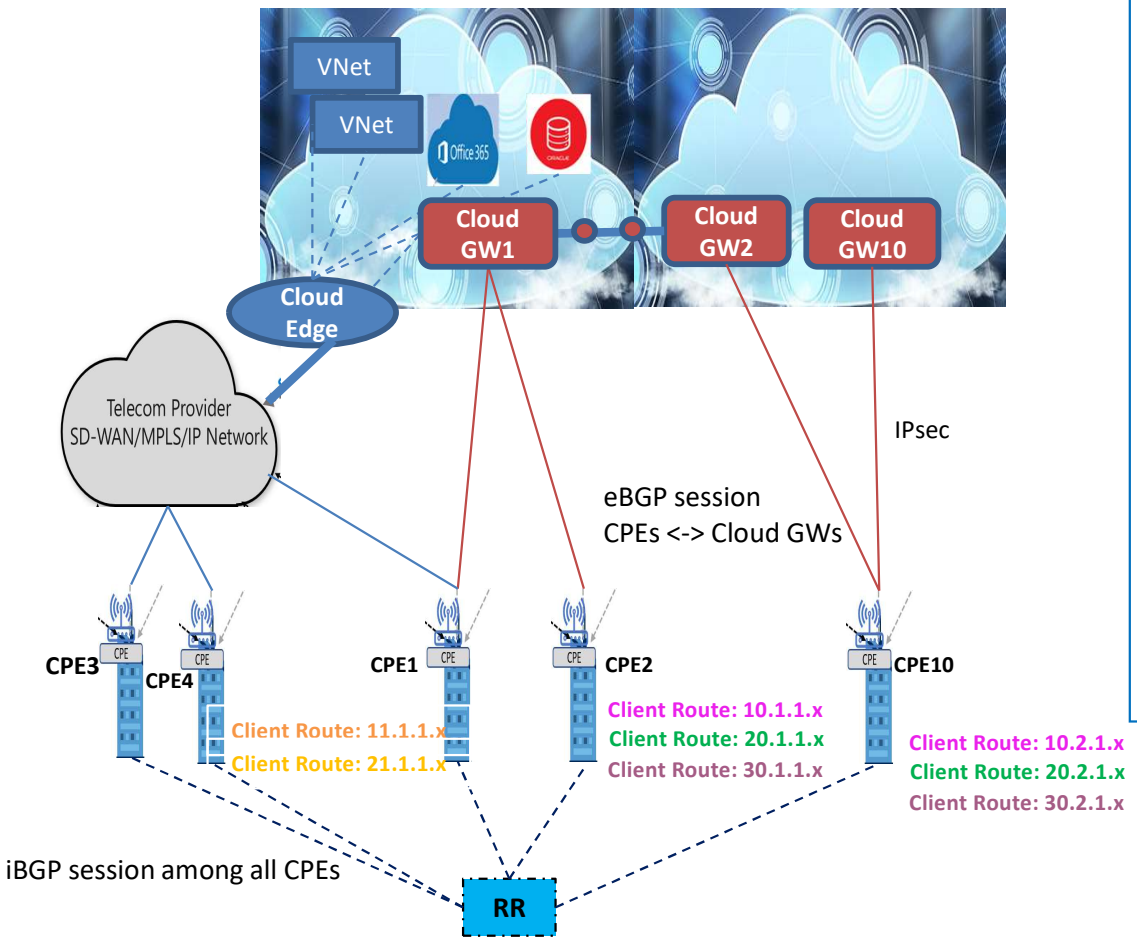
Multi-Segments SD-WAN via Cloud DCs

draft-ietf-rtgwg-multisegment-sdwan-02

Kausik Majumdar(kausik.majumdar@oracle.com)
Linda Dunbar (ldunbar@futurewei.com)
Venkit Kasiviswanathan (venkit@arista.com)
Ashok Ramchandra (aramchandra@microsoft.com)
Aseem Choudhary (achoudhary@aviatrix.com)

