Virtual Multi instance

draft-hegde-rtgwg-virtual-multi-instance-00

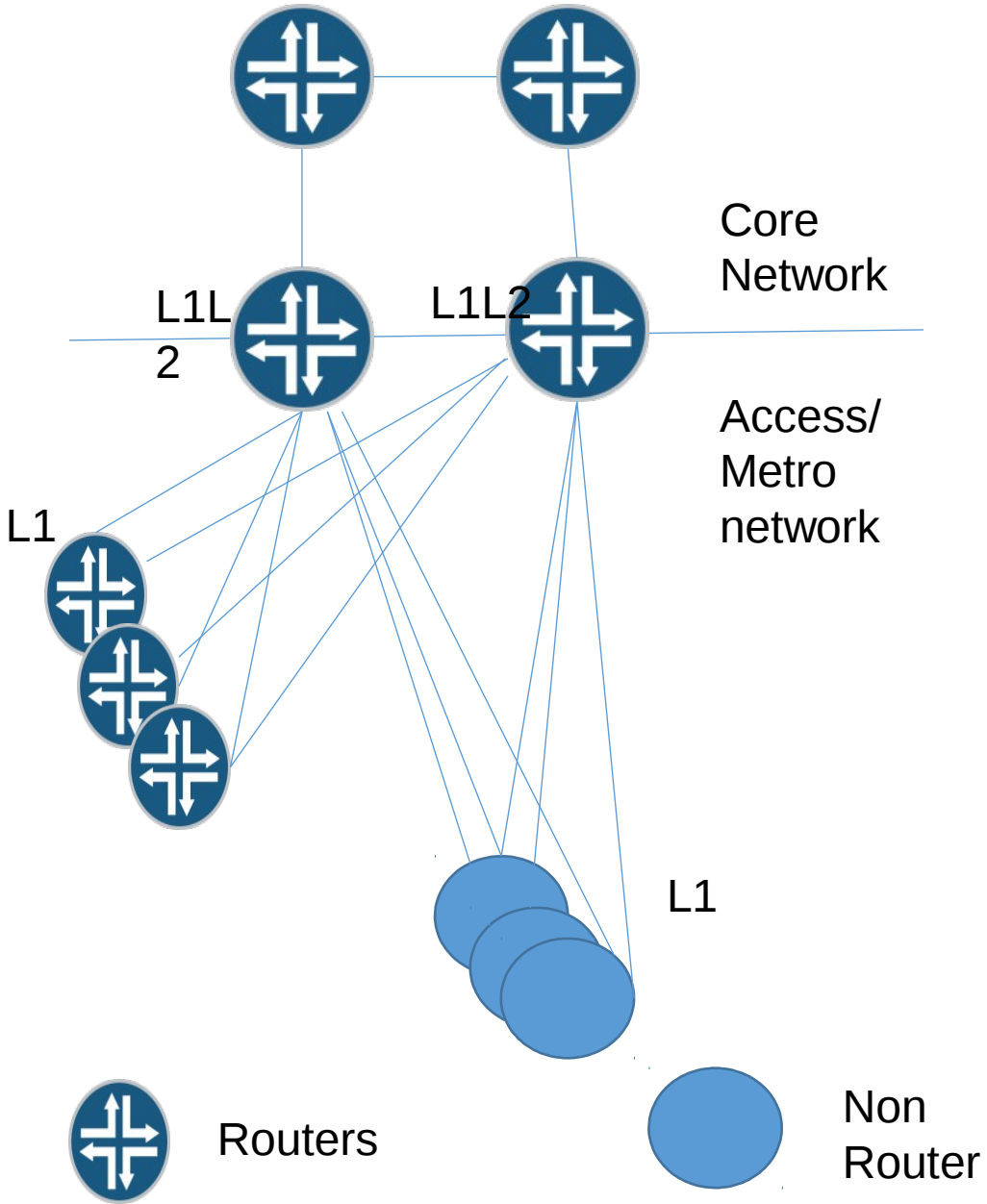
IETF-93

Shraddha Hegde
Salih K A
Mannan Venkatesan
Ross Callon
