What You Make Possible
Redundancy Mechanisms for Carrier Ethernet and Layer 2 VPN Services

BRKSPG-2207
Agenda

- Introduction
- Resiliency Fundamentals
- Access Resiliency Mechanisms
- Aggregation and Core Resiliency Mechanisms
- MAC Flushing Mechanisms
- Redundancy Solutions
- Summary
Introduction
Carrier Ethernet Networks

Policy Control Plane (per subscriber)

Access
- Mobile
- Residential
- Business
- Corporate
- Residential

Aggregation
- Portal
- Monitoring
- Billing
- Subscriber Database
- Identity
- Address Mgmt
- Policy Definition

Edge
- DSL
- Cable
- MSPP
- ETTx
- PON
- Ethernet
- MPLS / IP

Focus of presentation

Core Network
- MPLS / IP

Content Farm
- VOD
- TV
- SIP

ETTx
- PON
- MSPP
- Cable
- Residential
- Business
- Corporate
- Residential

Content Farm
- VOD
- TV
- SIP

Carrier Ethernet Networks
- Ethernet
- MPLS / IP
- Focus of presentation
Resiliency Fundamentals
Resiliency Fundamentals

- **Resiliency definition** from Metro Ethernet Forum:
  - “A self-healing property of the network that allows it to continue to function with minimal or no impact to the network users upon disruption, outages or degradation of facilities or equipment in the MEN” [MEF-2]

- **User’s perspective**
  - SLA attributes such as:
    - Availability
    - Mean Time To Restore (MTTR)
    - Mean Time Between Failure (MTBF)
  - Actual methods and mechanisms used by SP not relevant

- **Provider’s perspective**
  - Translation of SLAs to network protection requirements
  - Selection of mechanisms / protocols to provide such protection
Ethernet-Aware Resiliency Mechanisms

Key Requirements

- MUST NOT allow data-plane loops
  Not even transient ones, as Ethernet header has no Time To Live (TTL) or equivalent field

- MUST ensure congruency of forward and reverse data-plane paths
  Prevent MAC moves in scenarios with Load Balancing

- MUST ensure a unique entry/exit point into an Ethernet segment
  Prevent delivery of duplicate packets - Designated Forwarder notion

- MUST ensure MAC-flushing and relearning after topology change notification
  Prevent black-holing of traffic - MAC address tables must be updated after re-convergence events
Access Resiliency Mechanisms
Access Resiliency Mechanisms
Multi-Chassis LACP (mLACP) and Inter-Chassis Communication Protocol (ICCP)
Multi-Chassis LACP and ICCP Overview

- mLACP & ICCP enable a switch/router to use standard Ethernet Link Aggregation for device dual-homing, with active/standby redundancy.
- Dual-homed Device (DHD) operates as if it is connected to single virtual device and runs IEEE std. 802.1AX-2008 (LACP).
- Point of Attachment (PoA) nodes run Inter-chassis Communication Protocol (ICCP) to synchronize state & form a Redundancy Group (RG).
Protected Failure Points

mLACP Offers Protection Against 5 Failure Points:

- **A**: DHD Port Failure
- **B**: DHD Uplink Failure
- **C**: Active PoA Port Failure
- **D**: Active PoA Node Failure
- **E**: Active PoA Isolation from Core Network
Background: Link Aggregation Control Protocol

- **System attributes:**
  - **System MAC address:** MAC address that uniquely identifies the switch
  - **System priority:** determines which switch’s Port Priority values win

- **Aggregator (bundle) attributes:**
  - **Aggregator key:** identifies a bundle within a switch (per node significance)
  - **Maximum links per bundle:** maximum number of forwarding links in bundle – used for Hot Standby configuration
  - **Minimum links per bundle:** minimum number of forwarding links in bundle, when threshold is crossed the bundle is disabled
Background: Link Aggregation Control Protocol (Cont.)

- **Port attributes:**
  - **Port key:** defines which ports can be bundled together (per node significance)
  - **Port priority:** specifies which ports have precedence to join a bundle when the candidate ports exceed the Maximum Links per Bundle value
  - **Port number:** uniquely identifies a port in the switch (per node significance)
Extending LACP Across Multi-Chassis: mLACP

- mLACP uses ICCP to synchronize LACP configuration & operational state between PoAs, to provide DHD the perception of being connected to a single switch.
- All PoAs use the same System MAC Address & System Priority when communicating with DHD
  - Configurable or automatically synchronized via ICCP
- Every PoA in the RG is configured with a unique Node ID (value 0 to 7). Node ID + 8 forms the most significant nibble of the Port Number
- For a given bundle, all links on the same PoA must have the same Port Priority.
Inter-Chassis Communication Protocol

- ICCP allows two or more devices to form a ‘Redundancy Group’
- ICCP provides a control channel for synchronizing state between devices
- ICCP uses TCP/IP as the underlying transport
  - ICCP rides on targeted LDP session, but MPLS need not be enabled
- Various redundancy applications can use ICCP:
  - mLACP
  - Pseudowire redundancy
- Under standardization in the IETF:
  - draft-ietf-pwe3-iccp-07.txt
Failover Operation

Port/Link Failures

Step 1 – For port/link failures, active PoA evaluates number of surviving links (selected or standby) in bundle:

- If > M, then no action
- If < M, then trigger failover to standby PoA

Step 2A – Active PoA signals failover to standby PoA over ICCP

Step 2B – Failover is triggered on DHD by one of:

- **Dynamic Port Priority Mechanism**: real-time change of LACP Port Priority on active PoA to cause the standby PoA links to gain precedence
- **Brute-force Mechanism**: change the state of the surviving links on active PoA to admin down

Step 3 – Standby PoA and DHD bring up standby links per regular LACP procedures
Failover Operation

Node Failure

Step 1A – Standby PoA detects failure of Active PoA via one of:
- IP Route-watch: loss of IP routing adjacency
- BFD: loss of BFD keepalives

Step 1B – DHD detects failure of all its uplinks to previously active PoA

Step 2 – Both Standby PoA and DHD activate their Standby links per regular LACP procedures
### Failover Operation

**PoA Isolation from Core**

**Step 1** – Active PoA detects all designated core interfaces are down

**Step 2A** – Active PoA signals standby PoA over ICCP to trigger failover

**Step 2B** – Active PoA uses either Dynamic Port Priority or Brute-force Mechanism to signal DHD of failover

**Step 3** – Standby PoA and DHD bring up standby links per regular LACP procedures
Access Resiliency Mechanisms

mLACP Active/Active (per VLAN Load-Balancing) – a.k.a Pseudo mLACP
PoA ports are configured to assume mLACP Active/Active (mLACP-AA) role:
- Ports act as if connected to a virtual device over an MC-LAG with mLACP
- Ports placed in Active/Active Mode with manual VLAN load-balancing

Access node perceives the ports/links to each PoA as being independent.