IETF 122 March, Bangkok

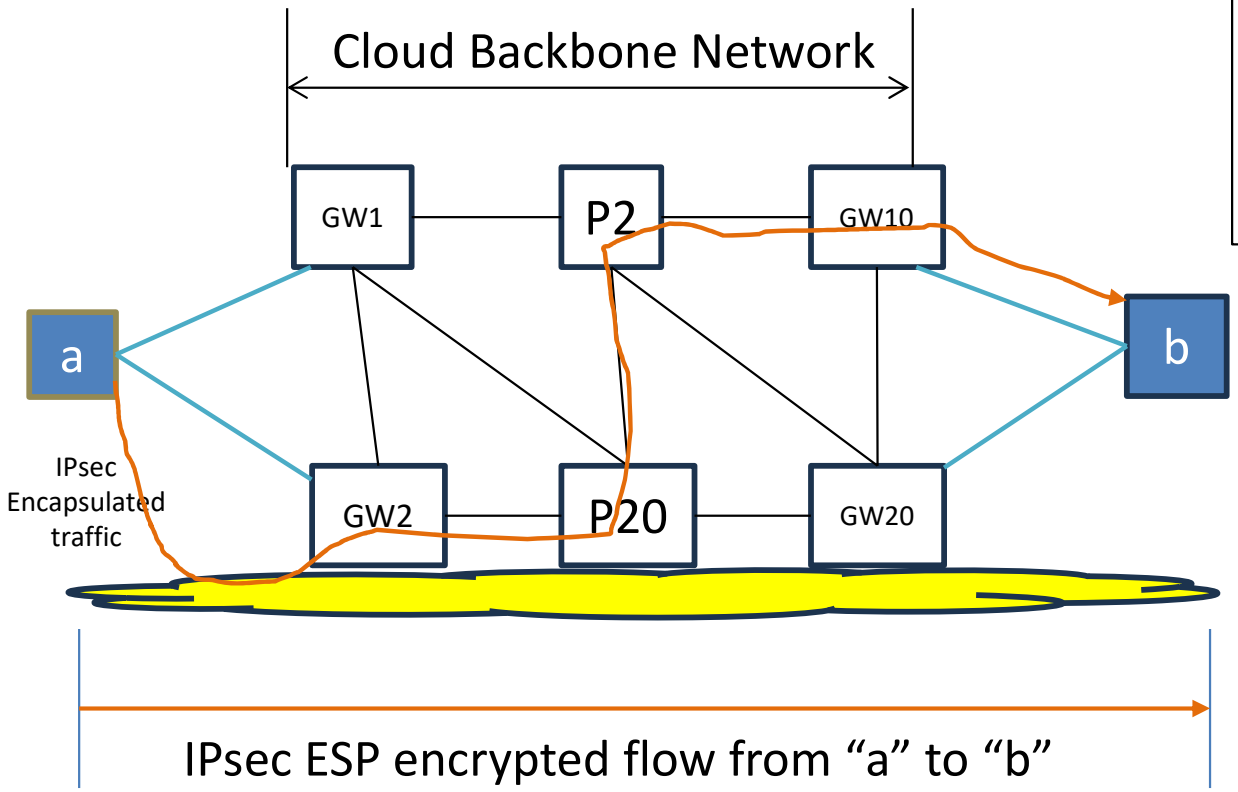
Geographic Faraway Branches Connected via Cloud Backbone



Why?

- **Reliable connectivity** – integrate geographically dispersed SD-WAN segments.
- **Integrated Security** – easier to utilize Cloud-based security services.
- **Advanced Threat Intelligence** – Cloud based SaaS analytics tools.

Traffic Steering Challenges in Multi-Segment SD-WAN



Goal:

- steer the IPsec encrypted flows from “a” to “b” through GW2-> P20-> GW10,

Challenges:

- lack of predictable routing for “a” → “b”.
- Difficult to enforce consistent policies

