TRILL for Data Center Networks
Agenda

1. TRILL Overview
2. Protocol Mechanism
3. Data Forwarding
4. Device Management and Fault Location
5. Use of TRILL
Data Center Development Trend

Traditional Data Center Structure

- In traditional data center networks, Layer 2 only extends to access or aggregation switches
- Virtual machines (VMs) can only be migrated within a Layer 2 domain
- To migrate VMs to another Layer 2 domain, IP addresses of the VMs must be changed
- If technologies such as load balancing are not used, services will be interrupted during VM migration

Next Generation Data Center Structure

- To better utilize existing data center resources, IDC carriers require VMs to be migrated within a data center
- Transparent Interconnection of Lots of Links (TRILL) is used to build a large Layer 2 network
- As huge east-west traffic exists in the data center, non-blocking forwarding of data frames is required to achieve full utilization of network link/bandwidth resources
TRILL Advantages

Loop Prevention
- Build loop free distribution tree and use TTL to avoid loops

Efficient Forwarding
- Forward data efficiently based on SPF and ECMP

Fast Convergence
- Listen to network topology changes and complete convergence within a few milliseconds

Easy Deployment
- Easy configuration
- Unified control protocol for Unicast and Multicast
Concepts

**TRILL**

- TRILL runs at Layer 2 and calculates routes based on the link state
- It is implemented based on the IS-IS protocol
- The device running the TRILL protocol is the route bridge (RB)
- The network where RBs run is the TRILL campus

**RB Connection Mode**

- RBs can be directly connected or connected by traditional Layer 2 network
TRILL Packet Format

**DA:** Outer destination MAC address. In Unicast forwarding, this is the MAC address of next-hop RB. In Multicast forwarding, this is reserved MAC address.

**SA:** Outer source MAC address. This is the local MAC address of each RB.

**VLAN:** Outer VLAN ID of TRILL data packets. This is the VLAN ID specified by the TRILL protocol.

**V:** TRILL version, which has a fixed value of 0 currently. If the version is not 0, the TRILL packet is discarded.

**R:** Reserved field.

**M:** Multicast flag. The value 0 indicates Unicast; the value 1 indicates Multicast.

**Op-Length:** Length of the TRILL header.

**Hop:** Number of hops.

**E-Rb-Nickname:** Nickname. In Unicast forwarding, it is the egress RB nickname. In Multicast, it is the root nickname.

**I-Rb-Nickname:** Ingress RB nickname.

**Original Frame:** Original Layer 2 packets sent by the server.
TRILL Data Encapsulation

- The original Layer 2 packets from the source end arrive at the destination through the TRILL network.
- The servers consider the TRILL network a bridge fabric.

- Nicknames are unchanged from end to end.
- Outer MAC is changed hop by hop.

Inner MAC
Nickname
Outer Mac
Nickname Concepts

**Nickname**

- Each RB on the TRILL network is identified by a nickname
- A nickname is a two digit number
- An RB can have multiple nicknames, which are generated automatically or configured manually
- Each nickname must be unique across the entire network
- A nickname has two priorities: 1) priority and 2) root priority:
  - These are respectively used for nickname collision negotiation and root election

**Nickname Collision Negotiation**

- When nicknames are automatically generated, two RBs may have the same nickname
- The priority field is introduced to avoid nickname collision
- When an RB is added to a network, the LSDB on the network is updated
- The RB is advertised only when the RB's nickname does not conflict with any nickname on the network
- If the RB's nickname conflicts with one on the network, another nickname must be selected for the RB
- Nickname collision will affect running services
# TRILL and Other Layer 2 Technologies Comparison