Supports Dual Homed Device (DHD)
Setup

- DHD configures all uplinks towards a single POA in a bundle (LAG)
  - Links towards different POAs belong to different bundles
- DHD enables all VLANs on both bundles to PoAs
- POAs configured to allow certain VLANs and block others
  - A given VLAN can be active on a single PoA at a time
  - Per VLAN load-balancing
- Traffic from DHD to core initially flooded to both PoAs until DHD learns which bundle is active for what VLANs
Fault Protection Points

- Provide Protection Against 5 Failure Points:
  - A: DHD Uplink Port Failure
  - B: DHD Uplink Failure
  - C: POA Downlink Port Failure
  - D: POA Node Failure
  - E: POA Isolation from core network
Failure Procedures

For Failure Points A, B, and C

1. DHD & Active POA detect port down
2. Active POA signals switchover to Standby via ICCP
3. Standby unblocks affected VLANs over downlink and flushes its MAC tables
4. Standby triggers Multiple VLAN Registration Protocol (MVRP) ‘new’ declaration towards DHD to induce MAC flushing
Failure Procedures

For Failure D

1. Standby POA detects failure of active POA via IP Route-Watch or BFD
2. Standby POA unblocks affected VLANs over downlink
3. Standby POA flushes its MAC tables & triggers MVRP MAC flush notification towards DHD
Failure Procedures

For Failure E

1. Active POA detects isolation from core, blocks its previously active VLANs
2. Active POA informs standby POA of need to failover via ICCP
3. Standby POA activates (unblocks) affected VLANs on downlink and flushes its MAC tables
4. Standby POA triggers MVRP registrations with ‘new” bit set (for affected VLANs) towards DHD to trigger MAC flushing.
Access Resiliency Mechanisms
Other Multi-chassis Link Aggregation Solutions
Virtual Port Channel – vPC

- vPC is a multi-chassis link aggregation mechanism
  - active/active redundancy model
  - flow-based load-balancing

- Independent control plane on the peers.

- Requires a dedicated interconnect between peers (vPC Peer Link)
  - synchronize state between peers
  - Carry normal flooded traffic and all traffic in case of vPC member port failure

- Uses Cisco Fabric Services (CFS) protocol
  - state synchronization and configuration validation between vPC peer devices

- Uses a Peer Keepalive link to detect split-brain condition
  - out of band heartbeat, not carried over Peer Link
  - either dedicated link or L3 interconnect over infrastructure
Virtual Switching System (VSS)

- Two physical switches appear as a single virtual device.
  - Single control-plane (e.g. one IP endpoint)
  - Single management point
  - Dual active forwarding planes

- Requires dedicated interconnect: Virtual Switch Link (VSL)
  - Used for control plane synchronization and data traffic.
  - Uses special Virtual Switch Header for encapsulating data.

- All control plane state is SSO synchronized from Active to Standby.
## Comparison

<table>
<thead>
<tr>
<th>Solution</th>
<th>Control Plane</th>
<th>Configuration Synchronization</th>
<th>Dedicated Physical Interconnect Required</th>
<th>Interconnect Usage</th>
<th>Load Balancing per DHD</th>
</tr>
</thead>
<tbody>
<tr>
<td>mLACP</td>
<td>Multiple</td>
<td>Manual (normalized by ICCP)</td>
<td>No</td>
<td>Control Plane Sync</td>
<td>None</td>
</tr>
<tr>
<td>mLACP Active-Active</td>
<td>Multiple</td>
<td>Manual</td>
<td>No</td>
<td>Control Plane Sync</td>
<td>Per VLAN</td>
</tr>
<tr>
<td>vPC</td>
<td>Multiple</td>
<td>Manual (verified by Cisco Fabric Services)</td>
<td>Yes</td>
<td>Control Plane Sync + Data Traffic</td>
<td>Per Flow¹</td>
</tr>
<tr>
<td>VSS</td>
<td>Single</td>
<td>Automatic</td>
<td>Yes</td>
<td>Control Plane Sync + Data Traffic</td>
<td>Per Flow</td>
</tr>
</tbody>
</table>

1: With MST or VPLS, there’s a single egress point to the Aggregation network.
Access Resiliency Mechanisms
Ethernet Ring Protection (ITU-T G.8032)
Overview

- Protection switching at Ethernet layer
  - Fast convergence (50 ms) with HW support

- Leverage Ethernet CFM (ITU-T Y.1731) for
  - Fault Detection (IEEE 802.1ag Continuity Check Message - CCM)
  - Control Channel (R-APS)

- Topology Support
  - Closed Ring
  - Open Ring (G.8032 v.2)
  - Cascaded Rings (Ladder Network) (G8032 v.2)

- Load Balancing (multi-instance support) (G.8032 v.2)

- Administrative Tools (G.8032 v.2)
  - Manual Switchover
  - Forced Switchover
Setup and Basic Operation

Setup

- Map VLANs into Ethernet Ring Protection (ERP) Instances
- Select Ring Protection Link (RPL) per instance and configure ports as RPL owners
- Optionally: Configure RPL Neighbor ports
- Use CFM Down MEPs to monitor link faults via CCMs

Normal Operation

- When no faults, RPL Owner (and neighbor) are blocked.
- RPL Owner (& neighbor) send R-APS message with No Request/Link Blocked every 5 sec.
G.8032 protects against any **single** Link, Port or Node failure within a ring

- **A:** Failure of a **port** within the ring
- **B:** Failure of a **link** within the ring
- **C:** Failure of a **node** within the ring
Failure Handling

1. Switches detect link failure via:
   - Link Down Event (PHY based)
   - Loss of CFM CCMs

2. Switches block ports connected to failed link & flush MAC tables

3. Send R-APS messages with Signal Fail (SF) code on other ring port

4. Switches receiving R-APS (SF) flush their MAC forwarding tables

5. RPL Owner (and neighbor) unblock their ports
Open Ring Support

Two Solutions:

