Routing Mechanism in Dragonfly Networks Gap Analysis, Problem Statement, and Requirements

slides-wang-draft-dragonfly-problem-statement-00

Ruixue Wang(China Mobile)

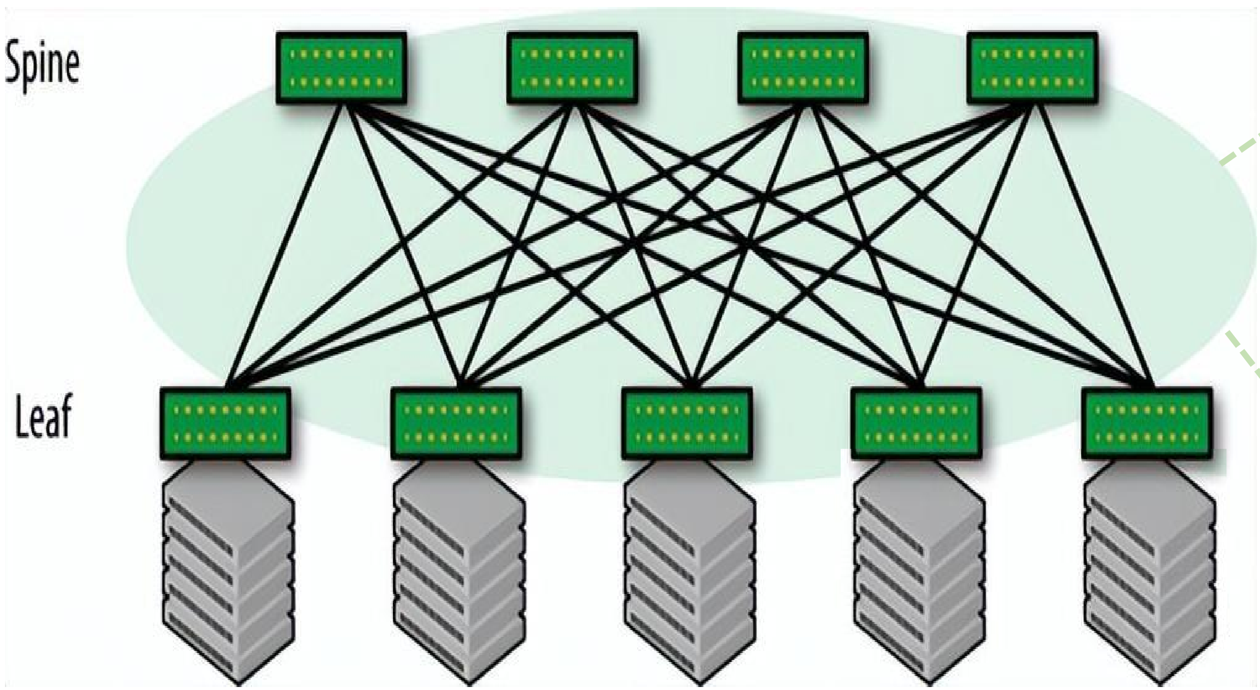
Changwang Lin(New H3C Technologies)

Wenxuan Wang(China Mobile) (Presenter)

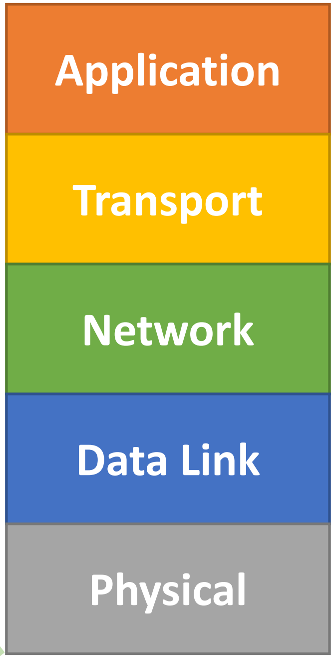
Weiqiang Cheng(China Mobile)

Possible solutions for AI data center networks

Topology Changes



Stack Changes



...