<table>
<thead>
<tr>
<th></th>
<th>Traditional Layer 2</th>
<th>CSS+iStack</th>
<th>TRILL</th>
<th>SPB</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Encapsulation type</strong></td>
<td>Traditional ETH header (without TTL)</td>
<td>Traditional ETH header (without TTL)</td>
<td>TRILL (with TTL)</td>
<td>MacInMac (with TTL)</td>
</tr>
<tr>
<td><strong>Loop protection</strong></td>
<td>MSTP</td>
<td>Management method</td>
<td>TRILL</td>
<td>SPB</td>
</tr>
<tr>
<td><strong>ECMP</strong></td>
<td>Not supported</td>
<td>Support ECMP using LAG</td>
<td>Support hop-by-hop ECMP, similar to IP network</td>
<td>Support flow-based ECMP on ingress node, but not support hop-by-hop ECMP</td>
</tr>
<tr>
<td><strong>Number of Multicast trees</strong></td>
<td>NA</td>
<td>NA</td>
<td>Few (Layer 2 shared Multicast tree)</td>
<td>Many (Layer 2 source Multicast tree)</td>
</tr>
<tr>
<td><strong>Shortest path forwarding</strong></td>
<td>Not supported</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td><strong>Convergence time</strong></td>
<td>Long, unstable convergence time</td>
<td>Short</td>
<td>Medium (hundreds of milliseconds)</td>
<td>Medium (hundreds of milliseconds)</td>
</tr>
<tr>
<td><strong>Multitenant support</strong></td>
<td>4K (isolated based on VLANs)</td>
<td>4K (isolated based on VLANs)</td>
<td>4K (isolated based on VLANs). In the future, tenants can be isolated using FineLabel, with a maximum of 16M tenants supported)</td>
<td>16M (isolated based on I-SID)</td>
</tr>
<tr>
<td><strong>Networking cost</strong></td>
<td>Low</td>
<td>High (inter-chassis communication occupies high bandwidth. Non-blocking forwarding is difficult to implement)</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td><strong>Network scale</strong></td>
<td>Small</td>
<td>Medium (the number of stacked devices is limited, non-blocking forwarding is not supported)</td>
<td>Large</td>
<td>Large</td>
</tr>
<tr>
<td><strong>Applicable network</strong></td>
<td>Applicable to hierarchical networks where the devices at each layer are aggregated to the upper layer, but not applicable to flat tree network</td>
<td>Applicable to flat tree networks</td>
<td>Applicable to flat tree networks</td>
<td>Applicable to flat tree networks and point-to-multipoint IPTV networks</td>
</tr>
</tbody>
</table>
Agenda

1. TRILL Overview
2. Protocol Mechanism
3. Data Forwarding
4. Device Management and Fault Location
5. Use of TRILL
TRILL Implementation Process

1. Establish Adjacency Relationships
   - Discover a neighbor, shake hands with the neighbor, and the neighbor is placed in the UP state
   - Elect DRB, advertise port roles, and specify AF and designated VLAN over the broadcast links

2. Synchronize Database
   - All devices obtain all the device system IDs, nicknames and properties, interested VLAN (access VLAN) of the ingress RB, and neighbor TLVs on the entire network

3. Calculate Unicast Routes
   - Each device uses itself as the source node to calculate the shortest paths to other nodes

4. Calculate Multicast Routes
   - Each device uses the distribution tree root as the source node to calculate the shortest paths to other nodes
   - Device performs distribution tree pruning and generates pruning entries based on access VLAN information advertised by ingress RBs
Adjacency Management: Neighbor Status Negotiation

**Hello Packet**
- Hello packets are used for negotiating neighbor relationships, specifying designated VLAN, electing the DRB, advertising port roles, and checking MTU
- On the multi-homed access interfaces, hello packets support the AF function

**Neighbor Status**
- **Down:** Initial state, indicating that the neighbor does not exist
- **Detect:** Indicates that a neighbor is detected, but handshake has not been successful
- **2-WAY:** Indicates that handshake is successful, but MTU detection is not complete if MTU detection is enabled
- **Report:** Indicates that handshake and MTU detection are successful

**Neighbor State Machine**
Adjacency Management: DRB Election

**DRB**

- Specifies the designated VLAN to transmit TRILL data over the local link
- Specifies the VLAN forwarder on the access interface
- Determines whether to create Pseudonodes:
  - When the Pseudonode has multiple RB connections over the link, the full mesh connections between RBs can be changed to star connections, reducing the number of advertised LSPs
- If only two RBs exist on the link, the DRB can set a bypass Pseudonode bit in hello packets, indicating that no Pseudonode will be created.

**Neighbor Status**

- **Down:** Indicates that the link status on the port is Down or Trill is disabled
- **Suspend:** Indicates that a TRILL Hello packet with the same <AC address ad the local end MAC address is received, but the local DRB priority is low. This state is similar to the Down state
- **DRB:** Indicates a dRB port, which can transmit and receive TRILL packets
- **Report:** Indicates a non-DRB port, which can transmit and receive TRILL packets
Adjacency Management: Port Role

**Port Roles**

- **Access**: UNI interface, which connects to user terminals, forwards Native Ethernet packets but does not forward TRILL packets. The link on the interface is not advertised by the LSP protocol packets. AF election is required only for this type of interfaces.