- **Open ring with R-APS Virtual Channel (VC)**
  - R-APS messages flow over a virtual channel supplied by another network to close the ring control channel
  - Ring is closed from control perspective but open from data perspective

- **Open ring without R-APS Virtual Channel (VC)**
  - Special handling of R-APS on the ring: R-APS control messages can pass over the RPL to reach all nodes
  - Requires independent blocking of control vs. data channels on RPL owner/neighbor

![Diagram with VC](image1)
![Diagram without VC](image2)
Interconnecting Rings

- Networks can be constructed out of closed and open rings
  - Rule: a given link must belong to a single ring
  - 1 Major ring (closed) and multiple Sub-rings (open)
- R-APS Event Message to signal ‘MAC flushing notification’ from one ring to another interconnected ring
- If one ring provides R-APS VC for a subtended ring, the R-APS channels for the two rings must be in different VLANs for correct operation
Ring Instances

- G.8032 v.2 supports multiple ERP instances over a ring
- Disjoint VLANs are mapped into instances
- Every ERP instance can have a different RPL
  - Enables load-balancing over the ring
Access Resiliency Mechanisms
Resilient Ethernet Protocol (REP)
REP Protocol Basics
A Segment Protocol

- REP operates on chain of bridges called segments
- A port is assigned to a unique segment using:
  (config-if)# [no] rep segment {id}
- A segment can have up to two ports on a given bridge
REP Protocol Basics

Blocked Port

- When all links are operational, a unique port blocks the traffic on the segment
  - No connectivity between edge ports over the segment
- If any failure occurs within the segment, the blocked port goes forwarding
Protected Failure Points

REP Protects Against Any Single Link, Port or Node Failure Within a Segment

- A: Failure of a port within the segment
- B: Failure of a link within the segment
- C: Failure of a node within the segment
REP Protocol Basics

REP Provides Two Redundant Gateways

- The segment provides one level of redundancy
- Hosts on the segment can reach the rest of the network through either edge port, as necessary
Access Resiliency Mechanisms

MST Access Gateway (MST-AG)
(a.k.a. Reverse Layer 2 Gateway Ports (R-L2GP))
Motivation for MST-AG

- Terminate multiple Ethernet access networks into same pair of ‘Gateway’ nodes
- Each access network maintains independent topology (control plane isolation)
- Fast convergence in all cases
- Access nodes run standard MST
- Gateway nodes act as root bridges
**MST-AG Overview**

- **MST-AG ports**
  - Send pre-configured BPDUs advertising “virtual root” by best bridge and 0 cost to root by second best bridge
  - Virtual Root may coincide with the MST-AG node, or not
  - Ignore incoming BPDUs from access network, except for TCN
  - Always in Designated Forwarding state

- React and relay TCN over a special control pseudowire

- **L2 access network**
  - Can have arbitrary topology (e.g. ring or mesh)
  - Runs standard MST protocol
  - Handles port blocking/unblocking
Protected Failure Points

MST-AG Provides Protection Against Any of the Following Failure Points:

- **A**: Failure of link connecting access network to gateway
- **B**: Failure of gateway access-facing port
- **C**: Gateway node failure
- **D**: Failure within access network, including access network total split
- **E**: Isolation of the gateway from core network (via Link State Tracking feature)
Failure Scenarios
Gateway Direct Failures

- Access switches detect failure
  - Note: for Failure E, gateway brings down line-protocol on link to access
- MST re-converges in access network, choosing path through second Gateway to reach the root
- TCN propagated all the way to new root
Failure Scenarios

Access Network Split

- Access network completely partitioned
- Sub-network isolated from original root selects path through second Gateway
- TCN is propagated to new root, relayed over control PW and into the other sub-network
Aggregation and Core Resiliency Mechanisms
One-Way Pseudowire Redundancy

Overview

- Allows dual-homing of one local PE to two or more remote PEs
- Two pseudowires: primary and backup provide redundancy for a single AC (1:1 Protection)
- Multiple backup PWs (different priorities) can be defined (N:1)
- Alternate LSPs (TE Tunnels) can be used for additional redundancy
- Upon primary PW failure, failover is triggered after a configurable delay (seconds)
- Configurable Revertive / Non-Revertive upon recovery
Pseudowire Redundancy with LDP

 PW Status Signaling

- 0x00000000 - Pseudowire forwarding (clear all failures)
- 0x00000001 - Pseudowire Not Forwarding
- 0x00000002 - Local Attachment Circuit (ingress) Receive Fault
- 0x00000004 - Local Attachment Circuit (egress) Transmit Fault
- 0x00000008 - Local PSN-facing PW (ingress) Receive Fault
- 0x00000010 - Local PSN-facing PW (egress) Transmit Fault
- 0x00000020 - PW Preferential Forwarding Status
- 0x00000040 - PW Request Switchover Status

When set == PW fwd Standby; when cleared == PW fwd Active
Only this bit is required/used (with help of ICCP)
One-Way Pseudowire Redundancy

Failure Protection Points

A. Loss of next hop P node as notified by IGP
   – PW failover is delayed to allow IGP chance to restore

B. Loss of Remote PE
   – LDP session timeout
   – BFD timeout
Two-Way Pseudowire Redundancy

Overview

- Allows dual-homing of two local PEs to two remote PEs
- PW Preferential Forwarding Status determined by ICCP application (e.g. mLACP)
  - Four pseudowires: 1 primary and 3 backup provide redundancy for a dual-homed device
Two-Way Pseudowire Redundancy

Failure Protection Points

A. Failure of primary PE node
B. Isolation of primary PE node from the MPLS core
Two-Way Pseudowire Redundancy

Independent Operation Mode

- Every PE decides the **local** forwarding status of the PW: Active or Standby
- A PW is **selected as Active** for forwarding if it is declared as Active by both local and remote PEs
- A PW is **selected as Standby** for forwarding if it is declared as Standby by either local or remote PE
Two-Way Pseudowire Redundancy

Determining Pseudowire State

- **VPWS / H-VPLS (U-PE) – two-way coupled:**
  - When AC changes state to Active\(^1\), both PWs will advertise Active
  - When AC changes state to Standby\(^1\), both PWs will advertise Standby

- **H-VPLS (U-PE) – two-way decoupled:**
  - Regardless from AC state, Primary PW and Backup PWs will advertise Active state

- **For H-VPLS (N-PE), all PWs in VFI are Active simultaneously, for both access and core PWs**

\(^1\) Active / Standby AC states determined for example by mLACP
Two-Way Pseudowire Redundancy

Determining Pseudowire State (Cont.)