Better RDMA

Simplified Protocols

Efficient Load balance

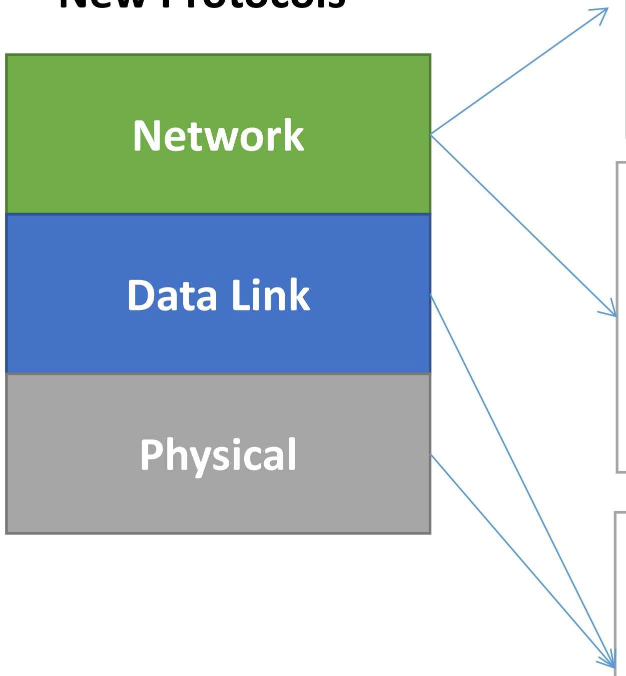
Lower Latency

Overview of some attempts in Networks

New Topology

New Topology: Dragonfly, Dragonfly+ ...
https://datatracker.ietf.org/doc/draft-wang-rtgwg-dragonfly-routing-problem/
https://datatracker.ietf.org/doc/draft-agt-rtgwg-dragonfly-routing/

New Protocols



SRv6 for DCN: source-driven path programming multicast rather than hop by hop establishing multicast tree.
https://www.ietf.org/archive/id/draft-cheng-rift-srv6-extensions-01.txt
https://datatracker.ietf.org/doc/draft-ietf-spring-srv6-srh-compression/

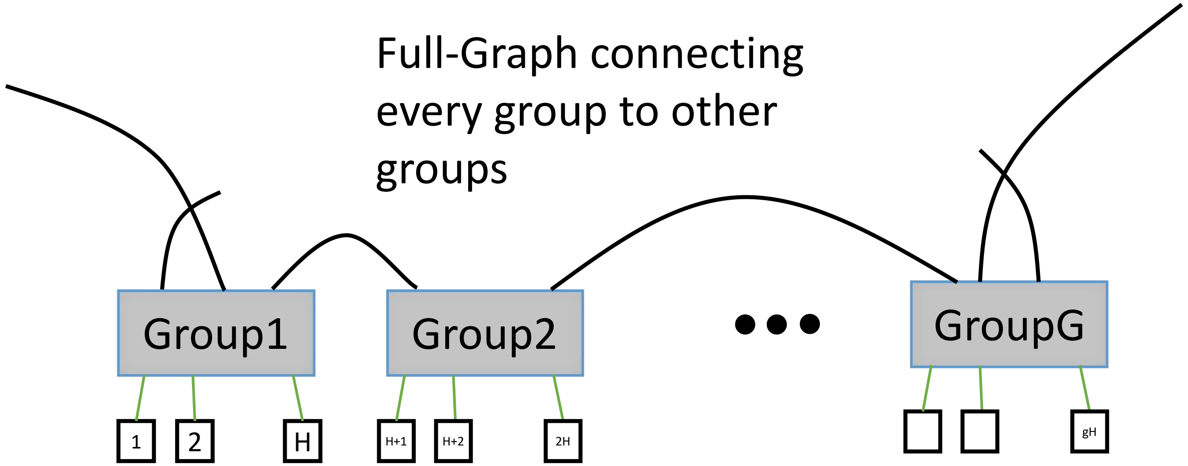
MSR6 for AI Multicast offloading: source-driven path programming multicast rather than hop by hop establishing multicast tree.
https://datatracker.ietf.org/meeting/116/materials/slides-116-bier-07-bier-multicast-use-case-in-dc-00.pdf
https://www.ietf.org/archive/id/draft-liu-multicast-for-computing-storage-00.txt

Globle Scheduling Ethernet(GSE) : Packet Spraying based on packet container and Lower Latency FEC in Ethernet layer are described in GSE white paper post by CMCC. You can scan the QR to download the white paper.

