

Using G.8032 Ethernet Stitching in a Mixed Environment

Use Cases

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

The document may contain information relating to Juniper Networks' development plans and plans for future products, features or enhancements ("SOPD"). SOPD information is subject to change at any time, without notice. Except as may be set forth in definitive agreements for the potential transaction, Juniper Networks provides no assurances, and assumes no responsibility, that such future products, features or enhancements will be introduced.

The information in this document is current as of the date on the title page.

Copyright © 2017, Juniper Networks, Inc. All rights reserved.

Contents

Overview	1
Using G.8032 in a Closed Ethernet Access Ring Use Case	2
Configuring Ethernet Access Node for G.8032 Ring Protection	2
Using G.8032 for Ethernet to VPLS Stitching Use Case.....	6
Configuring G.8032 with Ethernet to VPLS Stitching	7
Configuring Ethernet Access Node for G.8032 Protection	8
Configuring AGG Router for G.8032 Protection.....	8
Appendix A – Variables’ Definitions.....	14

Overview

You can use the IEEE G.8032 protocol [also known as Ethernet ring protection (ERP)] for link and node failure protection, as well as, for Layer 2 loop prevention in the Carrier Ethernet (CE) segment based on IEEE 802.3 Ethernet switching. Contrary to different flavors of spanning tree, IEEE G.8032 provides a much faster restoration—often compliant with 50 ms of restoration time. Juniper Networks recommends using this as the primary protection mechanism for E-LAN and ELINE/E-ACCESS services when end-points belong to the IEEE 802.3 Ethernet access segment.

Juniper Networks' MX Series and ACX Series platforms support the following two versions of ERP protocols:

- G.8032 v1
- G.8032 v2

This document shows how you can use ERP in a pure Ethernet bridging environment and in mixed topologies where an IEEE G.802.3 Ethernet segment is stitched to the VPLS segment in the aggregation part of the network (shown in Figure 1).

This document describes the following two use cases (as shown in Figure 1):

- Closed Ethernet Access Ring
- Ethernet to VPLS Stitching with an open ERP ring

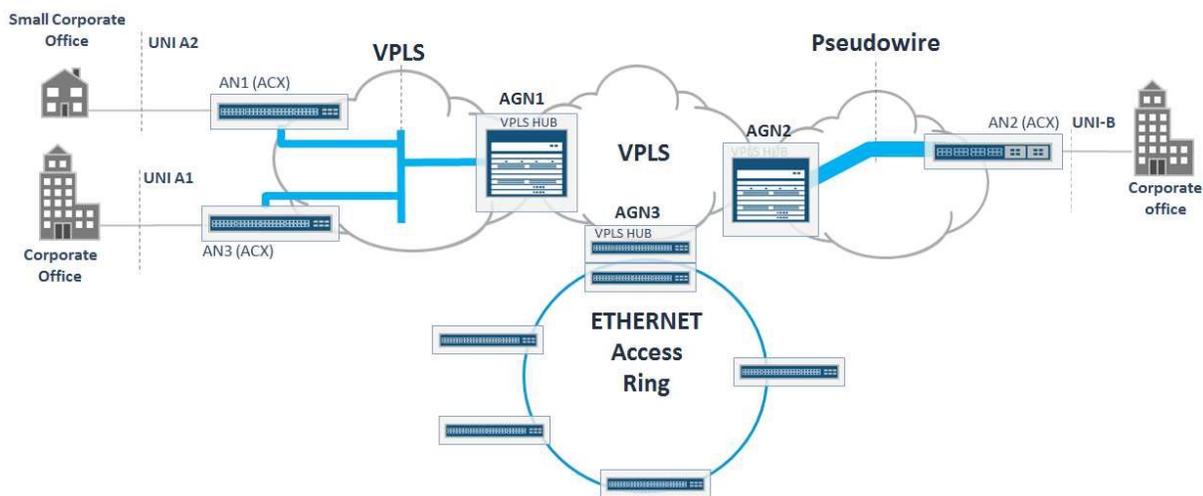


Figure 1 – Stitching Different Types of Ethernet Segments with VPLS

Using G.8032 in a Closed Ethernet Access Ring Use Case

The simplest case for setting up G.8032 protection occurs when the access segment consists of Ethernet nodes only (which could contain ACX Series or MX Series routers) arranged in single physical ring (shown in Figure 2).

