Delivering Multicast Traffic in Access and Aggregation Networks

Application Note

September 2016
Contents
Use Case Overview.................................................................................................................................................................. 1
Enabling Multicast Delivery in the MAN ................................................................................................................................. 2
    Customer CPE Connected Directly at UNI ........................................................................................................................... 6
    Metro-AN Connected to the BB-AN .................................................................................................................................... 7
    Multicast Delivery with IEEE802.3 Bridging in Access ........................................................................................................ 7
Enabling Connectivity for the Inbound OAM of the CPE/STB ................................................................................................. 7
Configuring Nodes for the IPTV Profile ................................................................................................................................... 9
    Configuring the Access Node for the IPTV Profile ............................................................................................................. 9
    Configuring the Metro-AGN for the IPTV Service Profile ................................................................................................. 10
    Configuring the Metro PE for the IPTV Profile .................................................................................................................. 12
Use Case Overview

This residential aggregation use case is for operators who provide broadband service to residential customers.

Metro Ethernet network (MEN) aggregates Ethernet links from the following sources:

- Service provider broadband access nodes such as: digital subscriber line access multiplexers (DSLAMs), optical line terminals (OLTs), Ethernet access devices (EADs), cable modem termination systems (CMTSs), and so on.
- Directly from residential customer premises equipment (CPE), which then delivers traffic to the Broadband Network Gateway (BNG) which provides actual broadband access (BBE) services to the subscriber.

The BNG or service edge platform can be located at the provider’s service edge, or distributed to the metro area network (MAN) itself.

This use case describes how service providers can deliver a few services targeting essentially different terminal units—computer, broadband access router, set-top box (STB), and voice over IP (VoIP) terminal—all within the consumer’s home network. This is commonly known as the Triple play service model which includes data, voice, and video services provided over IP. Additionally, service providers require a technological connection to the CPE and STB for inbound management and control. Generally, a single Ethernet virtual circuit (EVC), which is typically used between the CPE and the service edge, cannot optimally deliver all types of service data.

For this residential aggregation use case in the MAN, the access model must provide at least three connectivity services per each subscriber for the following types of traffic:

- Internet data traffic with customer VLAN (cVLAN) or service VLAN (sVLAN) BBE service delivery model. In most cases, VoIP traffic delivery and video on demand (VoD) streams both use this connection.
- Multicast traffic geared towards IPTV service.
- Operations, Administration, and Maintenance (OAM) traffic for customer’s CPE and STB control and management. The same connection must be used for bootstrapping and first time provisioning of the customer’s CPE and STB units.

Figure 1 shows residential aggregation service profiles and possible deployment scenarios. This case study provides an overview of the deployment options for each of the three types of the connectivity required by residential service profile. Each option is described individually with some deployment variations. Service providers have the ability to arbitrarily combine design options of different connectivity services (until they explicitly contradict each other to develop an optimal solution in each concrete deployment.
Enabling Multicast Delivery in the MAN

Several applications drive the deployment of the multicast service profile in the metro area network. For residential consumers, backhauling of IPTV/over-the-top (OTT) services is one of the most common applications within a Triple-play offer.

This use case provides recommendations on how to enable multicast traffic distribution in the MEN for the residential model. Several deployment options supported by the current solution are shown in Figure 2.
Based on the platform, ACX Series or MX Series, a different set of protocols is used in access and aggregation of the MAN. The platforms are used end-to-end throughout the MAN. For a summary of the types of Juniper Networks recommended deployment technologies, see Table 1.