- **Trunk**: NNI interface, which supports broadcast links, forwards only TRILL packets and protocol packets, but does not forward Native Ethernet packets.

- **P2P**: NNI interface, which functions the same as the trunk interface except it does not participate in DRB election.

Note: After TRILL is enabled on an interface, the interface becomes a hybrid interface by default. That is, it is the combination of access and trunk interfaces. Therefore, the interface can receive Native Ethernet packets from user terminals as well as forward TRILL packets.
Adjacency Management: AF Election

No AF Module

- The unknown Unicast or broadcast packets in a VLAN may form a loop on the TRILL network, causing network storms
- The access port removes the TRILL header, so the hop count function is invalid. The network cannot be protected

Using AF Module

- The TRILL hello protocol is run between access ports
- The DRB specifies an RB (for example, RB1) as the VLAN forwarder for access users
- Layer 2 loops are prevented at the access side

Diagram:

ES1 is Dual Homed to RB through Traditional Layer 2 Switch
Database Synchronization

### LSDB on Entire Network
- RB1
- RB2
- ... RBn

### Content in LSDB
- **Information Shared by All Nodes**
  - System ID
  - Nickname and properties
  - Neighbor information (link cost, MTU, etc.)

- **Information about Ingress RB**
  - Access user VLAN
  - Relationships between VLANs and distribution tree (Huawei protocol extension)

### Purpose
- Nickname collision negotiation
- Unicast route calculation
- Root election and calculation for Multicast distribution tree
- Pruning calculation
Unicast Routing Table Creation

**SPT Calculation**

- A node uses itself as the source node to generate an SPT to other nodes based on the LSDB of the entire network

**Neighbor Status**

- The outbound interface pointing to the neighbor and next hop address are obtained.
- Nickname Unicast entries are generated based on the nicknames advertised by all nodes

**Example Diagram**

- All links have the same cost
- The system MAC addresses of RB1 to RB6 are MAC 1-6
- The nicknames of RB1 and RB6 are Nickname 1-6
Nickname Unicast Forwarding Table Creation on RB1

- RB1 generates the shortest path tree to all other nodes, ensuring that Unicast traffic is forwarded along the shortest path.
- RB1 has two equal-cost shortest paths to each of RB2, RB3, and RB4; therefore, Unicast traffic is load balanced. Link bandwidth use efficiency is improved.
- RB1 searches the nickname Unicast forwarding table for the egress nickname contained in the TRILL header of the received data packet, and obtains the matching outbound interface and next hop.
- If multiple outbound interfaces are found, RB1 selects one based on ECMP algorithm to forward the packet.

<table>
<thead>
<tr>
<th>Neighbor</th>
<th>Outbound interface, next-hop MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>RB5</td>
<td>L1, MAC5</td>
</tr>
<tr>
<td>RB6</td>
<td>L2, MAC6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Destination Nickname</th>
<th>Outbound interface and next-hop MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>nickname2</td>
<td>L1, MAC5, L2, MAC6</td>
</tr>
<tr>
<td>nickname3</td>
<td>L1, MAC5, L2, MAC6</td>
</tr>
<tr>
<td>nickname4</td>
<td>L1, MAC5, L2, MAC6</td>
</tr>
<tr>
<td>nickname5</td>
<td>L1, MAC5</td>
</tr>
<tr>
<td>nickname6</td>
<td>L2, MAC6</td>
</tr>
</tbody>
</table>
Multicast Route Calculation

- **Elect the device with the highest root priority**: Each device obtains the nickname of the RB with the highest root priority and the minimum number (n) of distribution trees on the network.

- **Distribution tree root selection**: The RB with the highest root priority can specify the distribution tree roots. If the RB does not specify the roots, the RBs with the top N root priorities are used as roots.

- **Distribution tree calculation**: N roots are used as source nodes to calculate the shortest paths to other nodes.

- **RPF check table creation**: The RPF check table is created based on the distribution tree information advertised by each ingress RB. The RPF check table is used to prevent loops.

- **Prune calculation**: Prune is performed based on access VLAN information advertised by each ingress RB. The prune operation conserves bandwidth on the TRILL network.

Note: The RB with the highest root priority and the distribution tree roots must be reachable through Unicast routes; therefore, Multicast routing calculation must be performed after Unicast routing calculation.
### Multicast Forwarding Table and RPF Check Table

**RPF Check**

- Ingress RB6 selects distribution tree 1 to forward Multicast traffic. Traffic reaches interface L1 on RB2. The traffic reaching other interfaces is discarded because of RPF check failure.