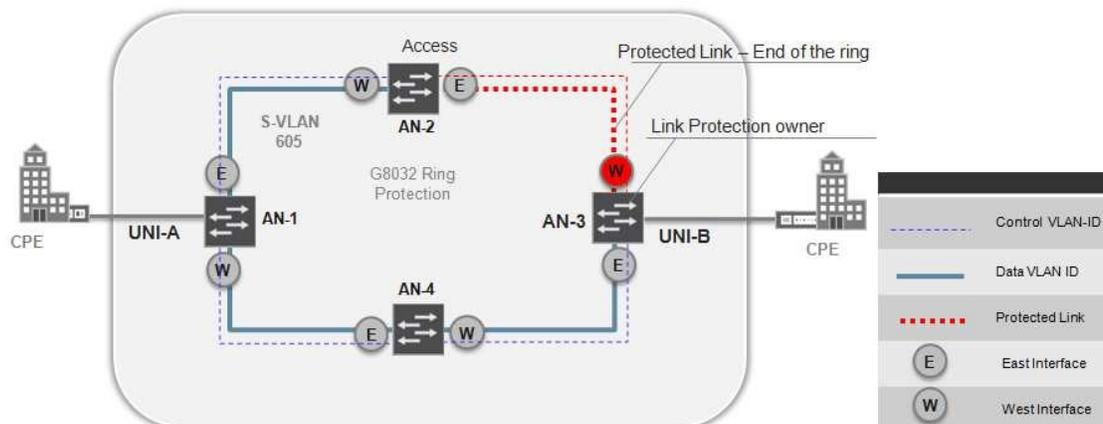


Figure 2 – G.8032 in Ethernet Access Ring Use Case

In this use case, one of the access nodes is configured as a G.8032 controller and protection link owner. It controls the status of the ring by exchanging G.8032 messages with other members of the ring, and in normal situations, it keeps the protected link in blocked status mode preventing Layer 2 loops in the ring. As soon as link failure occurs in the ring, a G.8032 protection group member (which detects the link failure) sends a G.8032 notification to the protection group controller. The protection ring controller changes the status of the protected link to unblocked mode thus restoring the connectivity within the ring. In case of failure detection, the G.8032 detection enforces MAC addresses to flash on each member of the ring that provides faster service restoration.

You can configure multiple protection groups in one physical ring. Each group can have different nodes assigned as the group controller, and different links configured as the protected link. This approach enables load balancing in the Ethernet ring. Each ring has a dedicated VLAN to exchange G.8032 control traffic that protects a group of VLANs that carries the actual data traffic. Figure 2 depicts the simplest case with a single physical ring. With G.8032 v2, topologies that are more sophisticated can be supported, however they are currently outside the scope of this document.

Configuring Ethernet Access Node for G.8032 Ring Protection

To set up ERP in the ring, follow these steps:

1. Configure AN's core facing interface attributes for data/service S-VLANs.
2. Configure AN's west/east core facing interfaces.
3. Configure AN bridge domain for data/service S-VLANs.
4. Configure AN's core facing interface with G.8032 control VLAN.
5. Configure AN bridge domain G.8032 control VLAN.
6. Configure AN-1, AN-2, and AN-4 G.8032 protection groups.
7. Configure AN-3 G.8032 protection group with AN-3 as protection link owner.

The following configuration template provides an example of how you can enable G.8032 in an Ethernet ring with AN-1, AN-2, and AN-4 as the non-protector nodes, and AN-3 as a G.8032 protector.

Notes:

The configuration templates are based on G.8032 CLI syntax supported on the ACX Series platform. In a mixed environment with an ACX5000 router, ACX Series, or MX Series platform, you should note which version of G.8032 is enabled. By default, version 2 is enabled on the following Junos OS Releases for the following platforms:

- Junos OS Release 14.2 R1 and later, on the MX Series routers
- Junos OS Release 15.1X54-D20 and later, on ACX5000 routers
- Junos OS Release 17.2R1 and later, on ACX Series routers

To verify the version of the G.8032 protocol used, enter the `show protection-group ethernet-ring configuration operational` commands.

If multiple ERP rings are configured on a single physical ring of ACX5000 routers, then you must configure the `ring-id` for each ERP ring. If version 2 is used, then you must configure the same `ring-id` on other routers in the ring.

CLI Syntax—Step 1: Configure AN's core facing interface attributes for data/service S-VLANs.

```
groups {
  GR-CSR-CORE-INTF {
    interfaces {
      "<[g|x]e-*>" {
        traps;
        mtu <MTU-LAN>;
        hold-time up 5000 down 0;
        optics-options {
          alarm low-light-alarm {
            link-down;
          }
          warning low-light-warning {
            syslog;
          }
        }
      }
    }
  }
}
```

CLI Syntax—Step 2: Configure AN's west/east core facing interfaces.

```
interfaces {
  <AN:ge|x|e-East> {
    apply-groups GR-CSR-CORE-INTF;
    description "connected to West NNI of the next Node in the Ring";
    vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit <EVC-UNIT-ID> {
      encapsulation vlan-bridge;
      vlan-id <EVC-S-VLAN>;
    }
  }
}
interfaces {
  <AN:ge|x|e-West> {
    /* Core Interface */
    apply-groups GR-CSR-CORE-INTF;
    description "connected to East NNI of the next Node in the Ring";
    vlan-tagging;
```

```

encapsulation flexible-ethernet-services;
unit <EVC-UNIT-ID> {
    encapsulation vlan-bridge;
    vlan-id <EVC-S-VLAN>;
}
}

