draft-lrss-bess-evpn-group-policy-04.txt

W. Lin (Juniper), D. Rao (Cisco), A. Sajassi (Cisco), L. Kreeger (Arrcus), Jorge Rabadan (Nokia)

IETF 127, November 2026

San Francisco

Change-1: Added a New Section on Use Cases

4.1. Enterprise DC and Campus Environments

Group Policy allows administrators to classify endpoints into isolated security groups and define scalable Group Based policies to govern communication.

- East-West (E-W) within a domain:
  - Application Tier Isolation: Granular control between tiers (e.g.,Web, App, DB) in a DC to prevent lateral threat movement.
  - Tenant Isolation: Enforcing selective, bidirectional communication between tenant systems. Campus Users & IoT: Providing granular filtering for diverse endpoints within the campus.
- North-South (N-S) across multiple domains:
  - Campus to DC: Securing traffic flows from campus users to data center workloads.

Cisco Confidential

Change-1: Added a New Section on Use Cases – Cont.

4.2. AI Data Center (AI DC) Environments

In multi-tenant AI GPU-as-a-Service deployments, shared resource pools are used to maximize expensive GPU utilization. The use of Group Policy enables secure, isolated environments for multiple tenants sharing GPU resources.

AI Job-Aware Segmentation groups endpoints in the same AI job and ensures traffic isolation between different AI jobs in the same tenant.

Cisco Confidential

Change-2: Added Flag bits in GPI EC

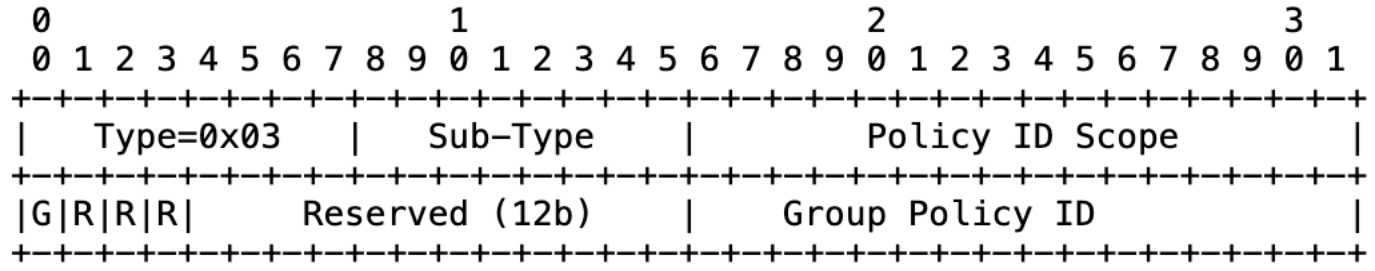


Figure 1: Group Policy ID Extended Community

Policy ID Scope: The Policy ID Scope field is 16-bit long, and is an optional field.

Group Policy ID (GPI): The GPI field is 16-bit long and it encodes the value of a Group Policy ID.

Flags: 4-bit field.

G-bit: Set to 1 to indicate intent to use Group Policy Extension in the data plane.

Cisco Confidential

Change-3: Added a new section on Explicit Signaling of Group Policy Header Extension

- To ensure deterministic behavior in a network comprising of devices with different local behavior, it is useful to explicitly signal in BGP-EVPN advertisements that a device intends to send and process received Group Policy extension fields in the data plane encapsulation.
- An ingress NVE can use this explicit signaling received from an egress NVE to set the Group Policy fields in the VXLAN header when sending VXLAN encapsulated traffic to the egress NVE.
- Similarly, an egress NVE can use this explicit signaling from an ingress NVE as a condition to process the Group Policy fields in the received VXLAN header.

Cisco Confidential

Next Step

- 7438bis which this draft depends on, is now in RFC editor queue
- Are we good for WG Call?

Cisco Confidential