Alia atlas

Agenda

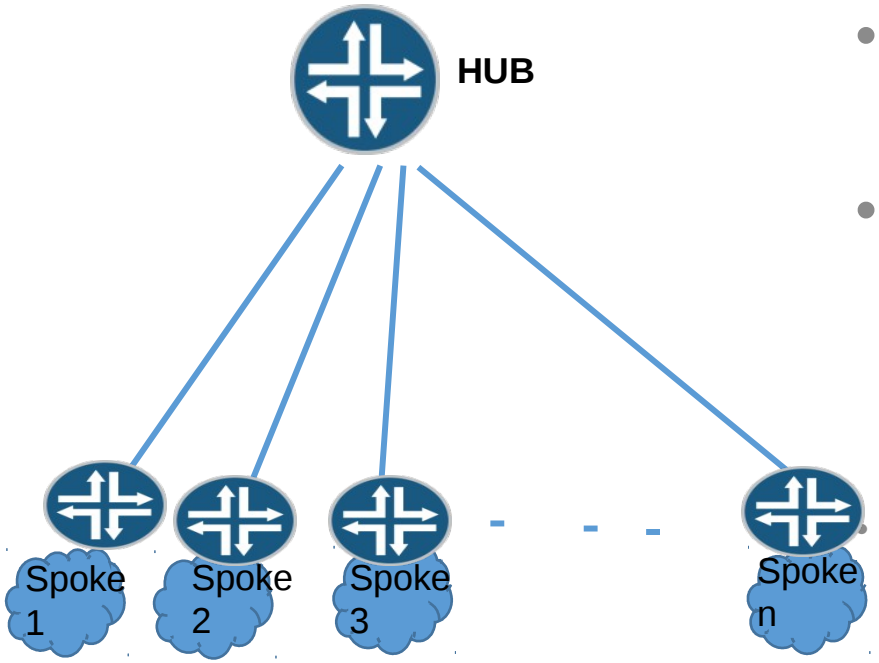
- Problem
- Motivation
- Solution
- Hub and Spoke topologies
- Ring topologies
- Protocol procedures
- Advantages