What's Dragonfly Topology?

Dragonfly is a hierarchical topology with the following properties:

- Several "**groups**", connected together using **all to all links**
- The topology inside each group can be any topology, such as Fat Tree,etc
- Focus on reducing the number of long links and network diameter to reduce total cost of network
- Requires Adaptive Routing to enable efficient operation

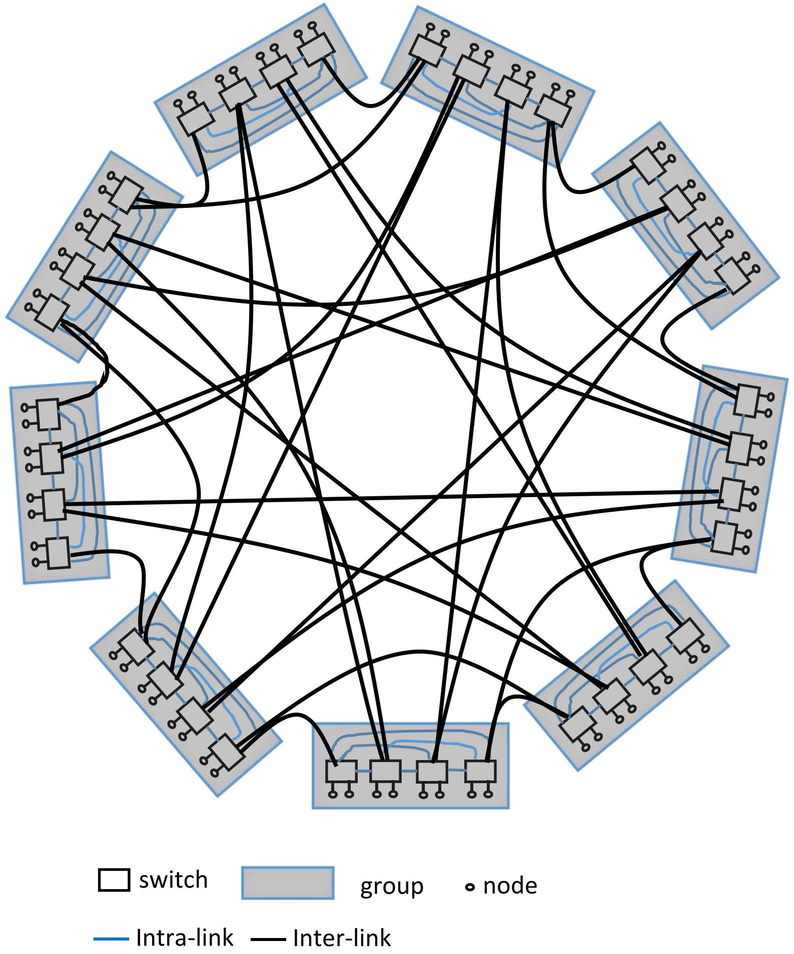


Dragonfly Topology

The Dragonfly topology is divided into three layers:

- Switch layer: The switch layer include one switch, p ports connecting to compute nodes, and h ports connecting to other groups
- Group layer: The group layer includes m switches, and the m switches in the switch layer are fully connected.
- System layer: The system layer includes g group layers, which are fully connected