- **VPLS – Two-way Coupled:**
  - When at least 1 AC in VFI changes state to Active, all PWs in VFI will advertise Active
  - When all ACs in VFI change state to Standby, all PWs in VFI will advertise Standby mode

- **VPLS – Two-way Decoupled:**
  - Regardless from AC states, all PWs in VFI will advertise Active state
MAC Flushing Mechanisms
Why MAC Flushing Is Needed?

Topology Changes

- Bridges learn the location of the stations from the traffic they forward
- Mac-addresses are added to a filtering table
- After a failure, the filtering table must be updated
G.8032 MAC Flushing Notification

- Nodes evaluate every R-APS message received. If the message indicates that the location of blocking has moved (via Node ID and BPR), then flushing is triggered.
- A specific R-APS Event Message with Flush indication is used to trigger a burst of 3 flushes from one ring to another in case of cascaded rings.
REP Topology Change Notification

- On topology change, nodes next to fault send Blocked Port Advertisement (BPA) with Topology Change (TC) bit set to 1
- Nodes react to this by flushing their MAC tables for affected VLAN(s)
- Topology changes not propagated beyond segment except by explicit configuration
RSTP Topology Change Notification

- Rapid STP (IEEE 802.1D-2004) introduced new Topology Change Notification mechanism (from IEEE 802.1D-1998)

- Detection — Transitions from blocking to forwarding state cause topology change
  - i.e., only increase in connectivity is TC
  - Link Down events no longer trigger TCN
  - Edge ports (port-fast) are not flushed

- Notification — via TCN Flag in configuration BPDU
  - TCN BPDU no longer used; no ack required (TCA flag not used)

- “Broadcasted” on the network by the initiator (not by the Root bridge as in IEEE 802.1D-1998)
Multiple VLAN Registration Protocol (MVRP)

- Application of IEEE 802.1ak Multiple Registration Protocol (MRP)
- Builds dynamic VLAN reachability trees within a spanning tree instance
  - Enables source pruning of floods
- Defines new declaration messages as a replacement for TCNs
  - Sent in addition to existing STP TC messages
  - Generated by ports declaring a given VID on bridges that detect a topology change
- Net effect — only VLANs active in the area of the network that is actually affected by the topology change are flushed
  - VLANs not present in that part of the network are unaffected
  - VLANs that are affected are only flushed in the affected sub-tree
LDP MAC Address Withdrawal

- Transmitted by a VPLS PE that detects a topology change to all other PEs in the VPLS instance
- Out of band indication
- Optionally may contain a list of MAC addresses to be flushed
  - If MAC list is empty → flush all addresses except those learnt from transmitting PE
  - If specific MAC → remove specified MAC address(es)
- Defined in RFC4762
End-to-End Redundancy Solutions
# End-to-End Redundancy Solutions

<table>
<thead>
<tr>
<th>Service Type</th>
<th>Transport Enabler</th>
<th>Access Redundancy</th>
<th>Protocol / Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-LINE</td>
<td>VPWS</td>
<td>Hub and Spoke (Active / Backup)</td>
<td>mLACP + 2-way PW Red. (coupled mode)</td>
</tr>
<tr>
<td>E-LINE</td>
<td>VPLS</td>
<td>Ring</td>
<td>MST + MST-AG</td>
</tr>
<tr>
<td>E-LINE</td>
<td>VPLS</td>
<td>Ring</td>
<td>G.8032</td>
</tr>
<tr>
<td>IP / L3VPN</td>
<td>Ethernet</td>
<td>Hub and Spoke (Active / Backup)</td>
<td>mLACP + VRRP</td>
</tr>
<tr>
<td>(*) E-LAN</td>
<td>VPLS</td>
<td>Hub and Spoke (Active / Backup)</td>
<td>mLACP + 2-way PW Red. (decoupled mode)</td>
</tr>
<tr>
<td>(*) E-LAN</td>
<td>H-VPLS</td>
<td>Hub and Spoke (Active / Backup)</td>
<td>mLACP + 2-way PW Red. (decoupled mode)</td>
</tr>
<tr>
<td>(*) E-LAN</td>
<td>VPLS</td>
<td>Ring</td>
<td>REP</td>
</tr>
</tbody>
</table>

(*) See Appendix Section
E-LINE Availability Models
Active/Backup Access Node Redundancy (mLACP)
E-LINE Availability Model
Active / Backup Access Node Redundancy (mLACP)

- Port / Link Failures

- For VPWS Coupled Mode, attachment circuit (AC) state (Active/Standby) drives PW state advertised to remote peers

### Events

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial state</td>
<td>Initial state</td>
</tr>
<tr>
<td>Port / Link Failures</td>
<td>Active PoA detects failure and signals failover over ICCP</td>
</tr>
<tr>
<td>Failover triggered on DHD</td>
<td>Failover triggered on DHD</td>
</tr>
<tr>
<td>Standby link brought up per LACP proc.</td>
<td>Standby link brought up per LACP proc.</td>
</tr>
<tr>
<td>Active PoA advertises “Standby” state on its PWs</td>
<td>Active PoA advertises “Standby” state on its PWs</td>
</tr>
<tr>
<td>Standby PoA advertises “Active” state on its PWs</td>
<td>Standby PoA advertises “Active” state on its PWs</td>
</tr>
</tbody>
</table>
E-LINE Availability Model
Active / Backup Access Node Redundancy (mLACP)

- Port / Link Failures (cont.)

- Local site access failure does not trigger LACP failover at remote site (i.e. control-plane separation between sites)

<table>
<thead>
<tr>
<th>Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
</tr>
<tr>
<td>FA-C</td>
</tr>
<tr>
<td>1A</td>
</tr>
<tr>
<td>1B</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>E</td>
</tr>
</tbody>
</table>

- VPWS
- VPWS Forwarding EoMPLS PW
- VPWS Non-Forwarding EoMPLS PW
E-LINE Availability Model
Active / Backup Access Node Redundancy (mLACP)

- PoA Node Failure
  - PoA node failures detected by BFD (session timeout) or IP route-watch (loss of routing adjacency)

- Events
  - 1: Initial state
  - $F_D$: Active PoA Node Failure
  - $1_A$: Standby PoA detects node failure (BFD timeout or IP route-watch)
  - $1_B$: Failover triggered on DHD
  - 2: Standby link brought up per LACP proc.
  - 3: Standby PoA advertises “Active” state on its PWs

VPWS
E-LINE Availability Model
Active / Backup Access Node Redundancy (mLACP)

- PoA Node Failure (cont.)