```

CLI Syntax—Step 3: Configure AN bridge domain for data/service S-VLANs.

```

bridge-domains {
    CE-EVC-<EVC-ID> {
        interface <AN:ge|xe-East>.<EVC-UNIT-ID>;
        interface <AN:ge|xe-West>.<EVC-UNIT-ID>;
        interface <ge|xe-UNI-A>.<EVC-UNIT-ID>;
    }
}

```

For every S-VLAN in the access segment that requires protection, use the configuration CLI snippets in Steps 1 through 3.

CLI Syntax—Step 4: Configure AN's core facing interface with G.8032 control VLAN.

```

interfaces {
    <AN:ge|xe-East> {
        apply-groups GR-CSR-CORE-INTF;
        description "connected to West NNI of the next Node in the Ring";
        vlan-tagging;
        encapsulation flexible-ethernet-services;
        unit <G.8032-UNIT-ID> {
            encapsulation vlan-bridge;
            vlan-id <G.8032-VLAN>;
        }
    }
}
interfaces {
    <AN:ge|xe-West> {
        /* Core Interface */
        apply-groups GR-CSR-CORE-INTF;
        description "connected to East NNI of the next Node in the Ring";
        vlan-tagging;
        encapsulation flexible-ethernet-services;
        unit <G.8032-UNIT-ID> {
            encapsulation vlan-bridge;
            vlan-id <G.8032-VLAN>;
        }
    }
}

```

CLI Syntax—Step 5: Configure AN bridge domain G.8032 control VLAN.

```

bridge-domains {
    CE-G.8032-<G.8032-VLAN> {
        interface <AN:ge|xe-East>.<G.8032-UNIT-ID>;
        interface <AN:ge|xe-West>.<G.8032-UNIT-ID>;
    }
}

```

CLI Syntax—Step 6: Configure AN-1, AN-2, and AN-4 G.8032 protection groups.

```

protocols {
  protection-group {
    ethernet-ring G8032-GROUP-<G.8032-VLAN> {
      node-id <G.8032-AN-1-ID>;
      east-interface {
        control-channel {
          <AN:ge|xe-East>.<G.8032-UNIT-ID>;
        }
      }
      west-interface {
        control-channel {
          <AN:ge|xe-East>.<G.8032-UNIT-ID>;
        }
      }
      data-channel {
        vlan [ <EVC-S-VLAN> ]; /* List all data VLANs which require protection
*/
      }
    }
  }
}

```

CLI Syntax—Step 7: Configure AN-3 G.8032 protection group with AN-3 as protection link owner.

```

protocols {
  protection-group {
    ethernet-ring G8032-GROUP-<G.8032-VLAN> {
      node-id <G.8032-AN-1-ID>;
      ring-protection-link-owner;
      east-interface {
        control-channel {
          <AN:ge|xe-East>.<G.8032-UNIT-ID>;
        }
      }
      west-interface {
        control-channel {
          <AN:ge|xe-East>.<G.8032-UNIT-ID>;
        }
        ring-protection-link-end;
      }
      data-channel {
        vlan [ <EVC-S-VLAN> ]; /* List all data VLANs which require protection
*/
      }
    }
  }
}

```

As shown in the previous example, ERP configuration touches core-facing interfaces only. You can configure a user network interface (UNI) for port based or VLAN-based service. The following CLI snippet shows UNI interface configuration for port based EP-Line and EP-LAN services on an ACX Series router:

CLI Syntax—AN-1. Configure UNI and EVC of the Ethernet AN for EP-LINE service.

```

interfaces {
  <ge|xe-UNI-A> {
    apply-groups GR-ACCESS-INTF-ETH;
    description "CE2.0 UNI for the EP Service";
    encapsulation ethernet-bridge;
    unit 0 {
      input-vlan-map {
        push;
        vlan-id <EVC-S-VLAN>;
      }
      output-vlan-map pop;
    }
  }
}

```

Using G.8032 for Ethernet to VPLS Stitching Use Case

Figure 3 depicts a high-level service and network architecture of the use case when Ethernet to VPLS stitching is required.

