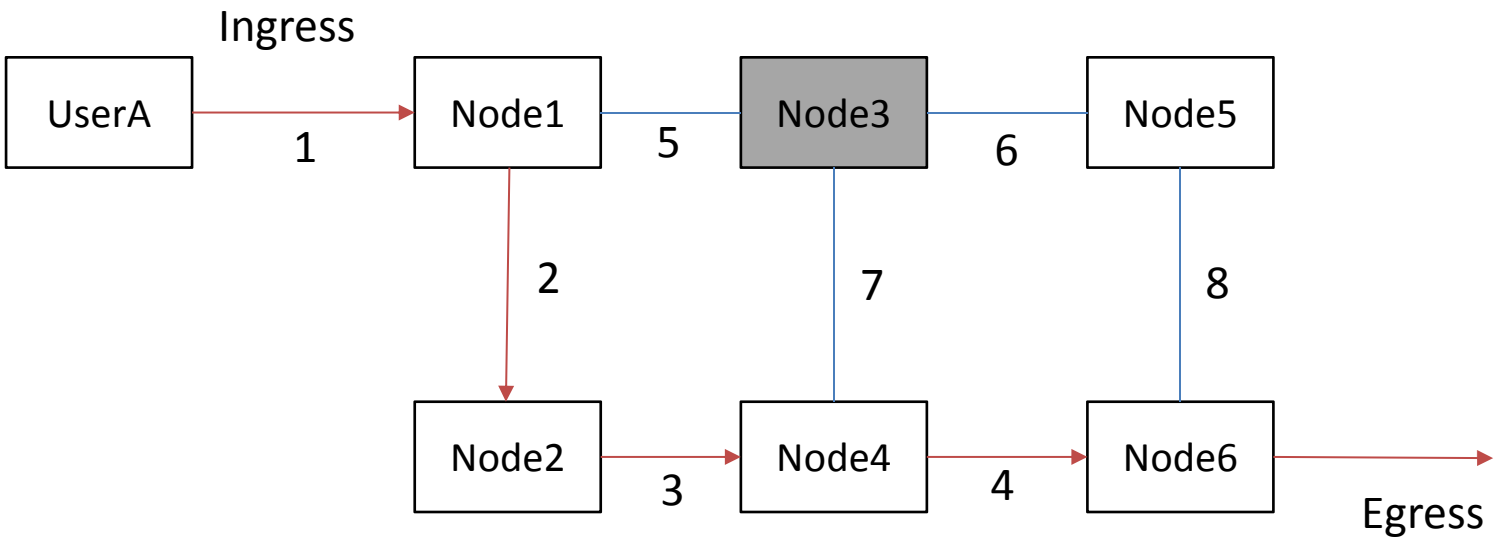
Next To Do

Comments, feedback, reviews, co-authors...

Appendix

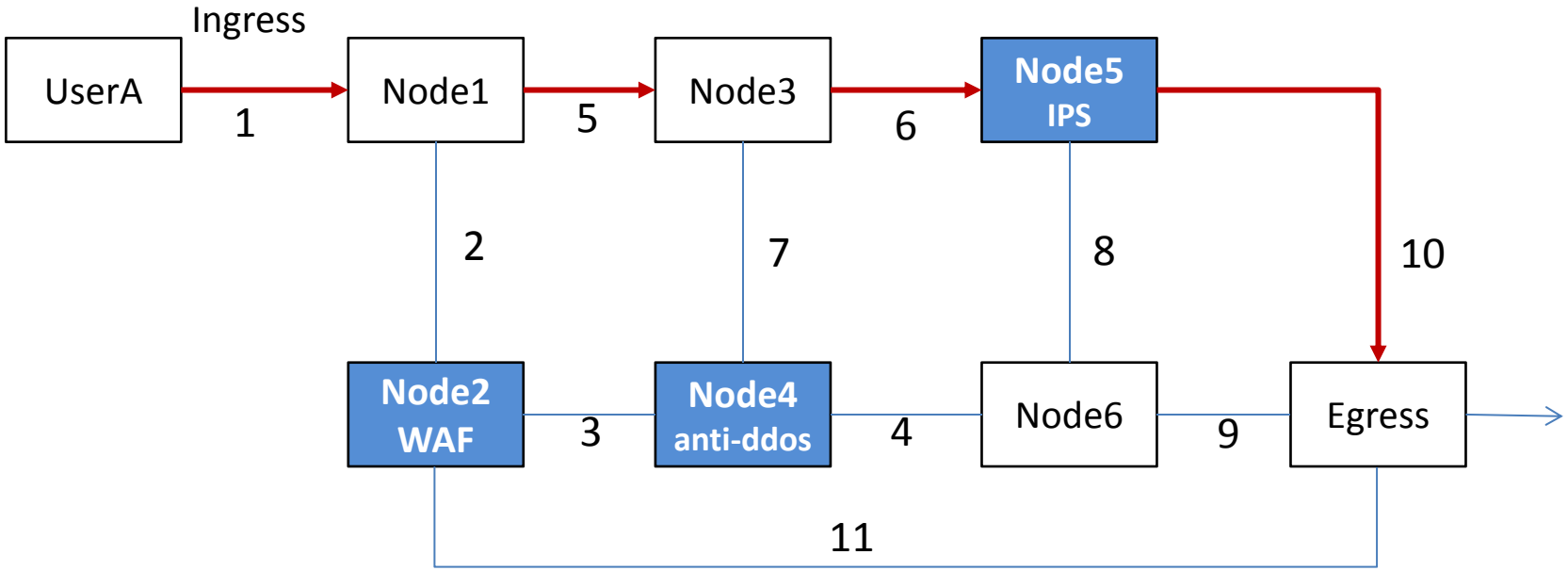
Use case1: path security (stage2)

- Based on the **security state of nodes and security functions supported by the nodes**, to form the routing path to meet the users' requirments for higher security.
  - If Node3 doesn't support specific security functions ,such as IPsec or physical isolation, or its security state isn't appraised OK, then it won't be included in the routing path for UserA.



Use case2: Customized security service(stage3)

- Based on **users' customized security requirements**, to form routing paths with corresponding various security services.
  - When userA needs IPS (Intrusion Prevention System) services, the path must pass through Node5 which provides IPS services.



functions required for implementation

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);