- Shared trees are used on the TRILL network. All ingress RBs may receive Multicast traffic; therefore, the RBs need to perform an RPF check, based on root nicknames, ingress RB nicknames, and inbound interfaces. RPF check prevents loops on the TRILL network.

**Multicast Forwarding**

- When forwarding Multicast packets, the processor must prune source interfaces to prevent Multicast packets from entering and leaving a device through the same interface. For example, packets arriving at interface L1 cannot leave through L1.

- Each RB calculates a Multicast distribution tree based on roots. They obtain the topology of the entire network and use the same algorithm; therefore, all RBs establish distribution trees in the same way. Thus, the uniform distribution tree entries can be created even if no Join or Prune message is transmitted on the PIM network.

### RPF check table on RB2

<table>
<thead>
<tr>
<th>Root nickname</th>
<th>Ingress Nickname</th>
<th>Inbound interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>RB1</td>
<td>RB6</td>
<td>L1</td>
</tr>
<tr>
<td>RB7</td>
<td>RB6</td>
<td>L3</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

### Nickname Multicast table on RB2

<table>
<thead>
<tr>
<th>Root nickname</th>
<th>Outbound interface list</th>
</tr>
</thead>
<tbody>
<tr>
<td>RB1</td>
<td>L1, L2, L3</td>
</tr>
<tr>
<td>RB7</td>
<td>L1, L3</td>
</tr>
</tbody>
</table>

### Replication and Forwarding
VLAN Based Pruning Calculation

Ingress RB Advertises Information

- As shown in the figure on the right, RB2, RB4, and RB9 access VLAN 1, and RB4 and RB10 access VLAN 2

All Other RBs Perform Prune Based on VLANs

- Other RBs perform pruning calculations based on information advertised by ingress RBs and generate pruning entries. Multicast traffic on the TRILL network is replicated only to edge RBs and forwarded on-demand. This method conserves bandwidth on the TRILL network.
VLAN Based Pruning Calculation

When forwarding Multicast packets, the RB uses the destination nickname and inner VLAN ID in the TRILL header as the key to search the Multicast entries of VLAN-based prune.

- RPF check is performed based on root nickname and ingress RB nickname, but is irrelevant to pruning calculation.
The ingress RB selects a distribution tree for each access VLAN. For example in the above figure, traffic in VLAN Odd is forwarded through the distribution tree with Root 1. Traffic in VLAN Even is forwarded through the distribution tree with Root 2. Thus Multicast traffic on the entire network is load balanced based on access VLANs.
Distribution tree pruning Optimization

<table>
<thead>
<tr>
<th>Root RB</th>
<th>VLAN ID</th>
<th>Outbound interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root1</td>
<td>1</td>
<td>L1</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>Root1</td>
<td>1000</td>
<td>L1</td>
</tr>
<tr>
<td>Root1</td>
<td>1001</td>
<td>L1</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>Root1</td>
<td>2000</td>
<td>L1</td>
</tr>
<tr>
<td>Root2</td>
<td>1</td>
<td>L2</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>Root2</td>
<td>1000</td>
<td>L2</td>
</tr>
<tr>
<td>Root2</td>
<td>1001</td>
<td>L2</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>Root2</td>
<td>2000</td>
<td>L2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Root RB</th>
<th>VLAN ID</th>
<th>Outbound interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root1</td>
<td>1</td>
<td>L1</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>Root1</td>
<td>1000</td>
<td>L1</td>
</tr>
<tr>
<td>Root2</td>
<td>1001</td>
<td>L2</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>Root2</td>
<td>2000</td>
<td>L2</td>
</tr>
</tbody>
</table>

Ingress RB Advertises Information

- The ingress RB load balances Multicast traffics based on VLANS
- The ingress RB advertises the relationships between VLANS and roots. RB1 advertises the relationships between VLANS 1-1000 and root 1; RB2 advertises the relationships between VLANS 1001-2000 and Root 2

All Other RBs Perform Prune Based on VLANS

- Other RBs perform pruning calculation based on the relationships between VLANS and distribution trees advertised by ingress RBs, not based on each distribution tree

The Number of Pruning Entries is Independent of the Number of distribution Trees
Agenda

1. TRILL Overview
2. Protocol Mechanism
3. Data Forwarding
4. Device Management and Fault Location
5. Use of TRILL
TRILL Data Forwarding Process