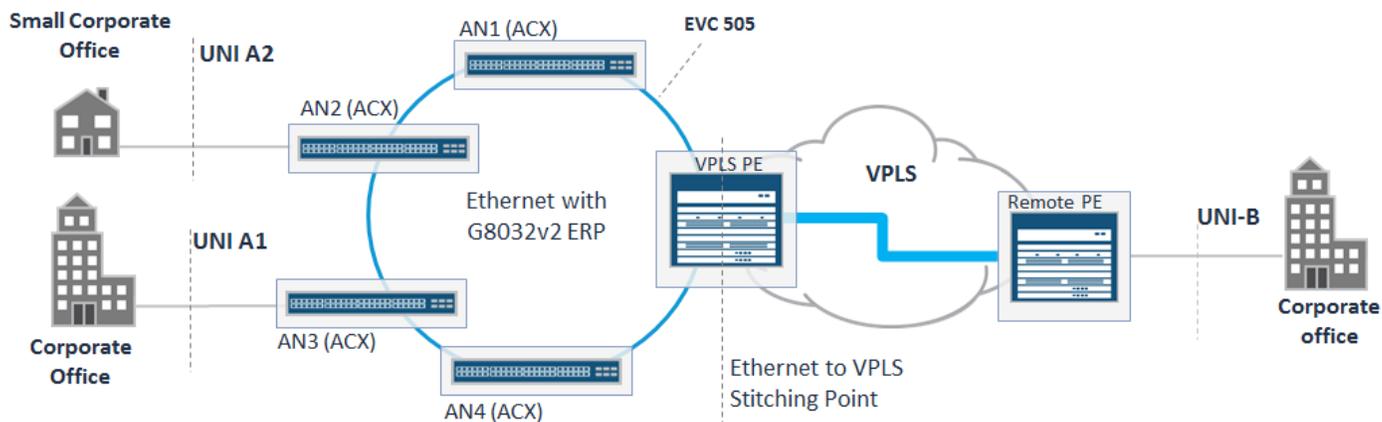


Figure 3 – Ethernet to VPLS Stitching Architecture Reference

Metro Ethernet Virtual connection (EVC) is provided between customer sites connected to the Ethernet access ring—UNI A1 and UNI A2 on the left side of the diagram; and customer site connected to the remote PE router—UNI B on the right side of the diagram. As in the previous example, ERP is used in the Ethernet ring for fast restoration and avoiding Layer 2 loops. To achieve the required functionality, you should enable G.8032 on each access switch—AN1 through AN4—as well as including the CE facing interfaces of the VPLS PE router.

On MX Series routers, you can enable the VPLS protocol for routing instance type VPLS, or instance type Virtual-Switch. G.8032 protection is supported on interfaces that use the vlan-bridge encapsulation; however, it is not supported on interfaces that use the vlan-vpls encapsulation type. To configure both protocols, G.8032 and VPLS simultaneously, you should select a virtual switch instance at the VPLS PE to enable stitching between access and aggregation segments. For a complete description of how to enable an end-to-end EVC with virtual switch instance on an MX Series router in a Metro Ethernet network, refer to the Metro Design Guide [1].

To identify end-to-end EVC and differentiate between multiple EVCs, you use the same S-VLAN across all metro segments—Ethernet and VPLS.

Configuring G.8032 with Ethernet to VPLS Stitching

In this use case, we assume that the Ethernet access half-ring is physically terminated on a pair of pre-aggregated routers—AG1.1 and AG1.2. The following are possible network architectures that can be used for different types of Metro services:

- E-LAN and E-TREE services—Use a combination of Ethernet ring and VPLS (see Figure 4).
- E-LINE or E-ACCESS services—Use a combination of Ethernet ring and redundant pair of the pseudowires established between AG1.1/AG1.2 routers, and remote MPLS access node, respectively (see Figure 5).

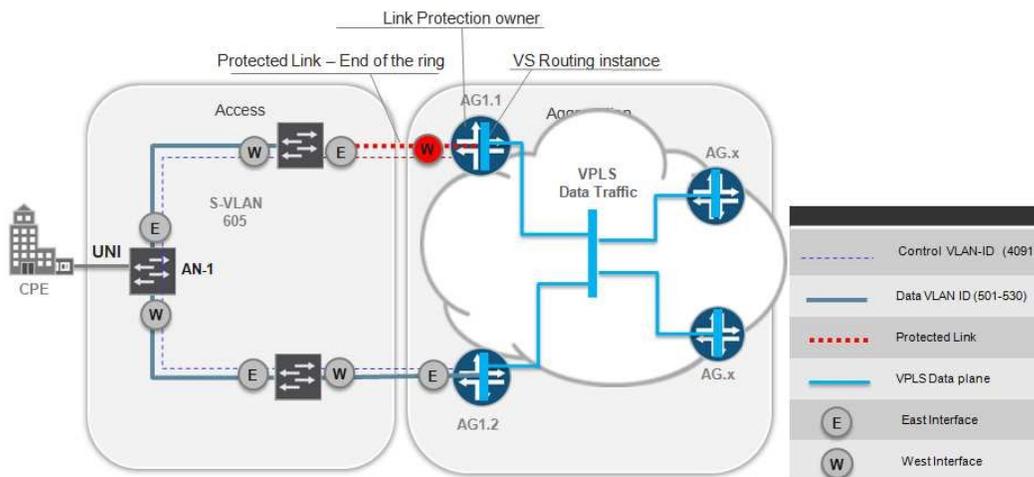


Figure 4 – G.8032 with Ethernet to VPLS Stitching: E-LAN or E-TREE

In the Ethernet ring, its S-VLAN tag identifies each EVC. S-VLANs are terminated on AG1.1/AG1.2 into dedicated, isolated bridge domains within a single VSI.