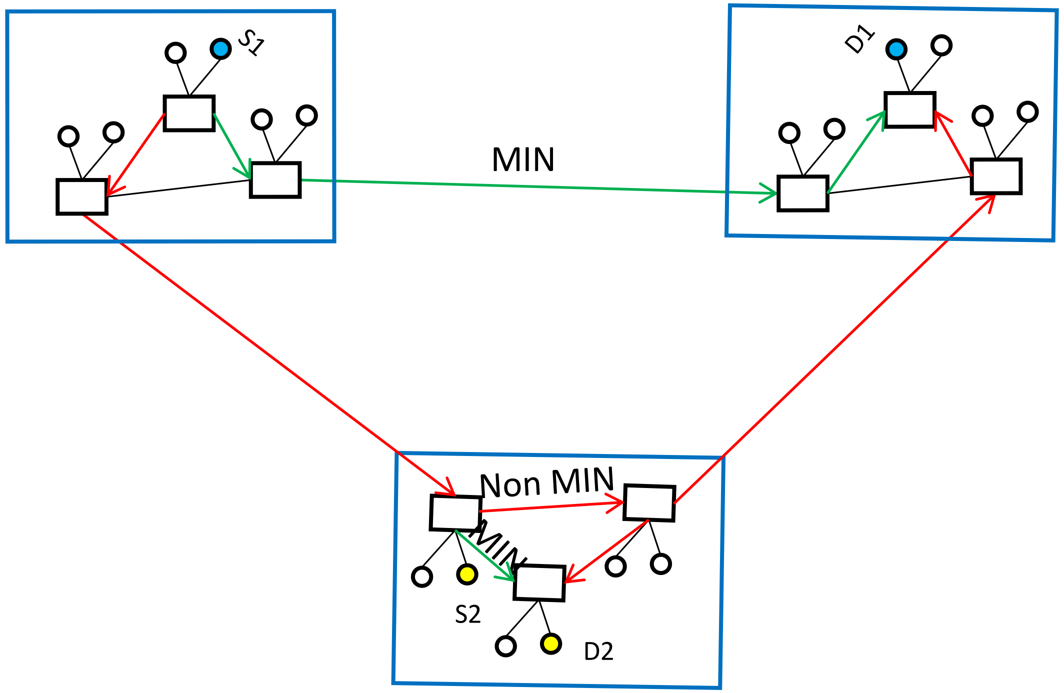
The routing between any two nodes in the topology is at most 3 hops, including one hop of the s-group intra-link, one hop of the inter-group link, and one hop of the d-group intra-link.



Existing Routing Mechanisms #1

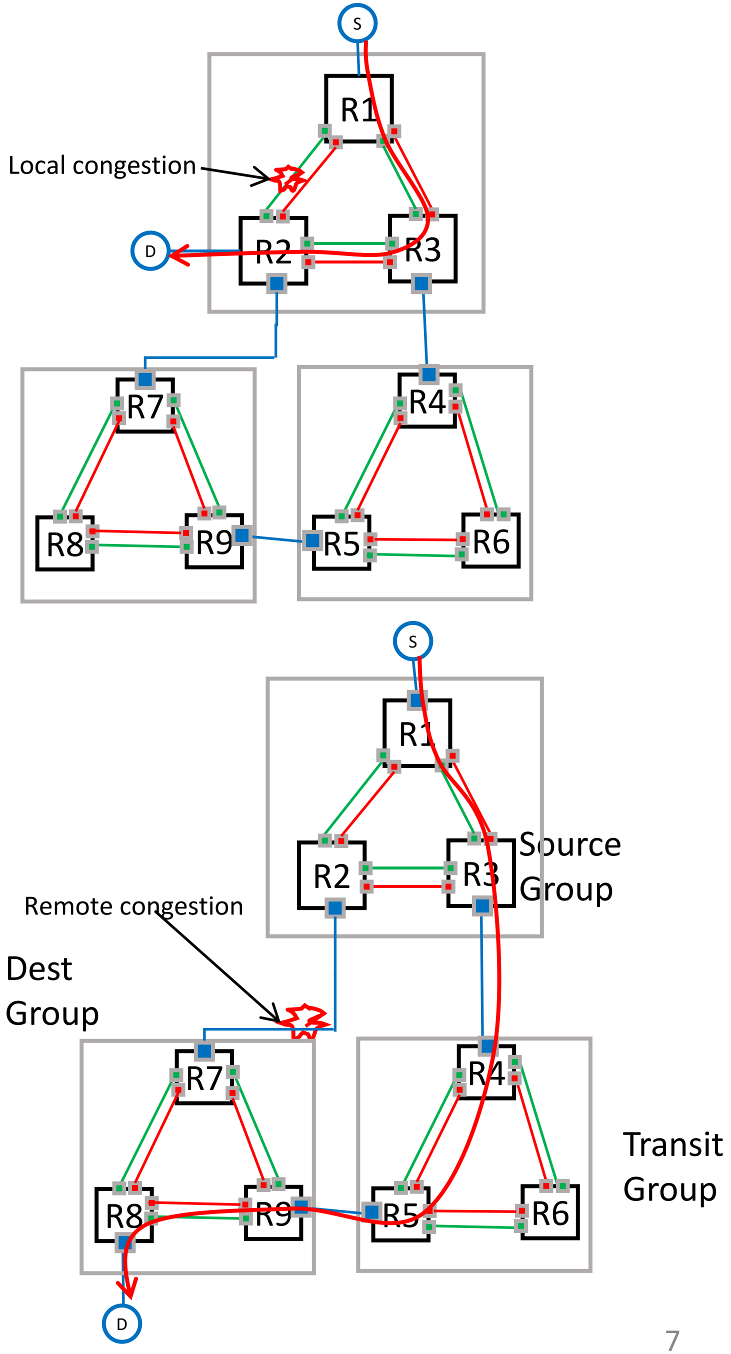
- Minimal Routing is the simplest and most commonly used routing mechanism in Dragonfly networks. It uses the path with the least number of channels to quickly deliver data to the destination node.
- Current routing protocols are based on the MIN routing mechanism, which cannot fully utilize all available bandwidth resources.