General Process

- Host A sends an ARP request packet to host B
- Host B returns an ARP reply packet to host A
- Host A sends a Unicast packet to host B
- Note: Hosts A, B, C, and D belong to VLAN 1
- The forwarding process for Multicast and broadcast packets in the VLAN is the same as the forwarding process for ARP request packets
**ARP Request Forwarding Process**

**Multicast distribution Tree with RB2 and RB5 as Roots**

1. The ingress RB searches Multicast forwarding entries based on the distribution tree roots corresponding to the VLAN, and encapsulates and forwards ARP packets.
2. The root RB sends packets to all Multicast group members.
3. After receiving the packets, the egress RB decapsulates and broadcasts the packets locally.
ARP Reply Forwarding Process

1. The ingress RB searches MAC forwarding entries, selects a link to the destination RB, encapsulates and forwards ARP packets.

2. The RBs along the forwarding path forward the packets based on the Unicast distribution tree.

3. After receiving the packets, the egress RB decapsulates and forwards packets locally.
Unicast Forwarding Process from A to B

1. The ingress RB searches MAC address table for the destination RB. It selects a link and encapsulates Unicast packets.

2. The RBs along the forwarding path forward the packets according to the Unicast distribution tree entries.

3. The egress RB receives and decapsulates the packets, and forwards them locally.
Agenda

1. TRILL Overview
2. Protocol Mechanism
3. Data Forwarding
4. Device Management and Fault Location
5. Use of TRILL
In-Band Management

- Each RB has a VLANIF interface corresponding to the inner management VLAN.
- An RB advertises network segment 10.1.1.0/24 corresponding to the management VLAN sub-interface.
- The network administrator connects to the in-band management VLANIF interface through egress router 1 (from the IP network to TRILL network) and the TRILL network.
- The network administrator can use Telnet, SNMP, or NetConf to manage and configure the RBs through in-band network.

**Diagram Details:**
- RB1: IP: 10.1.1.2
- RB2: IP: 10.1.1.3
- RB3: IP: 10.1.1.4
- TRILL Campus
- IP Network
- Router 1
- IP: 10.1.1.1/24
- Request
- Reply
- Network Administrator
- PC1
- IP: 100.1.1.1

**Diagram Notes:**
- VLANIF interface of the management VLAN.
- The management VLAN is the inner VLAN in TRILL encapsulation.
- Management VLAN sub-interface corresponding to the router.
Fault Location

- RBs perform TRILL ping to verify connectivity of the forwarding path
- The protocol packets are transmitted over the TRILL OAM channel

Ping Packet Forwarding Process

1. The user specifies the destination RB nickname, timeout interval, and hop count on the transmit RB, and performs a ping operation. The RB searches the nickname Unicast forwarding table to forward the ping packet.

2. The intermediate nodes search the nickname forwarding table until the TTL of the ping packet decreases to 0 or the packet reaches the destination, and forward the packet to the CPUs.

3. The CPU finds that the TTL of the packet is 1, and checks whether the local RB is the destination. If the RB is the destination, the RB returns an Echo Reply; otherwise, it returns an Error Notification with the error message “TTL timeout.”
<table>
<thead>
<tr>
<th></th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TRILL Overview</td>
</tr>
<tr>
<td>2</td>
<td>Protocol Mechanism</td>
</tr>
<tr>
<td>3</td>
<td>Data Forwarding</td>
</tr>
<tr>
<td>4</td>
<td>Device Management and Fault Location</td>
</tr>
<tr>
<td>5</td>
<td>Use of TRILL</td>
</tr>
</tbody>
</table>
Gateway Deployment and Server Access Mode

**Gateway Deployment**

- The core RB is separated from the Layer 3 gateway, or;
- The core RB is integrated with the Layer 3 gateway
- The device is divided into two VSs. One VS implements Layer 3 gateway function and the other one implements the RB function

**TRILL Network Deployment**

- Access switches are deployed in TOR or EOR mode
- The TRILL network can be extended to the access switches, covering the entire DC
- Access switches support the stack function. Servers are dual homed to the access switches to improve service reliability

**Network 1: Separating Layer 3 Gateway and Aggregation Switch**

**Network 2: Integrating Layer 2 Gateway and Aggregation switch**
Value Added Service Deployment

Features

- The FWs and LBs are located between access switches and egress routers to process southbound and northbound traffic.
- To process eastbound and westbound traffic between network segments, the gateway can be deployed on the FW if servers are located in un-trusted zones.
- If servers are located in the same trusted zone, the gateway can be deployed on the aggregation switch.
- The eastbound and westbound traffic within a network segment is forwarded at Layer 2 on the TRILL network.