This topology may cause one of two possible Layer 2 loops to form:

- A Layer 2 loop comprised of access switches in the half ring AG router.
- A Layer 2 loop formed between multiple half rings that carry same S-VLAN, and are connected to the same pair of the pre-aggregated routers.
(**Note:** This loop is not depicted in Figure 4, but you should consider this possibility when planning your access and aggregation network.)

You can avoid both types of Layer 2 loops by enabling G.8032 in the Ethernet access segment with the AG1.1/AG1.2 routers chosen as G.8032 protectors. In a multi-ring topology where the same pair of AG routers aggregates more than one Ethernet ring, you should configure each with its own G.8032 control channel. G.8032v1 requires that you reserve a dedicated VLAN tag for each control channel (two VLAN tags, if you are load balancing) per access ring.

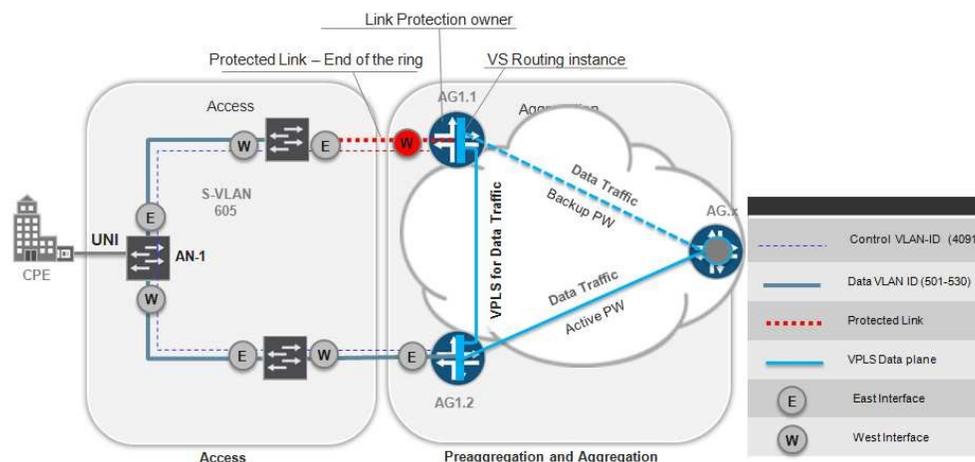


Figure 5 – G.8032 with Ethernet to VPLS Stitching: E-Line or E-Access

Note: For G.8032 version 2, you can use the same VLAN tag for control channels in different physical rings by assigning a different ring-id to each ERP ring.

To enable G.8032 on AN nodes, use the configuration for non-protector nodes as described in the previous use case ([Using G.8032 in a Closed Ethernet Access Ring Use Case](#)).

A closed Layer 2 loop exists only for data traffic but not for G.8032 control channel. By design, we assume that there is no direct Ethernet link between the AG1.1 and AG1.2 routers. As a result, the east interface on the AG1.1 and the west-interface on the AG1.2 routers, are configured as “no interfaces” under the G.8032 configuration hierarchy level.

The AG1.1 router acts as a protected-link owner, so that in its normal state without failure, the west Ethernet link is blocked. For the E-Line or E-Access deployment scenarios (shown in Figure 5), to enable optimal traffic flow in normal situations, use the AG1.2 router to terminate an active pseudowire, and use the AG1.1 router as the backup pseudowire.

The templates for configuring G.8032 on the AG routers are provided below.

Configuring Ethernet Access Node for G.8032 Protection

To configure the Ethernet access node for G.8032 protection, follow the steps that were previously described in the [Configuring Ethernet Access Node for G.8032 Ring Protection](#) section.

Configuring AGG Router for G.8032 Protection

To configure the AGG router for G.8032 protection, follow these steps:

1. Configure the AG1.1/AG1.2 attributes for the CE facing interface (NNI).
2. Configure the AG1.1 CE facing interface (NNI) of the AGG router for data/service VLAN.
3. Configure the AG1.1 CE facing interface (NNI) for G.8032 control channel VLAN.
4. Configure the AG1.2 CE facing interface (NNI) of the AGG router for data/service VLAN.
5. Configure the AG1.2 CE facing interface (NNI) for G.8032 control channel VLAN.
6. Configure the AG1.1 bridge domain for the G.8032 control VLANs.
7. Configure the AG1.2 bridge domain for the G.8032 control VLANs.