- No remote LACP switchover even if remote PoAs detect loss of PW before local LACP switchover is performed
E-LINE Availability Model
Active / Backup Access Node Redundancy (mLACP)

- Uplink Core Failure (PoA Core Isolation)

- Link and Node failures in the Core are handled by IP routing and/or MPLS FRR – do not trigger LACP switchover

Events

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>Initial state</td>
</tr>
<tr>
<td>$F_E$</td>
<td>Core Isolation</td>
</tr>
<tr>
<td>$1_A$</td>
<td>Active PoA detects core isolation and signals failover over ICCP</td>
</tr>
<tr>
<td>$1_B$</td>
<td>Active PoA signals failover to DHD (dynamic port priority changes / bruteforce)</td>
</tr>
<tr>
<td>2</td>
<td>Standby link brought up per LACP proc.</td>
</tr>
<tr>
<td>3</td>
<td>Standby PoA advertises “Active” state on its PWs</td>
</tr>
</tbody>
</table>
E-LINE Availability Model
Active / Backup Access Node Redundancy (mLACP)

- Uplink Core Failure (PoA Core Isolation) (cont.)

1. Active PoA detects core isolation and signals failover over ICCP
2. Active PoA signals failover to DHD (dynamic port priority changes / bruteforce)
3. Standby link brought up per LACP proc.
4. Standby PoA advertises “Active” state on its PWs

Events

<table>
<thead>
<tr>
<th></th>
<th>Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>Initial state</td>
</tr>
<tr>
<td>F_E</td>
<td>Core Isolation</td>
</tr>
<tr>
<td>1_A</td>
<td>Active PoA detects core isolation and signals failover over ICCP</td>
</tr>
<tr>
<td>1_B</td>
<td>Active PoA signals failover to DHD (dynamic port priority changes / bruteforce)</td>
</tr>
<tr>
<td>2</td>
<td>Standby link brought up per LACP proc.</td>
</tr>
<tr>
<td>3</td>
<td>Standby PoA advertises “Active” state on its PWs</td>
</tr>
<tr>
<td>E</td>
<td>End State</td>
</tr>
</tbody>
</table>

Diagram:
- LACP
- ICCP
- Forwarding EoMPLS PW
- Non-Forwarding EoMPLS PW

Uplink Core Failure (PoA Core Isolation) (cont.)
- Active PoA detects core isolation and signals failover over ICCP
- Active PoA signals failover to DHD (dynamic port priority changes / bruteforce)
- Standby link brought up per LACP proc.
- Standby PoA advertises “Active” state on its PWs

End State
E-LINE Availability Models
Ring Access Node Redundancy (MST)
E-LINE Availability Model
Ring Access Node Redundancy (MST)

- MST Ring Span Failure
  - MST isolation; not carried over MPLS cloud
  - MST Access Gateway (MST-AG) on Aggregation Nodes transmits statically configured BPDUs

### Events

<table>
<thead>
<tr>
<th>Events</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>Initial state</td>
</tr>
<tr>
<td>F_B</td>
<td>Ring Span failure</td>
</tr>
<tr>
<td>1</td>
<td>Access switch “A” detects link failure (loses root port), blocks failed port and sends root proposal to “B”</td>
</tr>
<tr>
<td>2_A</td>
<td>“B” selects bottom AGG as new root (unblocks port towards it)</td>
</tr>
<tr>
<td>2_B</td>
<td>“B” blocks port towards “A”</td>
</tr>
</tbody>
</table>
- Special VFI between AGG nodes to relay TCN BPDUs used to trigger MAC flushes after a Topology Change (TC)

Events:

3_{A-B} Proposal / Agreement handshake between “B” and “A”. “B” unblocks port towards “A”

3_{C} “B” flushes MAC table. Signals Topology Change (TC) to AGG device

4_{A} AGG flushes MAC table. Triggers LDP MAC add. withdrawal to VPLS peers

4_{B} AGG device propagates TCN over BPDU PW

5 AGG (local and remote) flush MAC tables

6 Top AGG generates TCN on local ring
E-LINE Availability Model
Ring Access Node Redundancy (MST)

- MST Ring Span Failure (cont.)
  - Each ring on unique TCN domain for control plane isolation
  - Two MST instances for VLAN load balancing over ring

Events

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Top AGG generates TCN on local ring</td>
</tr>
<tr>
<td>E</td>
<td>End State</td>
</tr>
</tbody>
</table>

82
E-LINE Availability Models

Ring Access Node Redundancy (G.8032)*

(*) – same principle applies to REP
E-LINE Availability Model
Ring Access Node Redundancy (G.8032)

- G.8032 Ring Span Failure

- G.8032 Open Ring without R-APS Virtual Channel, terminating on Aggregation Nodes
- VLAN load balancing using two ERP instances with RPL Owners on Aggregation Nodes.

Events

1. Initial state
2. Ring Span failure
3. Access switches “A” and “B” detect link failure. Send R-APS Signal Fail (SF) on the ring
4. Access nodes in the ring flush MAC tables and propagate R-APS SF
5. RPL owner AGG node receives R-APS and unblocks RPL owner port

- Forwarding EoMPLS PW
- Non-Forwarding EoMPLS PW
- R-APS Channel vlan
E-LINE Availability Model
Ring Access Node Redundancy (G.8032)

- G.8032 Ring Span Failure (cont.)

<table>
<thead>
<tr>
<th>Events</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>RPL owner AGG node receives R-APS SF and unblocks RPL owner port</td>
</tr>
<tr>
<td>4</td>
<td>AGG nodes flush MAC tables. Trigger LDP MAC add withdrawal to VPLS peers</td>
</tr>
<tr>
<td>5</td>
<td>Remote peers flush MAC tables</td>
</tr>
</tbody>
</table>

Forwarding EoMPLS PW
Non-Forwarding EoMPLS PW
R-APS Channel vlan
G.8032 Ring Span Failure (cont.)