### Table 1 – Protocol Stack Recommendations for Residential Multicast in MAN

<table>
<thead>
<tr>
<th>Platform</th>
<th>Transport</th>
<th>Protocol for Multicast Traffic Delivery in Access</th>
<th>Protocol for Multicast Traffic Delivery in Core and Aggregation</th>
</tr>
</thead>
<tbody>
<tr>
<td>MX Series</td>
<td>IP/MPLS</td>
<td>-</td>
<td>NG-MVPN with P2MP MPLS LSP or P2P LSP in global context</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NG-MVPN with P2MP LSP or P2P LSP (ingress replication)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NG-VPLS with provider tunnel set to P2MP LSP</td>
</tr>
<tr>
<td>ACX5000 Series</td>
<td>IP/MPLS</td>
<td>PIM SM</td>
<td>PIM SM</td>
</tr>
<tr>
<td></td>
<td>IEEE802.3</td>
<td>VLAN Bridging</td>
<td>VLAN Bridging</td>
</tr>
<tr>
<td>ACX Series</td>
<td>IP/MPLS</td>
<td>PIM SM</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>IEEE802.3</td>
<td>VLAN Bridging</td>
<td>-</td>
</tr>
</tbody>
</table>
To avoid suboptimal traffic replication in the MAN, multicast traffic distribution is detached from the individual circuits used to deliver unicast traffic towards the subscriber’s CPE.

For the core and aggregation segments, the deployment model leverages Next-Generation Multicast VPN (NG-MVPN). NG-MVPN introduces a BGP-based control plane that is modeled after its highly successful counterpart of the VPN unicast control plane. By leveraging the functionality of common unicast BGP-MPLS VPNs, NG-MVPNs use the following properties:

- The BGP protocol distributes all necessary routing information to enable the VPN multicast service.
- The BGP protocol distributes customer-multicast (C-multicast) routes which results in the control traffic exchange being out-of-band from the data plane. This implementation enables the separation of the control and data plane protocols and simplifies the use of new transport technologies (such as, point-to-multipoint MPLS) for delivering MVPN services.

A BGP-based NG MVPN control plane supports both flexible topologies (such as, extranet or hub-and-spoke) and IPv6 addressing. By implementing IPv6-based NG MVPN, you can use MPLS encapsulation for IPv6 multicast. As an added benefit, IPv6-based NG-MVPN uses the same model as IPv6 VPN for unicast (as defined in RFC 4659), ensuring a more compatible integration of IPv6 multicast services with existing IPv4 NG-MVPN or IPv6 unicast VPN models.

BGP-MVPN provides multihoming support to connect a multicast source to two provider edge (PE) devices, enabling sub-second failover from a PE node failure. The auto-discovery of MVPN members available with the BGP approach provides a high degree of automation to establish provider tunnels used to transport MVPN data between PE devices.

Most likely, an additional PE router resides between the source and the upstream Metro PE router (see Figure 3). For this case, to enable discovery of the source by Metro PE devices, configure the devices as Rendezvous Points (RP) for the PIM instance that hosts the source of the multicast streams. For redundancy, you can configure several RPs with each one residing on a different Metro PE device. RPs can share the same IP address (anycast RP). Information about active sources that are registered on different RPs is exchanged automatically using BGP thus eliminating the need to run Multicast Source Discovery Protocol (MSDP) between RPs.

In this scenario, BGP is used to signal information about active multicast sources and receivers, and facilitate PE router auto-discovery. Figure 3 shows how multicast traffic is delivered over an MPLS core using a provider tunnel, P2MP, signaled using RSVP-TE.
In the access segment of the MAN, PIM protocol is suggested as the main method to deliver multicast traffic from the aggregation node towards the metro access node. As shown in Figure 3, this method is combined with NG-MVPN in the core end aggregation segments. The customer’s STB units signal group membership to the metro AN routers using IGMP which is delivered within the customer’s video VLAN. Metro access nodes use PIM-SM to distribute join/prune messages towards metro aggregation nodes, which are configured as anycast RPs in the access PIM domain. Routing information from the PIM domain is distributed into MVPN towards the upstream Metro PE device via MB-BGP.

In the proposed solution, distribution of the multicast routing information in the aggregation and core segments is tied to the global Virtual Routing and Forwarding (VRF) context by configuring a VRF instance-type of mpls-internet-multicast. This VRF is used only for control plane procedures, and does not support any interface configurations. All multicast and unicast routes used for IP multicast are associated only with the default routing instance (inet.0).