8. Configure the AG1.1 as the G.8032 protection owner node.
9. Configure the AG1.2 as the G.8032 node.
10. Configure the AG1.1/AG1.2 attributes of the VPLS protocol.
11. Configure the AG1.1/AG1.2 dynamic-profile for VPLS pseudowires.
12. Configure the AG1.1 VSI with VPLS for EVC stitching.
13. Configure the AG1.2 VSI with VPLS for EVC stitching.

CLI Syntax—Step 2: Configure the AG1.1/AG1.2 attributes for the CE facing interface (NNI).

```
groups {
  GR-AGG-ETH-INTF {
    interfaces {
      "<[g|x]e-*>" {
        traps;
        mtu <MTU-LAN>;
        hold-time up 5000 down 0;
        optics-options {
          alarm low-light-alarm {
            link-down;
          }
          warning low-light-warning {
            syslog;
          }
        }
      }
    }
  }
}
```

CLI Syntax—Step 2: Configure the AG1.1 CE facing interface (NNI) of the AGG router for data/service VLAN .

```
interfaces {
  <ge/xe-AG1.1-NNI-West> {
    apply-groups GR-AGG-ETH-INTF;
    description " AG1.1 NNI connected to East NNI of the AN in the Ethernet Ring";
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit <AG1.1:EVC-UNIT-ID> {
      encapsulation vlan-bridge;
      family bridge {
        interface-mode trunk;
        vlan-id-list <EVC-S-VLAN>;
      }
    }
  }
}
```

CLI Syntax—Step 3: Configure the AG1.1 CE facing interface (NNI) for C.8032 control channel VLAN .

```
interfaces {
  <ge/xe-AG1.1-NNI-West> {
    apply-groups GR-AGG-ETH-INTF;
    description " AG1.1 NNI connected to East NNI of the AN in the Ethernet Ring";
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit <AG1.1:G.8032-UNIT-ID> {
      encapsulation vlan-bridge;
      vlan-id <G.8032-VLAN>;
    }
  }
}
```

CLI Syntax—Step 4: Configure the AG1.2 CE facing interface (NNI) of the AGG router for data/service VLAN .

```

interfaces {
  <ge|xe-AG1.2-NNI-East> {
    apply-groups GR-AGG-ETH-INTF;
    description " AG1.2 NNI connected to West NNI of the AN in the Ethernet Ring";
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit <AG1.2:G.8032-UNIT-ID> {
      encapsulation vlan-bridge;
      vlan-id <G.8032-VLAN>;
    }
  }
}

```

CLI Syntax—Step 5: Configure the AG1.2 CE facing interface (NNI) for C.8032 control channel VLAN .

```

interfaces {
  <ge|xe-AG1.2-NNI-West> {
    apply-groups GR-AGG-ETH-INTF;
    description " AG1.2 NNI connected to West NNI of the AN in the Ethernet Ring";
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit <AG1.2:G.8032-UNIT-ID>{
      encapsulation vlan-bridge;
      vlan-id <G.8032-VLAN>
    }
  }
}

```

CLI Syntax—Step 6: Configure AG1.1 bridge domain for the G.8032 control VLANs.

```

bridge-domains {
  CE-G.8032-<G.8032-VLAN> {
    interface <ge|xe-AG1.1-West>.<AG1.1:G.8032-UNIT-ID>;
  }
}

```

CLI Syntax—Step 7: Configure AG1.2 bridge domain for the G.8032 control VLANs.

```

bridge-domains {
  CE-G.8032-<G.8032-VLAN> {
    interface <ge|xe-AG1.2-East>.<AG1.2:G.8032-UNIT-ID>;
  }
}

```

CLI Syntax—Step 8: Configure AG1.1 as the G.8032 protection owner node.

```

protocols {
  protection-group {
    ethernet-ring G8032-GROUP-<G.8032-VLAN> {
      node-id <AG1.1-G.8032-NODE-ID>;
      ring-protection-link-owner;
      east-interface {
        interface-none;
      }
      west-interface {
        control-channel {
          <ge/xr-AG1.2-West>.<AG1.1:G.8032-UNIT-ID>;
        }
        ring-protection-link-end;
      }
      data-channel {
        vlan [ <EVC-S-VLAN> ];
      }
    }
  }
}

```

CLI Syntax—Step 9: Configure AG1.2 as the G.8032 node.

```

protocols {
  protection-group {
    ethernet-ring G8032-GROUP-<G.8032-VLAN> {
      node-id <AG1.2-G.8032-NODE-ID>;
      east-interface {
        control-channel {
          <ge/xr-AG1.2-East>.<AG1.2:G.8032-UNIT-ID>;
        }
      }
      west-interface {
        interface-none;
      }
      data-channel {
        vlan [ <EVC-S-VLAN> ];
      }
    }
  }
}

```

List all S-VLAN tags that require protection within the given protection group under the “data channel” statement for both AG routers.