- G.8032 Ring Access Node Redundancy (G.8032)

**Events**

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Remote peers flush MAC tables</td>
</tr>
<tr>
<td>E</td>
<td>End State</td>
</tr>
</tbody>
</table>

**Diagram Notes**

- Forwarding EoMPLS PW
- Non-Forwarding EoMPLS PW
- R-APS Channel vlan

**Nodes**

- G.8032
- RPL Owner
- Blocked port
IP / L3VPN Gateway Availability Models
mLACP + VRRP
IP / L3VPN Gateway Availability Model
Active / Backup Access Node Redundancy (mLACP)

- Port / Link Failures
  - Bridge Domain with associated SVI (BVI) for IP / L3VPN access.
  - VFI with a single PW to peer (Decoupled Mode).
  - VRRP Group on SVI (BVI) for L3 First Hop Redundancy.

### Events

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Initial state</td>
</tr>
<tr>
<td>F&lt;sub&gt;A-C&lt;/sub&gt;</td>
<td>Port / Link Failures</td>
</tr>
<tr>
<td>1&lt;sub&gt;A&lt;/sub&gt;</td>
<td>Active PoA detects failure and signals failover over ICCP</td>
</tr>
<tr>
<td>1&lt;sub&gt;B&lt;/sub&gt;</td>
<td>Failover triggered on DHD</td>
</tr>
<tr>
<td>2</td>
<td>Standby link brought up per LACP proc.</td>
</tr>
<tr>
<td>3</td>
<td>Standby PoA flushes MAC table.</td>
</tr>
<tr>
<td>4</td>
<td>Standby PoA triggers LDP MAC add. withdrawal to peer. Peer flushes its MAC table.</td>
</tr>
</tbody>
</table>
IP / L3VPN Gateway Availability Model
Active / Backup Access Node Redundancy (mLACP)

- Port / Link Failures (cont.)
  - Using VRRP Object Tracking on access links, it is possible to synchronize VRRP failover with mLACP failover (for optimal forwarding to core).

Events

- **I** Initial state
- **F<sub>A</sub>-C** Port / Link Failures
- **1<sub>A</sub>** Active PoA detects failure and signals failover over ICCP
- **1<sub>B</sub>** Failover triggered on DHD
- **2** Standby link brought up per LACP proc.
- **3** Standby PoA flushes MAC table.
- **4** Standby PoA triggers LDP MAC add. withdrawal to peer. Peer flushes its MAC table.
- **E** End State
IP / L3VPN Gateway Availability Model
Active / Backup Access Node Redundancy (mLACP)

Node Failure

Events

1. Initial state

FD. Active PoA Node Failure

1A. ICCP: Standby PoA detects node failure (BFD timeout or IP route-watch)

1B. VRRP: Standby PoA detects node failure after Hold Timer expiry (due to missed VRRP Advertisements)

2. Failover triggered on DHD

3. Standby link brought up per LACP proc.

4A. Standby PoA flushes its MAC table.

4B. Standby PoA assumes VRRP Master state.
IP / L3VPN Gateway Availability Model
Active / Backup Access Node Redundancy (mLACP)

- Node Failure (cont.)

Events

1. Initial state
2. Active PoA Node Failure
3. ICCP: Standby PoA detects node failure (BFD timeout or IP route-watch)
4. Standby link brought up per LACP proc.
5. Standby PoA flushes its MAC table.
6. Standby PoA assumes VRRP Master state.
7. End State
IP / L3VPN Gateway Availability Model
Active / Backup Access Node Redundancy (mLACP)

- Uplink Core Failure (PoA Core Isolation)

- VRRP Object Tracking must be enabled on the core-facing interfaces (same interfaces that are monitored by ICCP).

Events

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>Initial state</td>
<td></td>
</tr>
<tr>
<td>FE</td>
<td>Core Isolation</td>
<td></td>
</tr>
<tr>
<td>1A</td>
<td>ICCP: Active PoA detects core isolation and signals failover over ICCP</td>
<td></td>
</tr>
<tr>
<td>1B</td>
<td>VRRP: Active PoA decrements VRRP priority as a result of tracked object state Down</td>
<td></td>
</tr>
<tr>
<td>2A</td>
<td>Active PoA signals failover to DHD (dynamic port priority changes / bruteforce)</td>
<td></td>
</tr>
<tr>
<td>2B</td>
<td>Standby PoA assumes VRRP Master role.</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Standby link brought up per LACP proc.</td>
<td></td>
</tr>
</tbody>
</table>
IP / L3VPN Gateway Availability Model
Active / Backup Access Node Redundancy (mLACP)

- Uplink Core Failure (PoA Core Isolation)

- Note: mLACP Revertive operation must be used, since VRRP object tracking is revertive.

Events

4. Standby PoA flushes its MAC table.
5. Standby PoA triggers LDP MAC add. withdrawal to peer. Peer flushes its MAC table.
E. End State
Carrier Ethernet Portfolio
Cisco Platform Support

Access
Cisco ME3400 / ME3400E
Cisco ME3600X
Cisco MWR 2941
Cisco ME4924
Catalyst 4900
Cisco ASR 901

Pre-Aggregation / Aggregation
Small POP
Cisco ME3800X
Catalyst 4500
Cisco ASR 903

Aggregation Large POP
ASR 9000
Cisco 7600
Nexus 7K
Summary
Key Takeaways

- Various access redundancy mechanisms are available, which enable node as well as network multi-homing:
  - Multichassis LACP (mLACP)
  - mLACP Active/Active
  - G.8032
  - REP
  - MST Access Gateway

- Aggregation/core redundancy mechanisms operating at the pseudowire layer primarily protect against PE node failures:
  - One-way Pseudowire Redundancy
  - Two-way Pseudowire Redundancy

- Above mechanisms can interwork to provide comprehensive end-to-end resiliency solutions for E-Line, E-LAN and Layer 3 services
Summary

- Resiliency Fundamentals
- Access Resiliency Mechanisms
- Aggregation and Core Resiliency Mechanisms
- MAC Flushing Mechanisms
- Redundancy Solutions
References

- **Cisco IOS — L2VPN Pseudowire Redundancy**

- **Cisco IOS — Multichassis LACP Configuration Guide**

- **Cisco ME 3400 / 3400E — REP Configuration Guide**

- **Cisco 7600 — ES+ Layer 1 and Layer 2 features (covering MST / REP on EVC, Two-way PW redundancy, ICCP, mLACP, MST-AG)**

- **Cisco 7600 — H-VPLS N-PE Redundancy for QinQ and MPLS Access (covering MST on nPE, LDP MAC Address Withdrawal)**

- **Cisco 7600 — Link State Tracking**
References (Cont.)