The P2MP LSP template enables provider tunnels and is associated with the forwarding plane for the multicast traffic by adding corresponding configuration under the mpls-internet-multicast VRF at the upstream Metro PE router as shown in the following Junos OS configuration code snippet:
Delivering Multicast Traffic in Access & Aggregation Network

**Head End Metro PE**

```
head_endMetroPE

routing-instances {
  internet-multicast {
    instance-type mpls-internet-multicast;
    provider-tunnel {
      rsvp-te {
        label-switched-path-template {
          NGMVPN;
        }
      }
    }
    protocols {
      mvpn;
    }
  }
}
```

**Metro AGN**

```
metroAGN

routing-instances {
  internet-multicast {
    instance-type mpls-internet-multicast;
    protocols {
      mvpn;
    }
  }
}
```

Within the solution, there are two possible options of how individual end subscribers can connect to the network:

- Direct connectivity at ACX Series access router.
- Connectivity provided by means of third-party access devices such as DSLAM, passive optical network (PON), or EAD.

The type of connectivity determines which technique is used to place the multicast stream of the given group into the subscriber’s video VLAN.

**Customer CPE Connected Directly at UNI**

If the customer’s CPE is directly connected at User to Network Interface (UNI) of the metro access node (Metro-AN), then the Metro-AN is responsible for inserting the multicast streams into the customer video VLAN based on IGMP joins received from the customer IPTV STB (see Figure 3).

To directly connect the customer’s CPE, configure the following options at the Metro-AN (ACX Series router):

- Add each logical unit (IFLs) of the subscriber’s UNI with assigned customer video VLAN to the bridge domain (BD).
- Enable IGMP snooping at the IFLs of the BD.
- Enable IGMP protocol on the Integrated Routing and Bridging (IRB) interface.
- Enable no-local-switching on the CPE-facing IFLs of the BD.
- Add the IRB interface to the PIM domain.
Metro-AN Connected to the BB-AN

If Metro-AN is connected to the broadband access node (BB-AN), then the BB-AN option should be used to deliver multicast streams to the customer video VLAN. Using other options results in suboptimal multicast traffic replication on the link between the BB-AN and the Metro-AN.

With this deployment, you configure a dedicated logical unit on the Metro-AN’s physical port connected to the BB-AN:

1. Assign a dedicated Multicast VLAN tag to the logical unit.
2. Configure the logical unit with IGMP.
3. Add the logical unit to the PIM domain.

Multicast Delivery with IEEE802.3 Bridging in Access

When a service provider selects IEEE802.3 Ethernet bridging as the transport technology for the Ethernet services in the access segment, then multicast traffic delivery occurs by adding it to a dedicated multicast VLAN shared across all Metro-AN. You can combine this method with NG-VPLS to distribute multicast traffic in aggregation and core segments of the MAN.

NOTE: Although this deployment option provides the same benefits as NG-MVPN (such as, new members auto-discovery, and multihoming of the source and receivers), with most components supported by both ACX Series and MX Series platforms, the detailed description of this deployment option is out of scope for this document.

Enabling Connectivity for the Inbound OAM of the CPE/STB

To provide an inbound management and control of the IPTV STB devices, enable a dedicated connectivity service over the MAN network. You can also use this connectivity service to bootstrap and auto-provision customer CPE when first connects to the network.

A service provider network operational center resides somewhere in the provider network, and uses either global context or dedicated Layer 3VPN to establish inbound connectivity to the access nodes of the MAN. For security issues, Juniper Networks recommends establishing a dedicated Layer 3 VPN to manage customer onsite devices.