Problem



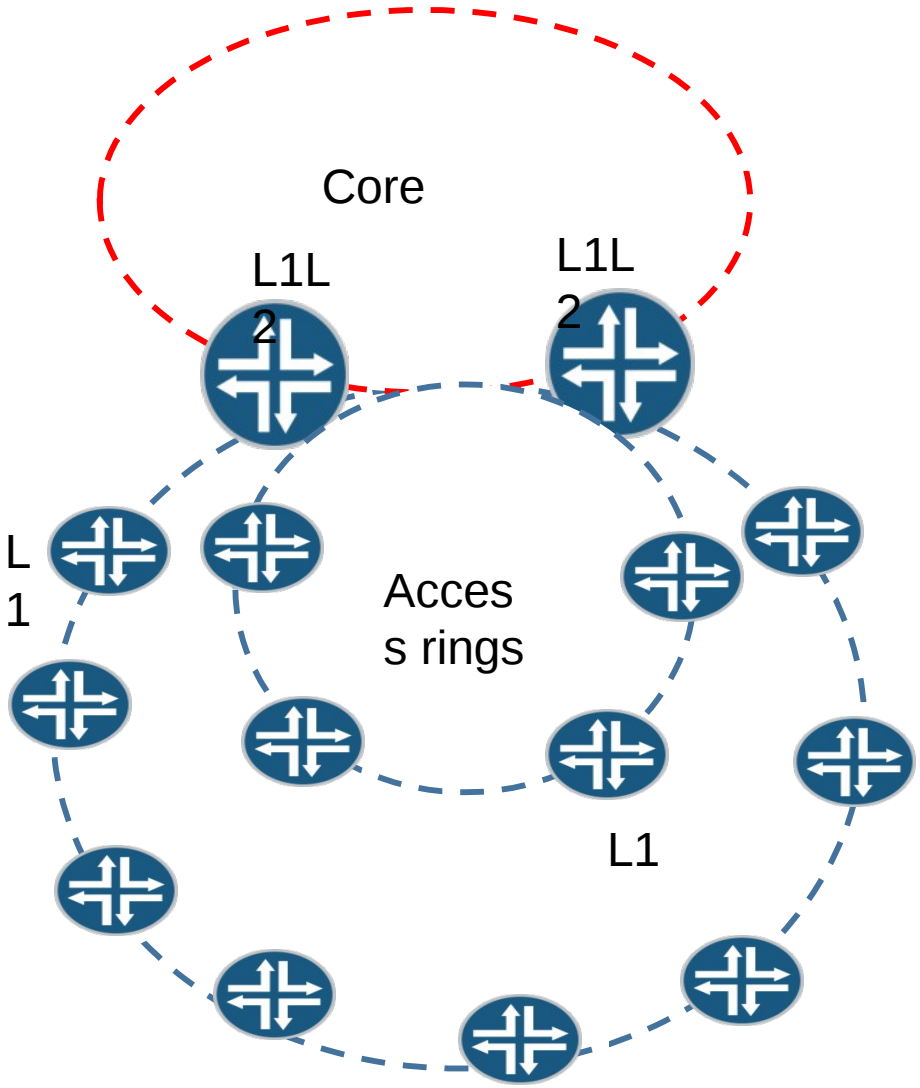
- All edge devices in single area.
- Customer premise events (power cycle, device failures) cause flooding/SPF process across all devices in the area.
- Non router devices like CMTS have limited ISIS capabilities
- Deploying separate L1L2 routers for each type of device

Problem: Hub and spoke topologies



- Huge number of spokes
- Spokes need only default route to HUB
- Link state protocols not well suited
  - Large LSDB size at spokes
  - Unnecessary flooding
- Multi-area design not suitable
  - Config overheads
  - IP address restrictions

