Multitopology Routing

Multitopology Routing (MTR) enables you to configure service differentiation through class-based forwarding. MTR provides multiple logical topologies over a single physical network. Service differentiation can be achieved by forwarding different traffic types over different logical topologies that could take different paths to the same destination. MTR can be used, for example, to define separate topologies for voice, video, and data traffic classes

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Multitopology Routing

- You should have a clear understanding of the physical topology and traffic classification in your network before deploying Multitopology Routing (MTR).

- MTR should be deployed consistently throughout the network. Cisco Express Forwarding or distributed Cisco Express Forwarding and IP routing must be enabled on all networking devices.
- We recommend that you deconfigure custom route configurations such as route summarization and default routes before enabling a topology and that you reapply custom route configuration only after the topology is fully enabled. This recommendation is designed to prevent traffic interruption because some destinations might be obscured during the transition. Custom route configuration is most useful when all of the more-specific routes are available in the routing table of the topology.

Restrictions for Multitopology Routing

- Only the IPv4 (unicast and multicast) address family is supported.
- Multiple unicast topologies cannot be configured within a virtual routing and forwarding (VRF) instance. However, multiple unicast topologies and a separate multicast topology can be configured under the global address space, and a separate multicast topology can be configured within a VRF.
- All topologies share a common address space. Multitopology Routing (MTR) is not intended to enable address reuse. Configuring address reuse in separate topologies is not supported.
- IP Differentiated Services or IP Precedence can be independently configured in a network where MTR is also deployed. However, MTR requires exclusive use of some subset of the differentiated services code point (DSCP) bits in the IP packet header for specific topology traffic. For this reason, simultaneous configuration must be carefully coordinated. Re-marking DSCP bits in the IP packet header is not recommended or supported on devices that contain class-specific topologies.
- Distance Vector Multicast Routing Protocol (DVMRP) CLI and functionality are not provided in Cisco software images that provide MTR support.

Information About Multitopology Routing

MTR Overview

Use Multitopology Routing (MTR) to configure service differentiation through class-based forwarding. Two primary components comprise MTR configuration: independent topology configuration and traffic classification configuration.

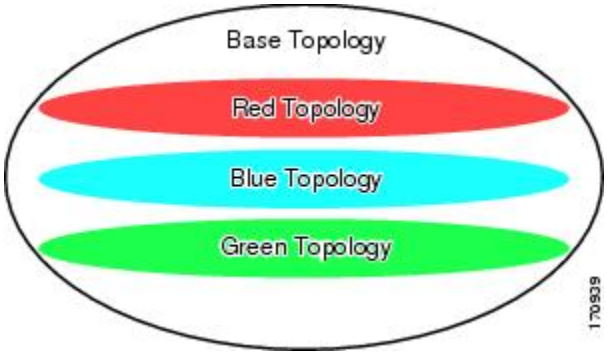
A topology is defined as a subset of devices and links in a network for which a separate set of routes is calculated. The entire network itself, for which the usual set of routes is calculated, is known as the base topology. The base topology (or underlying network) is characterized by the Network Layer Reachability Information (NLRI) that a device uses to calculate the global routing table to make routing and forwarding decisions. The base topology is the default routing environment that exists prior to enabling MTR.

Any additional topologies are known as class-specific topologies and are a subset of the base topology. Each class-specific topology carries a class of traffic and is characterized by an independent set of NLRI that is used to maintain a separate Routing Information Base (RIB) and Forwarding Information Base (FIB). This design allows the device to perform independent route calculation and forwarding for each topology.

MTR creates a selection of routes within a given device upon which to forward to a given destination. The specific choice of route is based on the class of the packet being forwarded, a class that is an attribute of the