- Cisco ASR 9000 — Configuring Link Bundles (covering Multichassis LACP)

- Cisco ASR 9000 — L2VPN and Ethernet Services Configuration Guide (covering MST, MST-AG, PW Redundancy, LDP MAC Address Withdrawal)

- Cisco ASR 9000 — Implementing Multipoint Layer 2 Services (covering G.8032)

- Cisco ASR 903 Aggregation Services Router Configuration Guide

- Cisco ASR 901 Aggregation Services Router Configuration Guide
## Acronyms—IP and MPLS

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC</td>
<td>Attachment Circuit</td>
</tr>
<tr>
<td>AS</td>
<td>Autonomous System</td>
</tr>
<tr>
<td>BFD</td>
<td>Bidirectional Failure Detection</td>
</tr>
<tr>
<td>CoS</td>
<td>Class of Service</td>
</tr>
<tr>
<td>ECMP</td>
<td>Equal Cost Multipath</td>
</tr>
<tr>
<td>EoMPLS</td>
<td>Ethernet over MPLS</td>
</tr>
<tr>
<td>FRR</td>
<td>Fast Re-Route</td>
</tr>
<tr>
<td>H-VPLS</td>
<td>Hierarchical VPLS</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>IGP</td>
<td>Interior Gateway Protocol</td>
</tr>
<tr>
<td>LDP</td>
<td>Label Distribution Protocol</td>
</tr>
<tr>
<td>LER</td>
<td>Label Edge Router</td>
</tr>
<tr>
<td>LFIB</td>
<td>Labeled Forwarding Information Base</td>
</tr>
<tr>
<td>LSM</td>
<td>Label Switched Multicast</td>
</tr>
<tr>
<td>LSP</td>
<td>Label Switched Path</td>
</tr>
<tr>
<td>LSR</td>
<td>Label Switching Router</td>
</tr>
<tr>
<td>MPLS</td>
<td>Multi-Protocol Label Switching</td>
</tr>
<tr>
<td>NLRI</td>
<td>Network Layer Reachability Information</td>
</tr>
<tr>
<td>PSN</td>
<td>Packet Switch Network</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PW</td>
<td>Pseudo-Wire</td>
</tr>
<tr>
<td>PWE3</td>
<td>Pseudo-Wire End-to-End Emulation</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>RD</td>
<td>Route Distinguisher</td>
</tr>
<tr>
<td>RIB</td>
<td>Routing Information Base</td>
</tr>
<tr>
<td>RR</td>
<td>Route Reflector</td>
</tr>
<tr>
<td>RSVP</td>
<td>Resource Reservation Protocol</td>
</tr>
<tr>
<td>RSVP-TE</td>
<td>RSVP based Traffic Engineering</td>
</tr>
<tr>
<td>RT</td>
<td>Route Target</td>
</tr>
<tr>
<td>TE</td>
<td>Traffic Engineering</td>
</tr>
<tr>
<td>tLDP</td>
<td>Targeted LDP</td>
</tr>
<tr>
<td>VC</td>
<td>Virtual Circuit</td>
</tr>
<tr>
<td>VCID</td>
<td>VC Identifier</td>
</tr>
<tr>
<td>VFI</td>
<td>Virtual Forwarding Instance</td>
</tr>
<tr>
<td>VPLS</td>
<td>Virtual Private LAN Service</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>VPWS</td>
<td>Virtual Private Wire Service</td>
</tr>
<tr>
<td>VRF</td>
<td>Virtual Route Forwarding Instance</td>
</tr>
<tr>
<td>VSI</td>
<td>Virtual Switching Instance</td>
</tr>
</tbody>
</table>
## Acronyms— Ethernet/Bridging

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL</td>
<td>Access Control List</td>
</tr>
<tr>
<td>BD</td>
<td>Bridge Domain</td>
</tr>
<tr>
<td>BPA</td>
<td>Blocked Port Advertisement (REP PDU)</td>
</tr>
<tr>
<td>BPDU</td>
<td>Bridge Protocol Data Unit</td>
</tr>
<tr>
<td>BRAS</td>
<td>Broadband Access Server</td>
</tr>
<tr>
<td>CE</td>
<td>Customer Equipment (Edge)</td>
</tr>
<tr>
<td>C-VLAN / CE-VLAN</td>
<td>Customer / CE VLAN</td>
</tr>
<tr>
<td>CoS</td>
<td>Class of Service</td>
</tr>
<tr>
<td>DHD</td>
<td>Dual Homed Device</td>
</tr>
<tr>
<td>DSLAM</td>
<td>DSL Access Modulator</td>
</tr>
<tr>
<td>E-LAN</td>
<td>Ethernet LAN service (multipoint)</td>
</tr>
<tr>
<td>E-Line</td>
<td>Ethernet Line service (point-to-point)</td>
</tr>
<tr>
<td>E-Tree</td>
<td>Ethernet Tree service (rooted multipoint)</td>
</tr>
<tr>
<td>EFP</td>
<td>Ethernet Flow Point</td>
</tr>
<tr>
<td>EPL</td>
<td>Ethernet Private Line</td>
</tr>
<tr>
<td>EP-LAN</td>
<td>Ethernet Private LAN</td>
</tr>
<tr>
<td>EVC</td>
<td>Ethernet Virtual Connection</td>
</tr>
<tr>
<td>EVPL</td>
<td>Ethernet Virtual Private Line</td>
</tr>
<tr>
<td>EVP-LAN</td>
<td>Ethernet Virtual Private LAN</td>
</tr>
<tr>
<td>ICCP</td>
<td>Inter-Chassis Communication Protocol</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>IPoETV</td>
<td>TV on IP over Ethernet</td>
</tr>
<tr>
<td>IPTV</td>
<td>Television over IP</td>
</tr>
<tr>
<td>L2GP</td>
<td>Layer 2 Gateway Ports</td>
</tr>
<tr>
<td>LACP</td>
<td>Link Aggregation Control Protocol</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>MEF</td>
<td>Metro Ethernet Forum</td>
</tr>
<tr>
<td>MEN</td>
<td>Metro Ethernet Network</td>
</tr>
<tr>
<td>MIRP</td>
<td>Multiple I-Tag Registration Protocol</td>
</tr>
<tr>
<td>mLACP</td>
<td>Multi-Chassis LACP</td>
</tr>
<tr>
<td>MRP</td>
<td>Multiple Registration Protocol</td>
</tr>
<tr>
<td>MST / MSTP</td>
<td>Multiple Instance STP</td>
</tr>
<tr>
<td>MSTG-AG</td>
<td>MST Access Gateway</td>
</tr>
</tbody>
</table>
# Acronyms— Ethernet/Bridging (Cont.)