- Non-Minimal Routing is a routing mechanism that avoids load imbalance by choosing a path other than the one with the least number of channels.
- There is currently no mature routing protocol that utilizes Non-MIN Routing for forwarding, and how to avoid traffic loops is a challenge for Non-MIN Routing.



Existing Routing Mechanisms #2

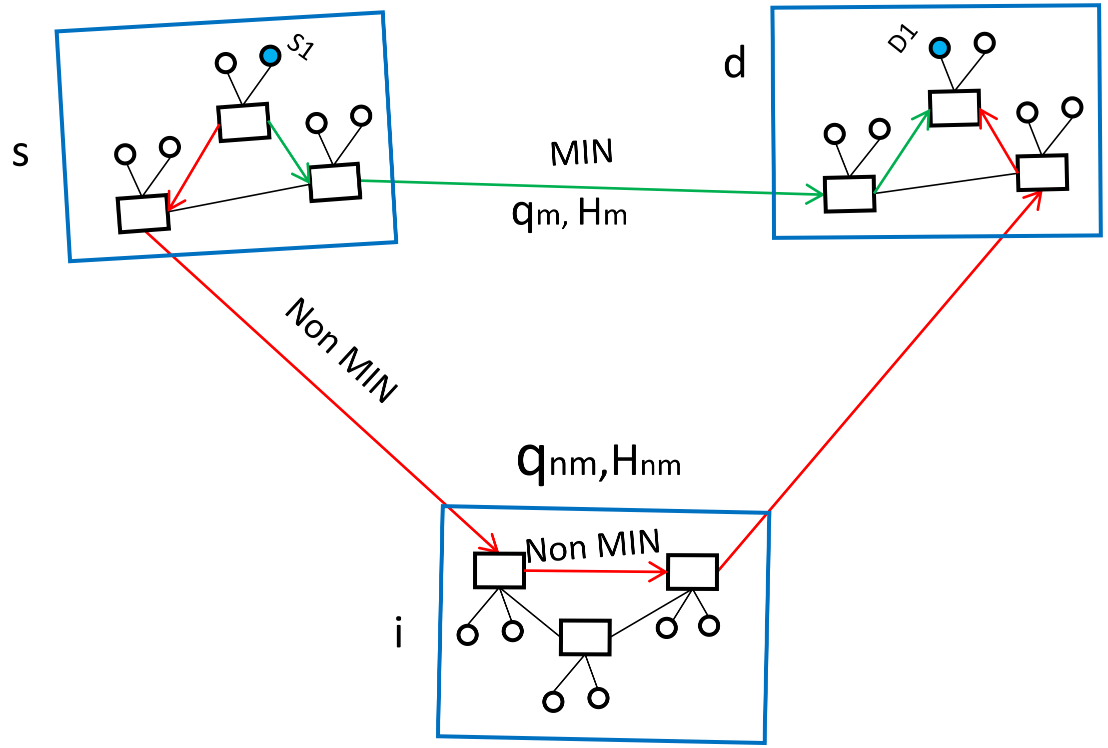
- Adaptive Routing is a mechanism that can dynamically adjust the routing path by intelligently judging the network congestion status. AR's strengths lie in its adaptability, which can control traffic in high-load situations and prevent congestion.
- To avoid loopback, isolation is achieved through VPN. The MIN link is assigned to the Public-VPN(Green), the Non-MIN link is assigned to the Private-VPN(Red), and the access link is assigned to the Mix-VPN(Blue). Each Intra-link is connected to two ports, with one serving as a MIN link and the other as a Non-MIN link.
- Local congestion: Switch to Non-MIN link due to local perception of link congestion.
- Remote congestion:Switch to Non-MIN link via an intermediate transmission group due to remote link congestion notified by a remote router.