Southbound and northbound traffic between client and server
Inter-network segment traffic between servers, filtered by firewall
Inter-network segment traffic between servers, not filtered by firewall
Inter-network segment traffic between servers
DC Seamless Migration 1

Preserve Customer Investment

**Migration Method**

- In the early history of DC, Layer 2 networks used MSTP because switches (such as S9300) hardware did not support TRILL
- With new devices (such as CE12800) DCs can support TRILL and large Layer 2, the large Layer 2 network can also run MSTP
- Servers can be connected to access switches on the MSTP or TRILL network. Thus, VMs can migrate the entire large Layer 2 network

**Implementation**

- The edge devices on the TRILL network simulate the MSTP root bridges to communicate with the MSTP network.
- After receiving a TCN packet indicating MSTP topology change, the edge devices clear their own MAC address entries and request the peer RBs to clear the related MAC address entries
DC Seamless Migration 2

Seamless Migration of O&M

Seamless Migration

VLAN 1-3000 VLAN 1-3000 VLAN 3001 VLAN 3001

VLAN 1-3000 VLAN 1-3000 VLAN 3001 VLAN 3001
**TRILL Application – Interconnection Between DCs (1)**

TRILL Network Capable of Interconnecting with Other types of Networks

- TRILL does not run between egress RBs or different DCs
- The interconnecting interfaces between the RBs are inbound interfaces for servers in the respective TRILL sites
- Different DCs are interconnected through a VPLS network or optical fibers
- Egress RBs must learn MAC addresses of all servers

### TRILL Network Capable of Interconnecting with Other types of Networks

<table>
<thead>
<tr>
<th>MAC1</th>
<th>Outbound Interface 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC of Site 2</td>
<td>L1</td>
</tr>
<tr>
<td>MAC of Site 3</td>
<td>L2</td>
</tr>
<tr>
<td>MAC of Site 1</td>
<td>Interface in Site 1</td>
</tr>
</tbody>
</table>
TRILL Application – Interconnection Between DCs (2)

Fewer MAC Addresses to be learned on Egress RBs

- Multiple DC sites participate in computing a distribution tree
- Egress RBs in each DC work as transit nodes and do not encapsulate or decapsulate TRILL data packets
- Egress RBs do not need to learn server MAC addresses
- The Multicast distribution tree uses an egress RB as the root, saving bandwidth on egress links
- Multicast packets are forwarded through local links if they do not need to traverse the local DC site
Campus Network 1

- **Access layer and aggregation layer**: At Layer 2, the TRILL protocol is used to replace MSTP to increase bandwidth use efficiency, reduce convergence time, implement automatic deployment, and prevent loops.

- **Aggregation layer and core layer**: Layer 3 networks are deployed between departments to forward inter-department traffic.

- Devices at the aggregation layer function as gateways to interconnect Layer 2 and Layer 3 networks.
Campus Network 2

- The sites of a service system are distributed in different locations:
  - For example, building sites need to communicate with each other through Layer 2
- Each site set up a Layer 2 network using Native Ethernet, and different sites are connected by the TRILL network
- The TRILL network forwards traffic between sites, forming a large Layer 2 network
- The gateway is deployed on the campus egress router or core switch to interconnect Layer 2 and Layer 3 networks
## Glossary of Terms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>RB</td>
<td>Router Bridge</td>
</tr>
<tr>
<td>AF</td>
<td>Appointed Forwarder</td>
</tr>
<tr>
<td>DRB</td>
<td>Designated Router Bridge</td>
</tr>
<tr>
<td>SPF</td>
<td>Shortest Path First</td>
</tr>
<tr>
<td>IS-IS</td>
<td>Intermediate System to Intermediate System</td>
</tr>
<tr>
<td>LSP</td>
<td>Link State PDU</td>
</tr>
<tr>
<td>P2P</td>
<td>Point to Point</td>
</tr>
<tr>
<td>VS</td>
<td>Virtual Switch</td>
</tr>
<tr>
<td>RPF</td>
<td>Reverse Path Forwarding</td>
</tr>
<tr>
<td>UNI</td>
<td>User Network Interface</td>
</tr>
<tr>
<td>NNI</td>
<td>Network Network interface</td>
</tr>
</tbody>
</table>
Thank You

enterprise.huawei.com