Problem: Ring topologies



- Multiple rings connect to

A pair of L1L2 routers

- Event in one ring causes

flooding across all the rings

- Large LSDB size at ring nodes
- Unnecessary flooding

- Flooding scope needs to be implemented by ring nodes

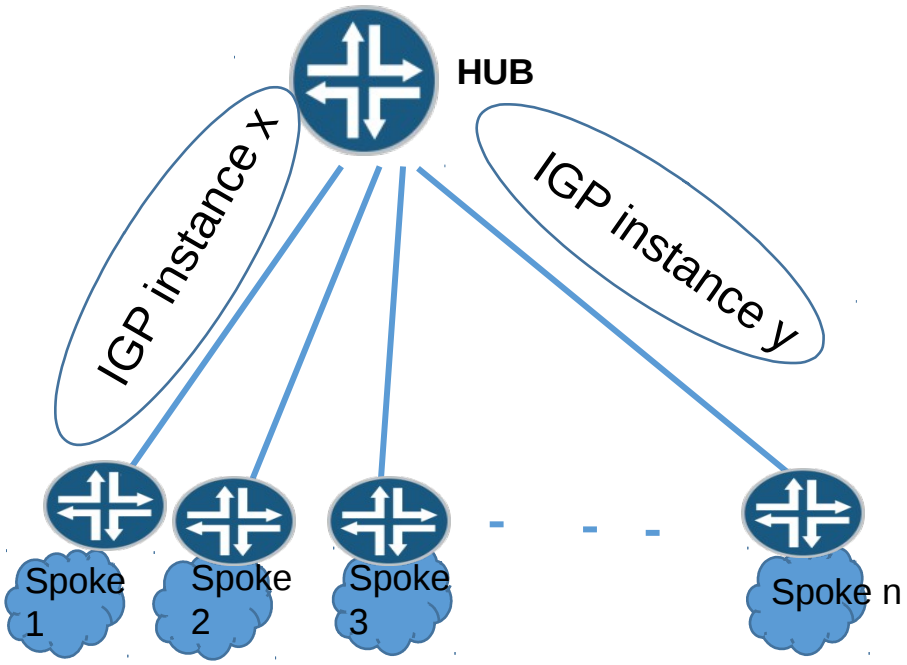
Motivation

- Ease of configuration
- Partial deployment
- Support Common topologies

Solution

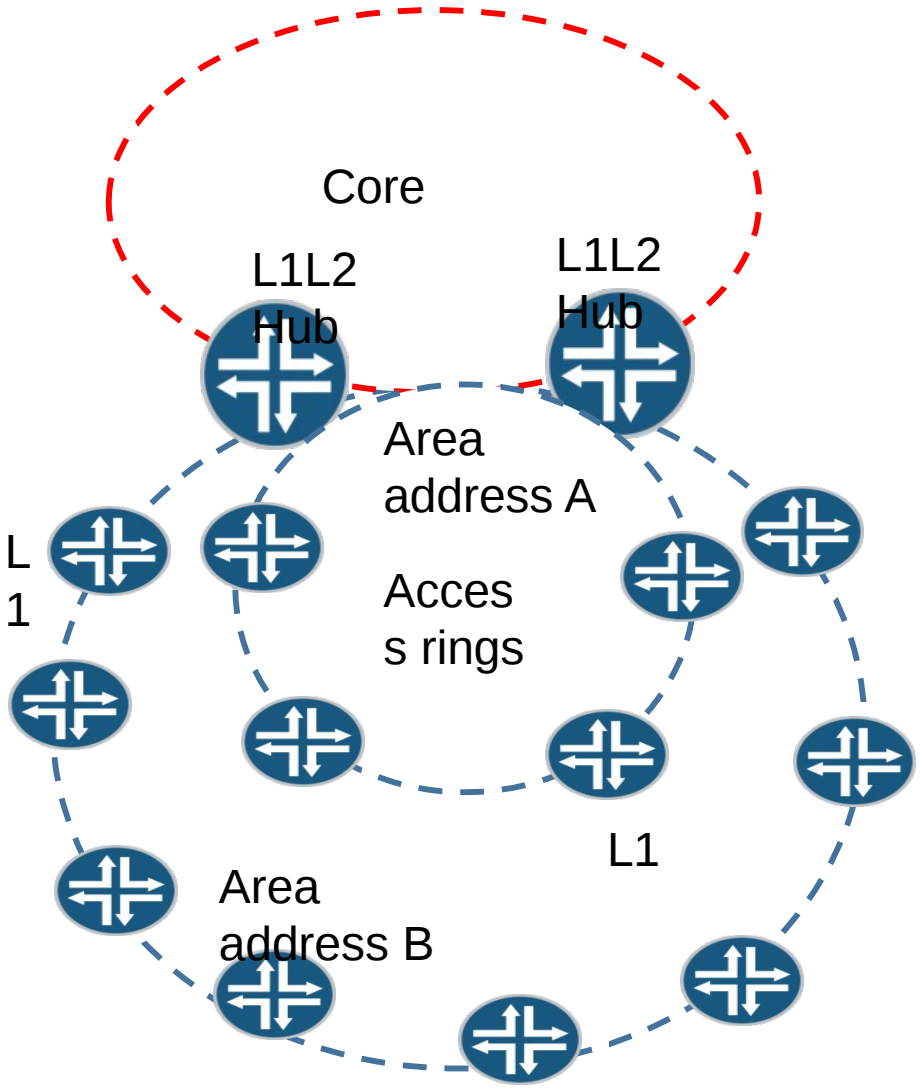
- Separate each spoke or Ring into a separate virtual instance/area dynamically
- Use source /destination router-id / system id pair to segregate messages into respective instances
- Configuration needed only on the interface to identify the kind of topology
- Remote ends may run standard software.