GENEVE Option Class for Multi-Seg SD-WAN

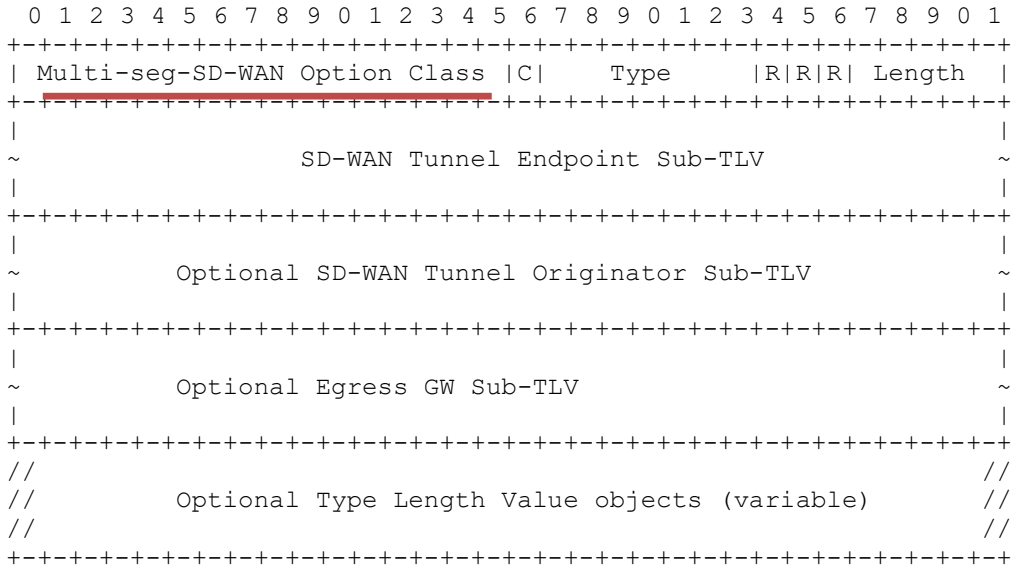
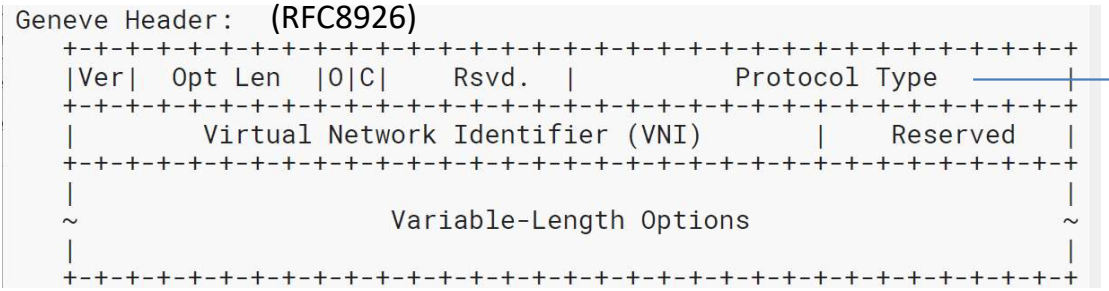


Figure 3 Multi Segment SD-WAN Option Class

- Multi-seg-SD-WAN Option Class = 0x0163, by IANA
- C-bit: drops the packet if not recognize the option per RFC8926
- Type: multi-segment SD-WAN forwarding model (Single Hop, Multi Hop, explicit egress,)
- the payload following the multi-seg-SD-WAN Option Class can be IPv4 or IPv6



carry an ESP packet → Use 0x32 (ESP)