CLI Syntax—Step 30: Configure the AG1.1/AG1.2 attributes of the VPLS protocol.

```

groups {
  GR-VPLS {
    routing-instances {
      <[*]> {
        protocols {
          vpls {
            mtu <MTU-LAN-VPLS>;
            mesh-group <*> {
              neighbor <*> {
                encapsulation-type ethernet-vlan;
                no-vlan-id-validate;
              }
            }
          }
        }
      }
    }
  }
}

```

CLI Syntax—Step 41: Configure the AG1.1/AG1.2 dynamic-profile for VPLS pseudowires.

```

dynamic-profiles {
  CE20-<EVC-ID>-PROFILE {
    interfaces {
      "$junos-interface-ifd-name" {
        unit "$junos-underlying-interface-unit" {
          family-bridge {
            interface-mode trunk;
            vlan-id-list-<EVC-S-VLAN>;
          }
        }
      }
    }
  }
}

```

CLI Syntax—Step 52: Configure the AG1.1 VSI with VPLS for EVC stitching.

```

routing-instance {
  CE20-VSI {
    apply-groups GR-VPLS;
    instance-type virtual-switch;
    interface <ge/xr-AG1.1-NNI-West>.<AG1.1:EVC-UNIT-ID>;
    protocols {
      vpls {
        no-tunnel-services;
        mac-flush;
        mesh-group <EVC-ID>-PW {
          associate-profile CE20-<EVC-ID>-PROFILE;
          vpls-id <AN-2:VC-ID-ACTIVE>; <----- vpls-id or active vc-id from the AG-x
          neighbor <AN-2:lo0.0-ip-address>;
          neighbor <AG1.2:lo0.0-ip-address>;
        }
      }
    }
    bridge-domains {
      CE20-ELINE-ANY {
        vlan-id-list <EVC-S-VLAN>;
      }
    }
  }
}

```

CLI Syntax—Step 63: Configure the AG1.2 VSI with VPLS for EVC stitching.

```

routing-instance {
  CE20-VSI {
    apply-groups GR-VPLS;
    instance-type virtual-switch;
    interface <ge/xe-AG1.2-NNI-East>.<AG1.2:EVC-UNIT-ID>;
    protocols {
      vpls {
        no-tunnel-services;
        mac-flush;
        mesh-group <EVC-ID>-PW {
          associate-profile CE20-<EVC-ID>-PROFILE;
          vpls-id <AG-x:VC-ID-BACKUP>; <----- vpls-id or backup vc-id from the AG-x
          neighbor <AG-x:lo0.0-ip-address>;
          neighbor <AG1.1:lo0.0-ip-address>;
        }
      }
    }
    bridge-domains {
      CE20-ELINE-ANY {
        vlan-id-list <EVC-S-VLAN>;
      }
    }
  }
}

```

Appendix A – Variables' Definitions

The Carrier Ethernet Services (CES) configuration templates described in this document use variables to reference objects within the router configurations, such as: interfaces, name of routing instances, and service- or network-specific attributes. When configuring your actual network, you should substitute real values for the variables.

Table 2 lists the variables defined in the CES configuration templates.

Table 2 – Variables, Descriptions, and Ranges/Examples

Variable	Description	Value Range/Example
<EVC-ID>	Unique EVC identifier	1 through 65534
<ge xe-UNI-A>	Name of the physical UNI-A interface of AN	Example: ge-0/0/1
<ge xe-UNI-B>	Name of the physical UNI-B interface of AN	Example: ge-0/0/1
<ge xe-ENNI-B>	Name of the physical ENNI-B interface of AN	Example: ge-0/0/1
<AN:ge xe-East>	Name of the physical interface of AN facing to the core in East direction	Example: ge-0/0/1
<AN:ge xe-West>	Name of the physical interface of AN facing to the core in West direction	Example: ge-0/0/1
<EVC-UNIT-ID>	Logical unit identifier of the interface used for EVC on AN	0 through 1073741823
lt-<Fn>/<Pn>/<Nn>	Logical tunnel name on AGG router	lt-1/0/10
<Fn>	FPC slot number	Value in the range: [0-11] (depends on router model)
<Pn>	PIC slot number	0 or 1 for MX Series
<Nn>	lt-interface port number	0 through 65534
<lt-UNIT-ID>	Logical unit identifier of the lt-interface on AGG router	0 through 1073741823
<AG1.1:G.8032-UNIT-ID>	Interface logical unit used for G.8032 to control VLAN traffic at the AG1.1 router	0 through 1073741823
<AG1.2:G.8032-UNIT-ID>	Interface logical unit used for G.8032 to control VLAN traffic at the AG1.2 router	0 through 1073741823
<MTU-LAN>	MTU on interface with VLAN-tagging or flexible VLAN tagging	1522 through 9192
<MTU-ETH>	MTU on interface with no VLAN tagging	1518 through 9188
<MTU-LAN-VPLS>	MTU used by LDP signaled PW for Ethernet VLAN encapsulation	1500 through 9192
<MTU-ETH-VPLS>	MTU used by LDP signaled PW for Ethernet encapsulation	1504 through 9192
<EVC-S-VLAN>	S-VLAN tag of the EVC in the Ethernet access segment	1 through 4094
<OVC-S-VLAN>	S-VLAN tag of the OVC at the ENNI interface of the E-ACCESS service	1 through 4094
<EVC-S-VLAN-NORMAL>	S-VLAN tag of the EVC service in the Ethernet access segment used for S-VLAN normalization	1 through 4094