Solution: Hub & spoke topology



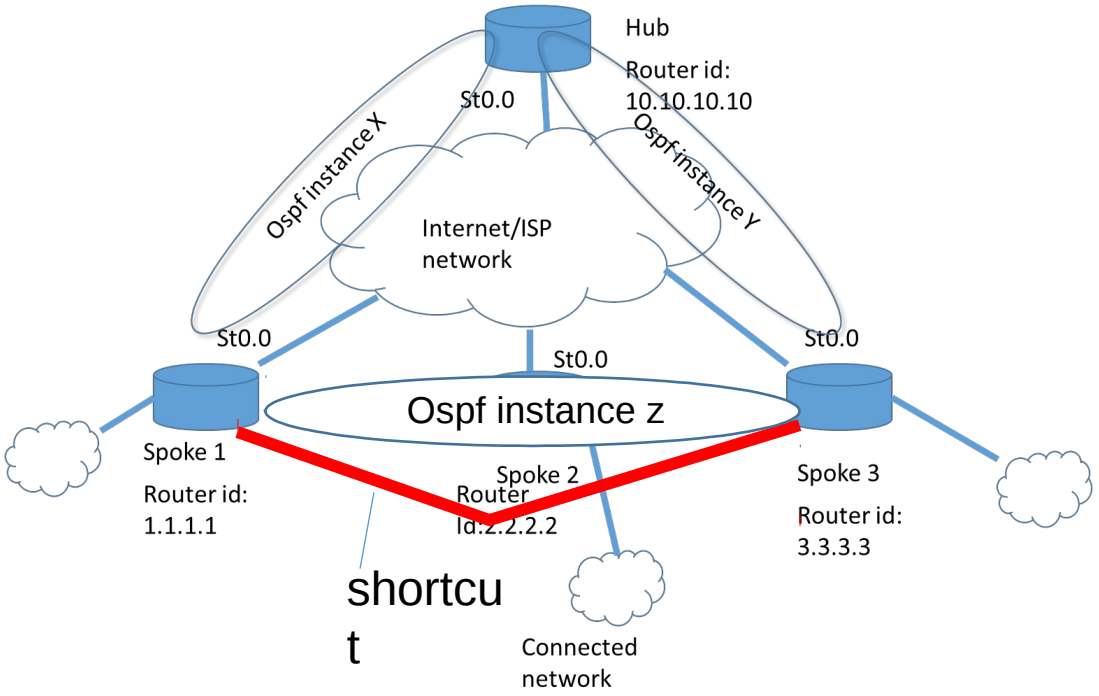
- Every spoke is modeled as a separate instance
- Source router id/system id , destination router-id/system id carried in OSPF/ISIS messages is the key
- Spoke may connect to multiple Hubs
- Flooding only within the virtual instance
- Separate Router LSA/LSP for each virtual instance
- Separate SPF for each virtual instance
- Redistribution and preference rules for the virtual instance to avoid spokes being used as transit

Solution: Ring Topologies



- Each ring node is configured with same area address
- L1L2 router segregates the rings into virtual instances based on area address received in ISIS messages
- The link between L1L2 Hubs is in default instance
- Each virtual instance performs separate standard SPF
- The link between the hubs is leaked into the virtual instances to facilitate Remote-LFA backup procedure

Solution: Dynamic Tunnels



- Optimisations in IPSEC domain
- Shortcuts between spokes to prevent large traffic going via Hub
- Dynamic tunnel bring-up/down based on traffic
- Virtual multi-instance on spokes helps reduce flooding
- Spoke1 has single interface and two virtual instances
- Redistribution rules for dynamic tunnels topology

Protocol procedures

- Identification of virtual instance/area
  - Based on topology
- SPF procedure
  - Separate SPF for each instance
- Route redistribution
  - Default route into virtual instance
  - Leaking of routes
  - Summarization
- Leaking of Links

Advantages

- Provides excellent scaling properties for IGPs in regular topologies
- Minimum configuration overhead
- Backward compatible; spoke router/Ring nodes not require software upgrade

Q &A

Thanks