Sub-TLVs within Multi-seg-SD-WAN Option Class

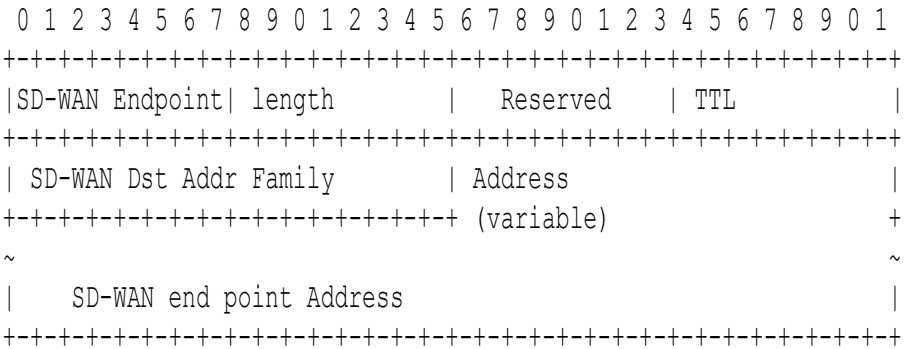


Figure 4 SD-WAN Endpoint Sub-TLV

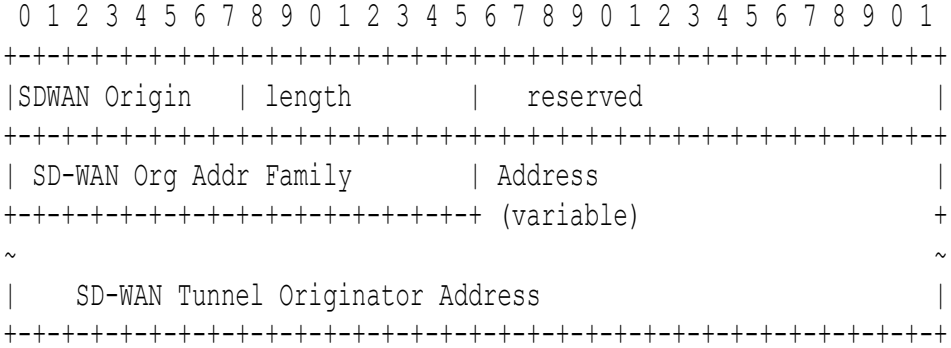


Figure 5 SD-WAN Tunnel Originator Sub-TLV

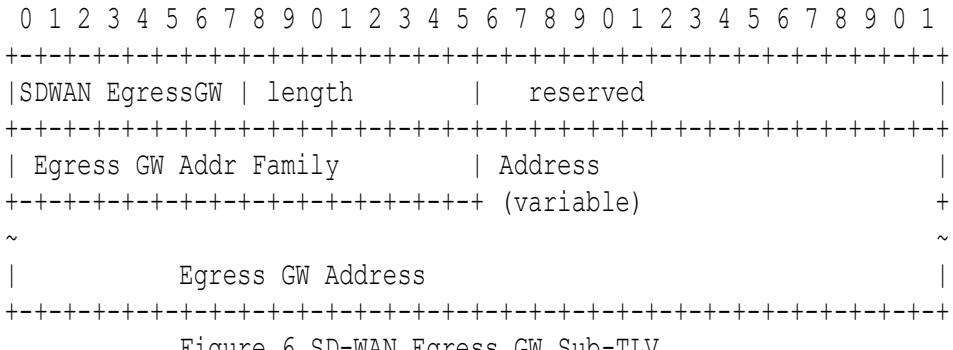


Figure 6 SD-WAN Egress GW Sub-TLV

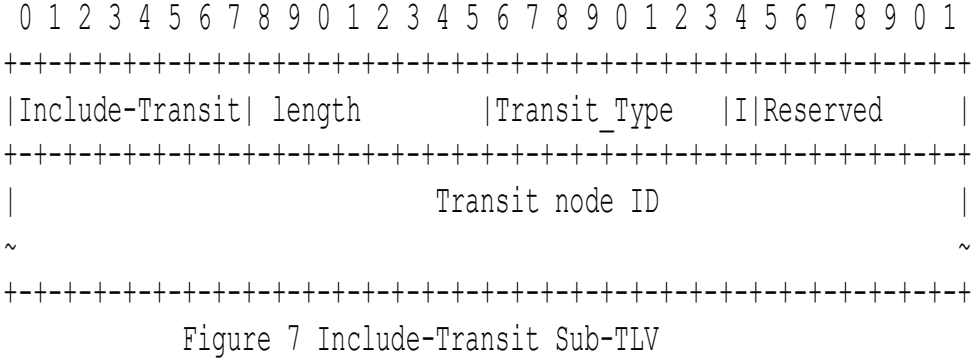
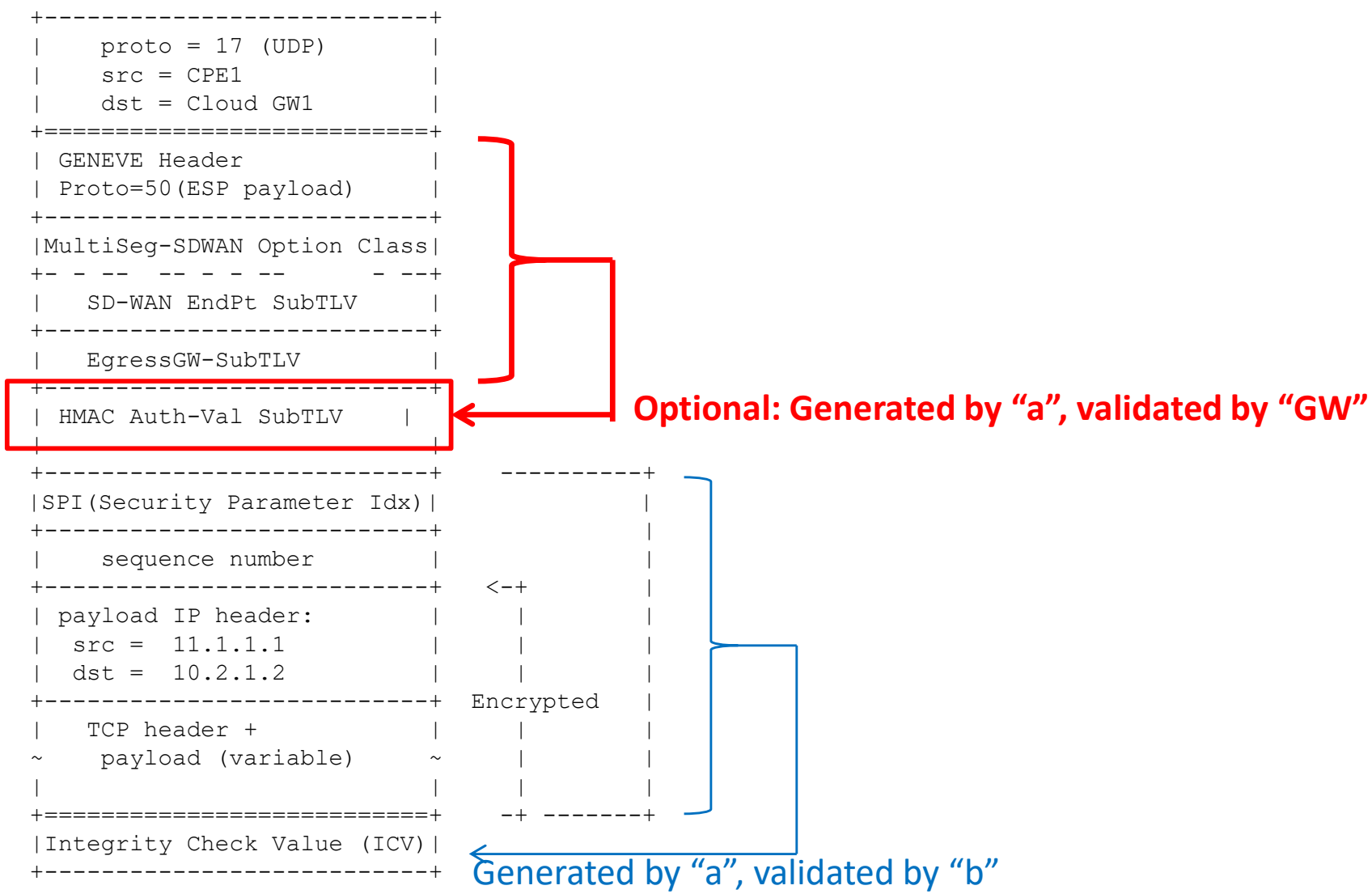