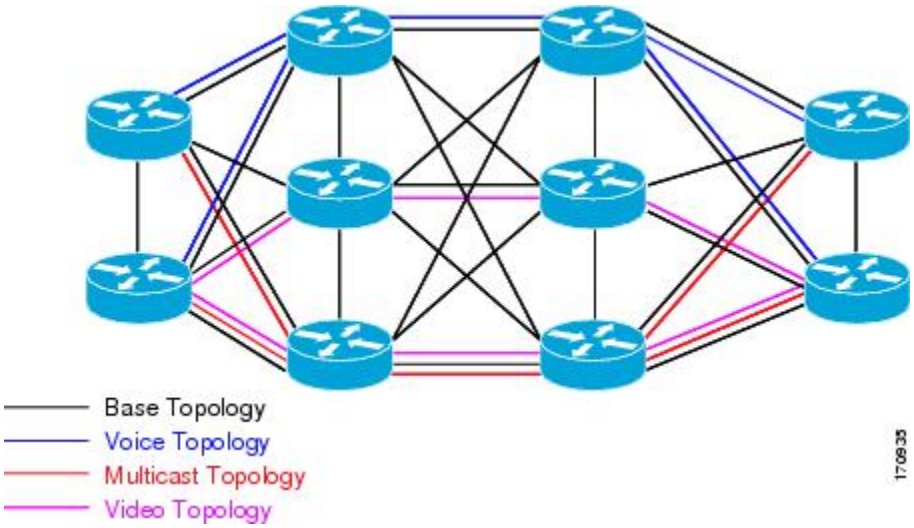
packet itself. This design allows packets of different classes to be routed independently from one another. The path that the packet follows is determined by classifiers configured on the devices and interfaces in the network. The figure below shows a base topology, which is a superset of the red, blue, and green topologies.

Figure 1: MTR Base Topology



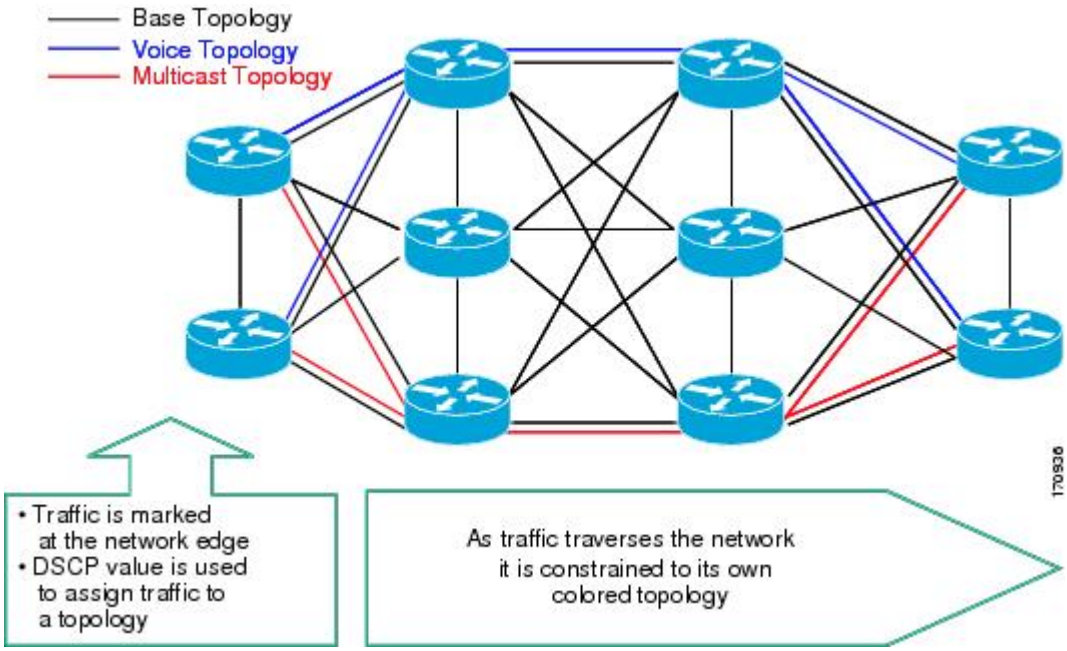
The figure below shows an MTR-enabled network that is configured using the service separation model. The base topology (shown in black) uses NLRI from all reachable devices in the network. The blue, red, and purple paths each represent a different class-specific topology. Each class-specific topology calculates a separate set of paths through the network. Routing and forwarding are independently calculated based on individual sets of NLRI that are carried for each topology.