Existing Routing Mechanisms #3

- Valiant Load-Balanced Routing uses the classic Valiant algorithm to select paths between global routing networks and then uses load-balancing routing algorithms between each group.

1. Hm= shortest path (SP) length
2. qm= congestion of the outgoing channel for SP
3. Pick i, a random intermediate node
4. Hnm= non-min path (s->i->d) length
5. qnm= congestion of the outgoing channel for (s->i->d)
6. Choose SP if Hmqm≤ Hnmqnm; else route via i, minimally in each phase



Gap Analysis #1 non-minimum-routing

Non-minimum routing refers to the routing strategy that does not prioritize the shortest or most direct path between endpoints.

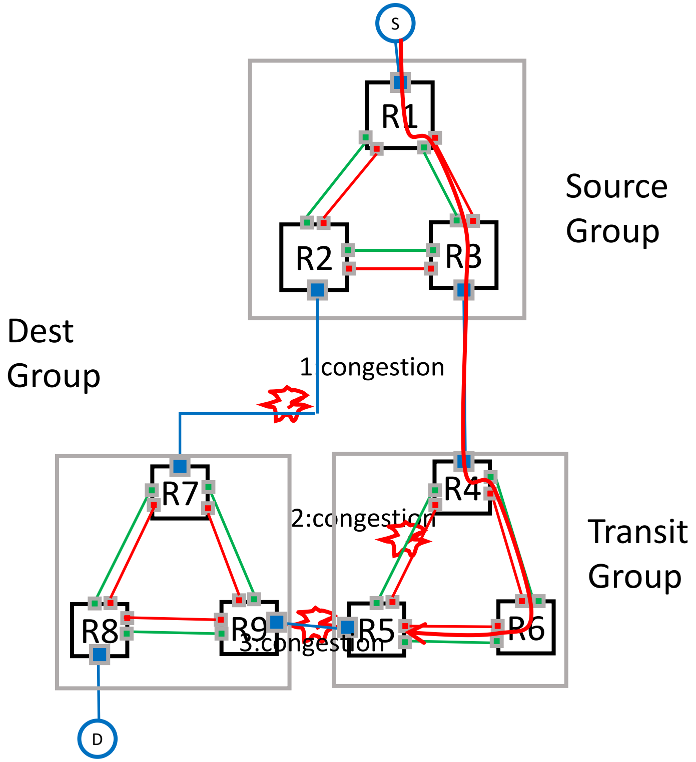
- **Implementation**
  - Using weights or path costs in IGP: Adjust the weights or path costs of routers in the Interior Gateway Protocol (IGP) to influence route selection.
  - Non-minimum routing with BGP refers to the practice of using policies and attributes to influence BGP's path selection algorithm.
- **Disadvantage**
  - Additional management and configuration: Using non-minimum path routing can increase network complexity, and special policies, marking, or attributes often require more complex configuration and management.
  - Longer latency: Additional latency generated from more complex path selection could impact application performance, especially for applications that require low latency.
  - Unnecessary overhead: In certain cases, using non-minimum path routing may lead to unnecessary network overhead, which could not only waste network resources but also negatively affect network performance.

Gap Analysis #2 Adaptive Routing

- Multiple VPNs are required to isolate the MIN link, Non-MIN link, and access link, occupying multiple ports and VPN resources.

- The MIN and Non-MIN links are both pre-planned through configuration, which are not flexible enough and make network expansion inconvenient.

