



Configuring Tenant Routed Multicast, Release 12.2.2

Table of Contents

New and Changed Information	1
Overview of Tenant Routed Multicast	2
Guidelines and Limitations	3
Overview of Tenant Routed Multicast with VXLAN EVPN Multi-Site	4
Tenant Routed Multicast with VXLAN EVPN Multi-Site Operations	5
Configuring TRM for Single Site Using Cisco Nexus Dashboard Fabric Controller	6
Configuring TRM for Multi-Site Using Cisco Nexus Dashboard Fabric Controller	9
Copyright	10

New and Changed Information

The following table provides an overview of the significant changes up to this current release. The table does not provide an exhaustive list of all changes or of the new features up to this release.

Release Version	Feature	Description
NDFC 12.2.2 release	Support added for creating VXLAN EVPN fabrics with a PIMv6 Underlay and TRM IPv6	<p>In previous releases of NDFC, NDFC supported an IPv6 underlay with ingress replication (IR). Beginning with the NDFC 12.2.2 release, NDFC added support for multicast replication. Previously NDFC supported a standalone VXLAN IPv4 fabric. Beginning with NDFC 12.2.2, NDFC supports creating a Multi-Site Domain (MSD) fabric with VXLAN IPv6.</p> <p>Prior to NDFC 12.2.2, NDFC supported Tenant Routed Multicast (TRM) IPv4. With NDFC 12.2.2, NDFC added a new TRM tab at the VRF level for supporting TRM IPv6.</p> <p>This feature is available for the following fabric types:</p> <ul style="list-style-type: none">• Data Center VXLAN EVPN fabric• BGP (eBGP EVPN) fabric• VXLAN EVPN Multi-Site fabric <p>For more information, see the following topics:</p> <ul style="list-style-type: none">• Configuring TRM for Single Site Using Cisco Nexus Dashboard Fabric Controller• "Configuring VXLAN EVPN Fabrics with a PIMv6 Underlay and TRMv6" section in Data Center VXLAN EVPN

Overview of Tenant Routed Multicast

Tenant Routed Multicast (TRM) enables multicast forwarding on the VXLAN fabric that uses a BGP-based EVPN control plane. TRM provides multi-tenancy aware multicast forwarding between senders and receivers within the same or different subnet local or across VTEPs.

With TRM enabled, multicast forwarding in the underlay is leveraged to replicate VXLAN encapsulated routed multicast traffic. A Default Multicast Distribution Tree (Default-MDT) is built per-VRF. This is an addition to the existing multicast groups for Layer-2 VNI Broadcast, Unknown Unicast, and Layer-2 multicast replication group. The individual multicast group addresses in the overlay are mapped to the respective underlay multicast address for replication and transport. The advantage of using a BGP-based approach allows the VXLAN BGP EVPN fabric with TRM to operate as fully distributed Overlay Rendezvous-Point (RP), with the RP presence on every edge-device (VTEP).

A multicast-enabled data center fabric is typically part of an overall multicast network. Multicast sources, receivers, and multicast rendezvous points might reside inside the data center but also might be inside the campus or externally reachable via the WAN. TRM allows a seamless integration with existing multicast networks. It can leverage multicast rendezvous points external to the fabric. Furthermore, TRM allows for tenant-aware external connectivity using Layer-3 physical interfaces or subinterfaces.

Guidelines and Limitations

Refer to the following documents for switch-level guidelines and limitations for Tenant Routed Multicast:

- [Guidelines and Limitations for Tenant Routed Multicast](#)
- [Guidelines and Limitations for Layer 3 Tenant Routed Multicast](#)

Following are additional guidelines and limitations at the NDFC level:

- When you perform a brownfield import on a fabric where the VRFs and the networks are deployed with the **Enable Tenant Routed Multicast** option enabled (without using a configuration profile), if the **Overlay Mode** option for the fabric is set to **cli**, the VRF-level **IPv4 TRM Enable** or the **IPv6 TRM Enable** option will not be enabled for VRFs imported into this fabric (in addition to the VRF-level **RP Address**, **RP Loopback ID**, **Underlay Mcast Address**, and **Overlay Mcast Groups** options, which will also not be enabled in this case).

In addition, if this VRF is deployed on a new leaf switch, IPv4 TRM or IPv6 TRM will not be enabled on that leaf switch for that VRF.

Overview of Tenant Routed Multicast with VXLAN EVPN Multi-Site

Tenant Routed Multicast with Multi-Site enables multicast forwarding across multiple VXLAN EVPN fabrics connected via Multi-Site.

The following two use cases are supported:

- Use Case 1: TRM provides Layer 2 and Layer 3 multicast services across sites for sources and receivers across different sites.
- Use Case 2: Extending TRM functionality from VXLAN fabric to source receivers external to the fabric.