A required connection service is established by an E-Tree Ethernet virtual connection from the Metro-AN towards the Metro-AGN. You can stitch the E-Tree service with management Layer 3 VPN via IRB interfaces. Figure 4 shows a service architecture for an MPLS access segment.
By configuring the Metro-AN for the multicast traffic delivery and enabling bridge domains, the logical interfaces (IFL) with customer VLAN assigned to each IFL, is aggregated. Within this example, a “VPLS light” configuration option of the ACX Series router is leveraged. To configure the options, follow these steps:

1. Add the Logical tunnel (LT) interface between the `vlan-bridge` family and the `vlan-ccc` family peers.
2. Add the `vlan-bridge` peer unit of the LT interface into the BD for video VLAN.
3. Originate a single, or active/standby MPLS pseudowire towards Metro-AGN and terminate it into the VPLS instance. You can share a single VPLS instance at the VPLS hub to connect to multiple Metro-ANs.
4. Provide connectivity to the Layer 3 VPN by enabling traffic forwarding between the VPLS instance and management Layer 3 VPN. Then, add the IRB interface into configuration of the VPLS and L3VPN at Metro-AGN.

You can now establish connectivity between the management and control systems of the IPTV STB.

To enable bootstrapping of the customer CPE, configure native VLAN at the access port of the Metro-AN to forward any untagged traffic (similar to the initial BOOTP/DHCP request) within the native VLAN towards the management Layer 3 VPN. The DHCP Relay function, activated at the IRB interface of the Metro AGN router, enables an initial network configuration to be assigned to the STB/CPE, and enables further provisioning of the customer unit with the production configuration.

You can use the same service architecture when you select Ethernet as a transport protocol for the metro Ethernet services in the access segment of the MAN.
Configuring Nodes for the IPTV Profile

Configuring the Access Node for the IPTV Profile

To configure the AN1.1 access node for the ACX Series:

1. Configure the following interfaces.

```plaintext
interfaces {
  <ge|xe-UNI-A-1> {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    native-vlan-id 100;
    unit <EVC-UNIT-ID> {
      family vlan-bridge;
      vlan-id <S-VLAN> ---- Here it stands for VLAN tag used for Customer Video VLAN
    }
  }
  <ge|xe-UNI-A-1> {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    native-vlan-id 100;
    unit <EVC-UNIT-ID> {
      family vlan-bridge;
      vlan-id <S-VLAN> ---- Here it stands for VLAN tag used for Customer Video VLAN
    }
  }
  <ge|xe-UNI-A-1> {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    native-vlan-id 100;
    unit <EVC-UNIT-ID> {
      family vlan-bridge;
      vlan-id <S-VLAN> ---- Here it stands for VLAN tag used for Customer Video VLAN
    }
  }
  irb {
    unit 0 {
      family inet {
        address 10.1.1.4/24;
      }
    }
  }
  lt-0/1/0 {      ---- This interface will be used for unicast only
    unit 0 {
      encapsulation vlan-bridge;
      vlan-id <S-VLAN>;
      peer-unit 1;
    }
    unit 1 {      ---- This interface will be used for unicast only
      encapsulation vlan-ccc;
      vlan-id <S-VLAN>;
      peer-unit 0;
    }
  }
}
```
2. Add interfaces to the bridge domain.

bridge-domains {
  bd-1 {
    vlan-id $S-VLAN$;
    interface lt-0/1/0.0;  // This interface will be used for unicast only
    interface <ge|xe-UNI-A-1>.<EVC-UNIT-ID>;
    interface <ge|xe-UNI-A-2>.<EVC-UNIT-ID>;
    interface <ge|xe-UNI-A-3>.<EVC-UNIT-ID>;
    routing-interface irb.0;  // This interface will be used for multicast
    protocols {
      igmp-snooping;
    }
  }
}

3. Enable IGMP and PIM protocols.

protocols {
  igmp {
    traceoptions {
      file igmp_irb;
    }
    interface irb.0;
  }
  pim {
    rp {
      auto-rp discovery;
    }
    interface <AN:ge|xe-West>;
    interface <AN:ge|xe-East>;
  }
  l2circuit {
    neighbor <AGN-1.1-Lo0.0> { // Will be used for unicast only
      interface lt-0/1/0.1 {
        virtual-circuit-id 10;
        no-control-word;
        ignore-encapsulation-mismatch;
      }
    }
  }
}

Configuring the Metro-AGN for the IPTV Service Profile

To configure the AGN1.1 metro access node for the MX Series:

1. Configure the following interface.

interfaces {
  irb {  // This interface will be used for unicast only
    unit 0 {
      family inet {
2. Enable IGMP and PIM protocols.

```plaintext
protocols {
  bgp {
    group ACCESS_RING {
      type internal;
      local-address 203.0.113.1;
      family inet {
        unicast;
      }
      family inet-vpn {
        unicast;
      }
      family inet-mvpn {
        signaling;
      }
      neighbor 198.51.100.0;
    }
  }
  msdp {
    local-address 203.0.113.1;
    peer 203.0.113.2;
  }
  pim {
    rp {
      local {
        address 203.0.113.10;
      }
    }
    interface <ge|xe-AG1.1-NNI-West>;
    interface <ge|xe-AG1.1-NNI-East>;
    mpls-internet-multicast;
  }
}
```

3. Configure the mpls-internet-multicast instance to enable NG-MVPN in global context.

```plaintext
routing-instances {
  internet-multicast {
    instance-type mpls-internet-multicast;
    protocols {
      mvpn;
    }
  }
}
```

4. Configure the Layer 3 VPN instance for video OAM/MNG (see Figure 4 for the architecture description).

```plaintext
routing-instances {
  IPTV_DHCP {
    instance-type vrf;
    interface irb.0;
  }
}
```
route-distinguisher 1:1;
vrftarget target:1:1;
vrftable-label;
forwarding-options {
dhcp-relay {
server-group {
    iptvservergroup {
        172.16.0.1;
    }
}
active-server-group iptvservergroup;
group iptvclientgroup {
    interface irb.0;
}
}
}

5. Configure the virtual switch interface (VSI) with VPLS protocol to aggregate the spokes pseudowire (PW) from access nodes for video OAM/MNG unicast traffic.

routing-instances {
    IPTV-control {
        instance-type virtual-switch;
        protocols {
            vpls {
                no-tunnel-services;
                mesh-group access {
                    inactive: associate-profile iptv;
                    vpls-id 100;
                    neighbor 10.0.0.1 {
                        encapsulation-type ethernet-vlan;
                        no-vlan-id-validate;
                    }
                    neighbor 10.0.0.6 {
                        encapsulation-type ethernet-vlan;
                        no-vlan-id-validate;
                    }
                }
            }
        }
    }
}
bridge-domains {
    iptv {
        domain-type bridge;
        vlan-id 11;
        routing-interface irb.0;
    }
}

Configuring the Metro PE for the IPTV Profile

To configure the metro PE1 device:
1. Enable IGMP and PIM protocols.

```plaintext
protocols {
    mpls {
        label-switched-path NGMVPN {
            template;
            link-protection;
            p2mp;
        }
        ---> Add a list of mpls core facing interfaces here
    }
    bgp {
        group BGP-GR-001 {
            type internal;
            local-address 198.51.100.0;
            family inet {
                unicast;
            }
            family inet-vpn {
                unicast;
            }
            family inet-mvpn {
                signaling;
            }
            export sourceleak;
            neighbor 203.0.113.1;  <---- Peering to AGN1.1
            neighbor 203.0.113.2;  <---- Peering to AGN1.2
        }
    }
    pim {
        rp {
            local {
                address 203.0.113.10;
            }
        }
        interface <ge|xe-PE-ENNI>;  <---- Interfaces
        mpls-internet-multicast;
    }
}
```

2. Configure the mpls-internet-multicast instance to enable NG-MVPN in global context.

```plaintext
routing-instances {
    internet-multicast {
        provider-tunnel {
            rsvp-te {
                label-switched-path-template {
                    NGMVPN;
                }
            }
        }
        instance-type mpls-internet-multicast;
        protocols {
            mvpn;
        }
    }
}
```
3. Configure the Layer 3 VPN instance for video OAM/MNG (see Figure 4 for the architecture description).

```bash
routing-instances {
    IPTV_DHCP {
        instance-type vrf;
        interface irb.0;
        route-distinguisher 1:1;
        vrf-target target:1:1;
        vrf-table-label;
    }
}
```