Figure 7 Include-Transit Sub-TLV


proto = 17 (UDP)
src = CPE1
dst = Cloud GW1
GENEVE Header
Proto=50(ESP payload)
MultiSeg-SDWAN Option Class
SD-WAN EndPt SubTLV
EgressGW-SubTLV
HMAC Auth-Val SubTLV
SPI(Security Parameter Idx)
sequence number
payload IP header:
src = 11.1.1.1
dst = 10.2.1.2
TCP header +
payload (variable)
Integrity Check Value (ICV)
Encrypted
Optional: Generated by “a”, validated by “GW”
Generated by “a”, validated by “b”

Packet Header Processing at Ingress GW

- Authenticate the packet using a preconfigured authentication method.
  - drop packets containing unrecognized source addresses or invalid values in the GENEVE Sub-TLVs
- Check if the Egress GW Sub-TLV is present:
  - If the Egress GW Sub-TLV exists, the Cloud Backbone uses it to identify the egress Cloud GW.
  - If the Egress GW Sub-TLV is not present, the Cloud Backbone determines the optimal egress Cloud GW based on the destination CPE address.
- Change the destination address in the outer IP header of the GENEVE packet to the address of the identified egress Cloud GW (either extracted from the GENEVE header or determined by the Cloud Backbone).

Packet Header Processing at Egress GW

- Decapsulate the GENEVE header to extract the IPsec-encrypted payload.
- Perform additional security checks:
- Validate that the SD-WAN Tunnel Endpoint Sub-TLV corresponds to a registered destination CPE.
  - Drop any packet that lacks a valid destination CPE or originates from an untrusted source.
- Ensure the source Cloud GW is an authorized forwarding node to prevent unauthorized traffic injection.
- Forward the IPsec-encrypted payload to the destination CPE, preserving the end-to-end encryption.

Control Plane Consideration

- Control Plane for CPEs/vCPEs:
  - iBGP among CPEs/vCPEs
  - SD-WAN-Edge-Discovery via iBGP for additional properties
- Control Plane between CPEs and Cloud GWs:
  - eBGP between CPEs and Cloud GWs
  - IKEv2 key exchange to establish the IPsec SA

Next Step:

- Ready for WGLC