TRM Multi-Site is an extension of BGP-based TRM solution that enables multiple TRM sites with multiple VTEPs to connect to each other to provide multicast services across sites in most efficient possible way. Each TRM site is operating independently and border gateway on each site allows stitching across each site. There can be multiple Border Gateways for each site. In a given site, the BGW peers with Route Server or BGWs of other sites to exchange EVPN and MVPN routes. On the BGW, BGP will import routes into the local VRF/L3VNI/L2VNI and then advertise those imported routes into the Fabric or WAN depending on where the routes were learnt from.

Tenant Routed Multicast with VXLAN EVPN Multi-Site Operations

The operations for TRM with VXLAN EVPN Multi-Site are as follows:

- Each Site is represented by Anycast VTEP BGWs. DF election across BGWs ensures no packet duplication.
- Traffic between Border Gateways uses ingress replication mechanism. Traffic is encapsulated with VXLAN header followed by IP header.
- Each Site will only receive one copy of the packet.
- Multicast source and receiver information across sites is propagated by BGP protocol on the Border Gateways configured with TRM.
- BGW on each site receives the multicast packet and re-encapsulate the packet before sending it to the local site.

For information about guidelines and limitations for TRM with VXLAN EVPN Multi-Site, see [Configuring Tenant Routed Multicast](#).

Configuring TRM for Single Site Using Cisco Nexus Dashboard Fabric Controller

This section assumes that a VXLAN EVPN fabric has already been provisioned using Cisco Nexus Dashboard Fabric Controller.

Perform the following steps to enable TRM for a single site.

1. Enable TRM for the selected Easy Fabric as follows:
 - a. If the fabric template is **Data Center VXLAN EVPN**, from the **Fabric Overview** > **Actions** drop-down list, choose **Edit Fabric**.
 - b. Click the **Replication** tab and configure the fields on the tab as follows:

Field	Description
Enable IPv4 Tenant Routed Multicast (TRM)	Check this check box to enable Tenant Routed Multicast (TRM) with IPv4 that allows overlay IPv4 multicast traffic to be supported over EVPN/MVPN in VXLAN EVPN fabrics.
Enable IPv6 Tenant Routed Multicast (TRM)	Check this check box to enable Tenant Routed Multicast (TRM) with IPv6 that allows overlay IPv6 multicast traffic to be supported over EVPN/MVPN in VXLAN EVPN fabrics.
Default MDT IPv4 Address for TRM VRFs	The multicast address for Tenant Routed Multicast traffic is populated. By default, this address is from the IP prefix specified in the Multicast Group Subnet field. When you update either field, ensure that the address is chosen from the IP prefix specified in Multicast Group Subnet .
Default MDT IPv6 Address for TRM VRFs	The multicast address for Tenant Routed Multicast traffic is populated. By default, this address is from the IP prefix specified in the IPv6 Multicast Group Subnet field. When you update either field, ensure that the address is chosen from the IP prefix specified in IPv6 Multicast Group Subnet .

- c. Click **Save** to save the fabric settings.

At this point, all the switches turn "Blue" as the switch is in the pending state.

- d. From the **Fabric Overview** > **Actions** drop-down menu, choose **Recalculate Config** and then choose **Deploy Config** to enable the following:
 - Enable feature ngmvpn: Enables the Next-Generation Multicast VPN (ngMVPN) control plane for BGP peering.
 - Configure ip multicast multipath s-g-hash next-hop-based: Multipath hashing algorithm for the TRM-enabled VRFs.
 - Configure ip igmp snooping vxlan: Enables IGMP Snooping for VXLAN VLANs.
 - Configure ip multicast overlay-spt-only: Enables the MVPN Route-Type 5 on all MPVN-enabled Cisco Nexus 9000 switches.
 - Configure and establish MVPN BGP AFI peering: This is necessary for the peering between

BGP RR and the leaf nodes.


For a VXLAN EVPN fabric created using a **BGP Fabric** template, enable the following fields depending on if you are enabling IPv4 or IPv6:

- **Enable IPv4 Tenant Routed Multicast (TRM)** or **Enable IPv6 Tenant Routed Multicast (TRM)**
- **Default MDT Address for TRM VRFs** or **Default MDT IPv6 Address for TRM VRFs**

You can find these fields by navigating to the **EVPN** tab.