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSTi</td>
<td>MST Instances</td>
</tr>
<tr>
<td>MTBF</td>
<td>Mean Time Between Failures</td>
</tr>
<tr>
<td>MTTR</td>
<td>Mean Time To Recover</td>
</tr>
<tr>
<td>MVRP</td>
<td>Multiple VLAN Registration Protocol</td>
</tr>
<tr>
<td>OAM</td>
<td>Operations, Administration and Maintenance</td>
</tr>
<tr>
<td>PE</td>
<td>Provider Edge device</td>
</tr>
<tr>
<td>PoA</td>
<td>Point of Attachment</td>
</tr>
<tr>
<td>Q-in-Q</td>
<td>VLAN tunneling using two 802.1Q tags</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>R-L2GP</td>
<td>Reverse L2GP</td>
</tr>
<tr>
<td>REP</td>
<td>Resilient Ethernet Protocol</td>
</tr>
<tr>
<td>REP-AG</td>
<td>REP Access Gateway</td>
</tr>
<tr>
<td>RG</td>
<td>Redundancy Group</td>
</tr>
<tr>
<td>SLA</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>SLS</td>
<td>Service Level Specification</td>
</tr>
<tr>
<td>STP</td>
<td>Spanning Tree Protocol</td>
</tr>
<tr>
<td>SVI</td>
<td>Switch Virtual Interface (interface vlan)</td>
</tr>
<tr>
<td>S-VLAN</td>
<td>Service VLAN (Provider VLAN)</td>
</tr>
<tr>
<td>TC</td>
<td>Topology Change</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCN</td>
<td>Topology Change Notification</td>
</tr>
<tr>
<td>UNI</td>
<td>User to Network Interface</td>
</tr>
<tr>
<td>VID</td>
<td>VLAN Identifier</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual LAN</td>
</tr>
<tr>
<td>VoD</td>
<td>Video on Demand</td>
</tr>
<tr>
<td>VoIP</td>
<td>Voice over IP</td>
</tr>
</tbody>
</table>
# Acronyms—Provider Backbone Bridging

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>B-BEB</td>
<td>B-Component BEB</td>
</tr>
<tr>
<td>BCB</td>
<td>Backbone Core Bridge</td>
</tr>
<tr>
<td>B-DA</td>
<td>Backbone Destination Address</td>
</tr>
<tr>
<td>BEB</td>
<td>Backbone Edge Bridge</td>
</tr>
<tr>
<td>B-MAC</td>
<td>Backbone MAC Address</td>
</tr>
<tr>
<td>B-SA</td>
<td>Backbone Source Address</td>
</tr>
<tr>
<td>B-Tag</td>
<td>B-VLAN Tag</td>
</tr>
<tr>
<td>B-VLAN</td>
<td>Backbone VLAN</td>
</tr>
<tr>
<td>C-DA</td>
<td>Customer Destination Address</td>
</tr>
<tr>
<td>CE</td>
<td>Customer Equipment (Edge)</td>
</tr>
<tr>
<td>C-MAC</td>
<td>Customer MAC Address</td>
</tr>
<tr>
<td>C-SA</td>
<td>Customer Source Address</td>
</tr>
<tr>
<td>80</td>
<td>C-VLAN Tag</td>
</tr>
<tr>
<td>C-VLAN/CE-VLAN</td>
<td>Customer / CE VLAN</td>
</tr>
<tr>
<td>DA</td>
<td>Destination MAC Address</td>
</tr>
<tr>
<td>FCS</td>
<td>Frame Check Sequence</td>
</tr>
<tr>
<td>IB-BEB</td>
<td>Combined I-Component &amp; B-Component BEB</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>I-BEB</td>
<td>I-Component BEB</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>I-SID</td>
<td>Instance Service Identifier</td>
</tr>
<tr>
<td>I-Tag</td>
<td>I-SID Tag</td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control</td>
</tr>
<tr>
<td>N-PE</td>
<td>Network-facing Provider Edge device</td>
</tr>
<tr>
<td>PB</td>
<td>Provider Bridge</td>
</tr>
<tr>
<td>PBB</td>
<td>Provider Backbone Bridge / Bridging</td>
</tr>
<tr>
<td>PBBN</td>
<td>Provider Backbone Bridging Network</td>
</tr>
<tr>
<td>PBN</td>
<td>Provider Bridging Network</td>
</tr>
<tr>
<td>PE</td>
<td>Provider Edge device</td>
</tr>
<tr>
<td>Q-in-Q</td>
<td>VLAN tunneling using two 802.1Q tags</td>
</tr>
<tr>
<td>SA</td>
<td>Source MAC Address</td>
</tr>
<tr>
<td>S-Tag</td>
<td>S-VLAN Tag</td>
</tr>
<tr>
<td>S-VLAN</td>
<td>Service VLAN (Provider VLAN)</td>
</tr>
<tr>
<td>UNI</td>
<td>User to Network Interface</td>
</tr>
<tr>
<td>U-PE</td>
<td>User-facing Provider Edge device</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual LAN</td>
</tr>
</tbody>
</table>

**Acronyms**—Provider Backbone Bridging
Complete Your Online Session Evaluation

- Give us your feedback and you could win fabulous prizes. Winners announced daily.
- Receive 20 Passport points for each session evaluation you complete.
- Complete your session evaluation online now (open a browser through our wireless network to access our portal) or visit one of the Internet stations throughout the Convention Center.

Don’t forget to activate your Cisco Live Virtual account for access to all session material, communities, and on-demand and live activities throughout the year. Activate your account at the Cisco booth in the World of Solutions or visit www.ciscolive.com.
Final Thoughts

- Get hands-on experience with the Walk-in Labs located in World of Solutions, booth 1042
- Come see demos of many key solutions and products in the main Cisco booth 2924
- Visit [www.ciscoLive365.com](http://www.ciscoLive365.com) after the event for updated PDFs, on-demand session videos, networking, and more!
- Follow Cisco Live! using social media:
  - Facebook: [https://www.facebook.com/ciscoliveus](https://www.facebook.com/ciscoliveus)
  - Twitter: [https://twitter.com/#!/CiscoLive](https://twitter.com/#!/CiscoLive)
  - LinkedIn Group: [http://linkd.in/CiscoLI](http://linkd.in/CiscoLI)
BUILT FOR THE HUMAN NETWORK