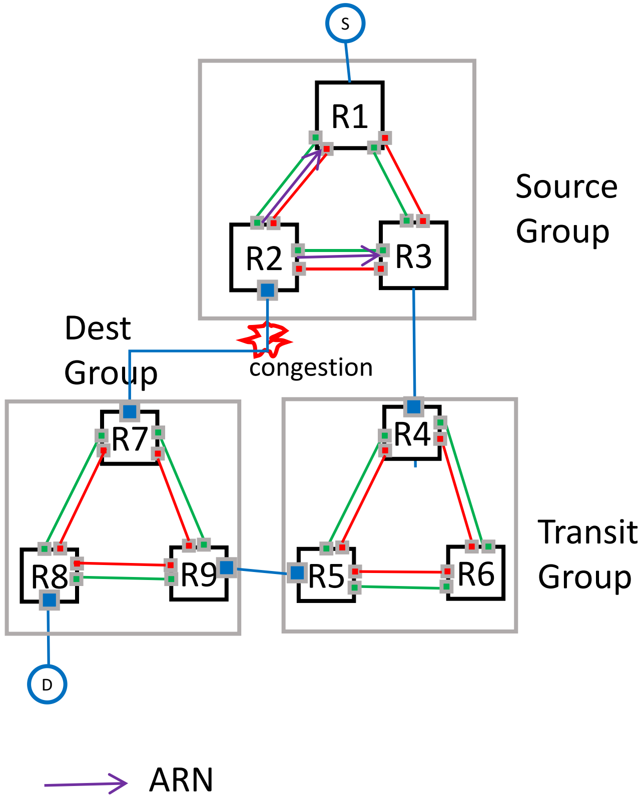
- It is difficult to handle situations where congestion occurs multiple times：
  - First, link congestion between the Source Group and Dest Group, router 1 selects the Non-MIN link between 1 and 4；
  - Then, link congestion between 5 and 7, router 5 selects the Non-MIN link between 5 and 6.
  - Finally, if a link congestion occurs again between the Transit Group and the Dest Group, no further adjustments can be made.



Gap Analysis #3 Adaptive Routing Notifications

Adaptive Routing Notifications for Remote Congestion (ARN)

- Local link congestion needs to be announced so that remote routers can promptly switch paths.Do not depend on existence of other messages for piggybacking,
  Sent towards the resolving routers only, does not waste bandwidth on other links.
- No independent protocol standard for Adaptive Routing Notifications (ARN), the method and approach to implementing ARN may vary. This may lead to compatibility and interoperability issues among different vendors.
- Latency and delay: ARN involves the exchange of notifications and updates between network devices to detect and react to congestion.
- Limited scalability: ARN may face scalability challenges when applied to large-scale networks with numerous interconnected devices.
- Security and privacy concerns: The exchange of congestion status and routing information in ARN can potentially introduce security vulnerabilities if not properly protected.



Problem Statement

- **Problem 1:**

  The existing routing protocols lack dynamic load balancing mechanisms.

- **Problem 2:**

  The existing network architecture lacks standard definitions of network congestion and a notification mechanism for remote congestion, which makes it difficult to timely exchange congestion information.

Requirements for Dragonfly Topology

- **Low latency:** The routing protocol must be fast and efficient to ensure that packets are transmitted to the destination node promptly.
- **Load balancing:** The routing protocol needs to support multiple available paths for load balancing. It should dynamically select among multiple available paths to ensure fast packet transmission and distribute the load across network connections.
- **Scalability:** The Dragonfly architecture is typically deployed at large scale with a large number of nodes communicating with each other. Hence, the routing protocol needs to be scalable and capable of supporting route selection and packet transmission among a large number of nodes.
- **Adaptability:** The network topology in the Dragonfly architecture can change over time. The routing protocol needs to be adaptive and capable of re-computing optimal paths when the network topology changes, ensuring the selection of the best path for packet transmission.
- **Reliability:** The routing protocol in the Dragonfly architecture needs to ensure packet reliability. It should support link failure detection and recovery to ensure that packets can be correctly transmitted to the destination node in the event of link failures.

Next Step

- These requirements serve as practical guidelines that can be met, in part or in full, by proposing new techniques
- Any questions or comments are Welcomed

THANKS