2. Enable TRM for the VRF as follows:

- a. Navigate to **Fabric Overview > VRFs** and edit the selected VRF.
- b. Navigate to the **TRM** tab and edit the following TRM settings:

Field	Description
IPv4 TRM Enable	Check the check box to enable IPv4 TRM. If you enable IPv4 TRMv4, and provide the RP address, you must enter the underlay multicast address in the Underlay Mcast Address field.
NO RP	Check the check box to disable RP fields. You must enable IPv4 TRM to edit this check box. If you enable No RP , then the Is RP External , RP Address , RP Loopback ID , and Overlay Mcast Groups fields are disabled.
Is RP External	Check this check box if the RP is external to the fabric. If this check box is not checked, RP is distributed in every VTEP.
RP Address	Specifies the IP address of the RP.
RP Loopback ID	Specifies the loopback ID of the RP, if Is RP External is not enabled.
Underlay Multicast Address	Specifies the multicast address associated with the VRF. The multicast address is used for transporting multicast traffic in the fabric underlay. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>The multicast address in the Default MDT Address for TRM VRFs field on the fabric settings page is auto-populated in this field. You can override this field if a different multicast group address should be used for this VRF.</p> </div>
Overlay Mcast Groups	Specifies the multicast group subnet for the specified RP. The value is the group range in the <code>ip pim rp-address</code> command. If the field is empty, 224.0.0.0/24 is used as the default.
TRMv6 Enable	Check this check box to enable IPv6 TRM.
TRMv6 No RP	Check this check box to disable RP fields in TRMv6 as only PIM-SSM is used.
Is TRMv6 RP External	Check this check box if the RP is external to the fabric in TRMv6.

Field	Description
TRMv6 RP Address	Enter the IPv6 address for TRMv6 RP.
Overlay IPv6 Mcast Groups	Specifies the IPv6 multicast group subnet for the specified RP. The value is the group range in the <code>ipv6 pim rp-address</code> command. If the field is empty, <code>ff00::/8</code> is used as the default.
Enable MVPN inter-as	Check this check box to use the inter-AS keyword for the Multicast VPN (MVPN) address family routes to cross the BGP autonomous system (AS) boundary. This option is applicable if you enabled the TRM option.

3. Click **Save** to save the settings. The switches go into the pending state, that is, blue color. These settings enable the following:
 - o Enable PIM on L3VNI SVI.
 - o Route-Target Import and Export for MVPN AFI.
 - o RP and other multicast configuration for the VRF.
 - o Loopback interface using the above RP address and RP loopback id for the distributed RP.
4. Enable TRM for the network as follows:
 - a. On the **Fabric Overview** page, go to the **Networks** tab.
 - b. Edit the selected network and go to the **TRM** tab.
 - c. Check the **IPv4 TRM Enable** check box to enable TRM for IPv4 or check the **TRMv6 Enable** check box to enable TRM for IPv6.
 - d. Click **Save** to save the settings. The switches go into the pending state, that is, the blue color. The TRM settings enable the following:
 - Enable PIM on the L2VNI SVI.
 - Create a PIM policy **none** to avoid PIM neighborship with PIM routers within a VLAN. The **none** keyword is a configured route map to deny any IPv4 or IPv6 addresses to avoid establishing a PIM neighborship policy using anycast IP.

Configuring TRM for Multi-Site Using Cisco Nexus Dashboard Fabric Controller

This section assumes that a Multi-Site Domain (MSD) has already been deployed by Cisco Nexus Dashboard Fabric Controller and TRM needs to be enabled.

Perform the following steps to enable TRM for an MSD.

1. Enable TRM on the BGWs.
2. Navigate to **Fabric Overview > VRFs**. Make sure that the right Data Center VXLAN EVPN fabric is selected and edit the VRF.
3. Navigate to the **TRM** tab.
4. Edit the TRM settings as described in Step 2 of [Configuring TRM for Single Site Using Cisco Nexus Dashboard Fabric Controller](#).
5. Click **Save**.

The switches go into the pending state, that is, blue color. These settings enable the following:

- o Enable feature ngmvpn: Enables the Next-Generation Multicast VPN (ngMVPN) control plane for BGP peering.
 - o Enables PIM on L3VNI SVI.
 - o Configures the L3VNI multicast address.
 - o Route-target import and export for MVPN AFI.
 - o RP and other multicast configurations for the VRF.
 - o Loopback interface for the distributed RP.
 - o Enable the multi-site BUM ingress replication method for extending the Layer 2 VNI.
6. Establish MVPN AFI between the BGWs, as follows:
 - a. Double-click the MSD fabric to open the **Fabric Overview** page.
 - b. Choose **Links**. Filter it by the policy - **Overlays**.
 7. Select and edit each overlay peering to enable TRM by checking the **IPv4 Enable TRM** or the **TRMv6 Enable** check box.
 8. Click **Save** to save the settings.

The switches go into the pending state, that is, the blue color. The TRM settings enable MVPN peering between the BGWs, or BGWs and the route server.

Copyright

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2017–2024 Cisco Systems, Inc. All rights reserved.