Variable	Description	Value Range/Example
<EVC-S-VLAN-1>	S-VLAN tag of the EVC service in the Ethernet access segment that requires normalization	1 through 4094
<G.8032-VLAN>	G.8032 control channel VLAN	1 through 4094
<C-VLANs>	List of customer VLAN tags of the EVP Service at UNI interface	A separate C-VLAN tag in the list should be in the range: 1 through 4094
<NATIVE-C-VLAN>	Native C-VLAN tag for the UNI-A for the C-VLAN translation scenario	1 through 4094
<LOCAL-C-VLAN>	Local C-VLAN tag for the UNI-B for the C-VLAN translation scenario	1 through 4094
<VC-ID-ACTIVE>	Virtual circuit identifier used for active LDP signaled PW on AN	0 through 65534
<VC-ID-BACKUP>	Virtual circuit identifier used for backup LDP signaled PW on AN	1 through 4294967295
<AN:VC-ID-ACTIVE>	Virtual circuit identifier used for active LDP signaled PW on Agg router in direction of the AN	1 through 4294967295
<AN:VC-ID-BACKUP>	Virtual circuit identifier used for backup LDP signaled PW on Agg router in the direction of the AN	1 through 4294967295
<ge xe-AG1.1-NNI-West>	Interface Name of the AG1.1 router interface facing the Ethernet ring in the west direction	Example: ge-0/0/1
<ge xe-AG1.2-NNI-East>	Interface Name of the AG1.2 router interface facing the Ethernet ring in the east direction	Example: ge-0/0/1
<ge xe-AG2.1-NNI-West>	Interface Name of the AG2.1 router interface facing the Ethernet ring in the west direction	Example: ge-0/0/1
<ge xe-AG2.2-NNI-East>	Interface Name of the AG2.2 router interface facing the Ethernet ring in the east direction	Example: ge-0/0/1
<AG1.1:EVC-UNIT-ID>	Logical unit identifier of the interface used for EVC on AG1.1	0 through 1073741823
<AG1.2:EVC-UNIT-ID>	Logical unit identifier of the interface used for EVC on AG1.2	0 through 1073741823
<AG2.1:EVC-UNIT-ID>	Logical unit identifier of the interface used for EVC on AG2.1	0 through 1073741823
<AG2.2:EVC-UNIT-ID>	Logical unit identifier of the interface used for EVC on AG2.2	0 through 1073741823
<AN-1:lo0.0-ip-address>	IP address of the lo0.0 interface of the AN-1 access node	IP address format
<AN-2:lo0.0-ip-address>	IP address of the lo0.0 interface of the AN-2 access node	IP address format
<AG1.1:lo0.0-ip-address>	IP address of the lo0.0 interface of the AG1.1 access node	IP address format
<AG1.2:lo0.0-ip-address>	IP address of the lo0.0 interface of the AG1.2 access node	IP address format
<AG2.1:lo0.0-ip-address>	IP address of the lo0.0 interface of the AG2.1 access node	IP address format
<AG2.2:lo0.0-ip-address>	IP address of the lo0.0 interface of the AG2.2 access node	IP address format
<AG1.1-NODE-ID>	Node identifier used within VPLS instance configuration to define site ID	0 through 65534
<AG1.2-NODE-ID>	Node identifier used within VPLS instance configuration to define site ID	0 through 65534
<AG2.1-NODE-ID>	Node identifier used within VPLS instance configuration to define site ID	0 through 65534

Variable	Description	Value Range/Example
<AG2.2-NODE-ID>	Node identifier used within VPLS instance configuration to define site ID	0 through 65534
<AS>	Autonomous System Number	0 through 65534
<AN-2-ID>	Node identifier used within VPLS instance configuration to define site ID	0 through 1073741823
<G.8032-UNIT-ID>	Identifier of the Interface logical unit used for the G.8032 control channel	0 through 1073741823
<G.8032-AN-1-ID>	Node identifier within the G.8032 protection group	MAC address format: 00:00:01:02:03:04