Figure 2: Defining MTR Topologies



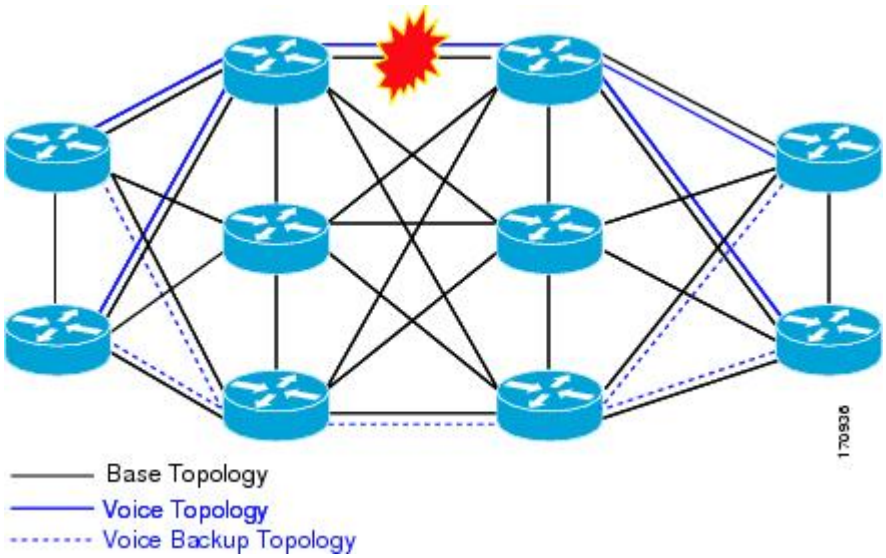
The figure below shows that the traffic is marked at the network edge. As the traffic traverses the network, the marking is used during classification and forwarding to constrain the traffic to its own colored topology.

Figure 3: Traffic Follows Class-Specific Forwarding Paths



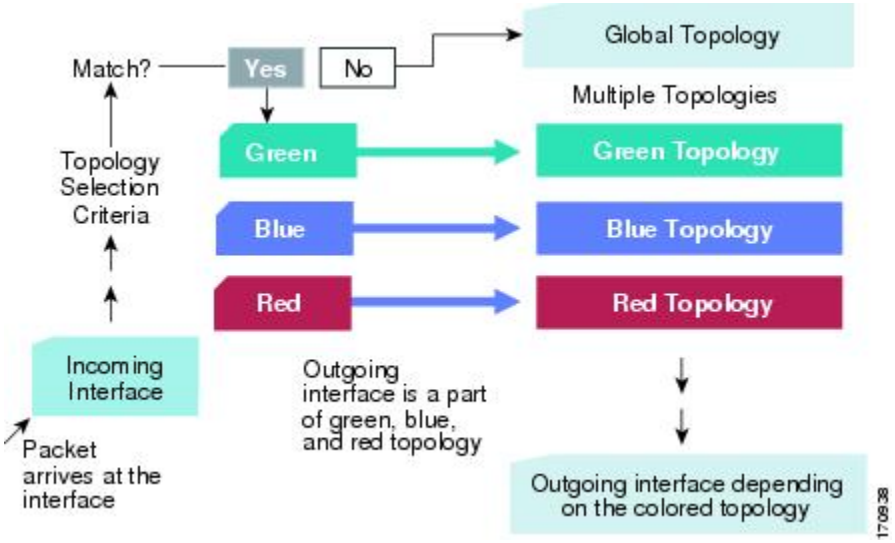
The same topology can have configured backup paths. In the figure below, the preferential path for the voice topology is represented by the solid blue line. In case this path becomes unavailable, you can configure MTR to choose the voice backup path represented by the dotted blue line. Both of these paths represent the same topology and none overlap.

Figure 4: MTR Backup Contingencies Within a Topology



The figure below shows the MTR forwarding model at the system level. When a packet arrives at the incoming interface, the marking is examined. If the packet marking matches a topology, the associated topology is consulted, the next hop for that topology is determined, and the packet is forwarded. If there is no forwarding entry within a topology, the packet is dropped. If the packet does not match any classifier, it is forwarded to the base topology. The outgoing interface is a function of the colored route table in which the lookup is done.

Figure 5: MTR Forwarding at the System Level



MTR is implemented in Cisco software according to a address family and subaddress family basis. MTR supports up to 32 unicast topologies (including the base topology) and a separate multicast topology. A topology can overlap with another or share any subset of the underlying network. You configure each topology with a unique topology ID. You configure the topology ID under the routing protocol, and the ID is used to identify and group NLRI for each topology in updates for a given protocol.

MTR Support for Multicast

Cisco software supports legacy (pre-Multitopology Routing (MTR) IP multicast behavior by default. MTR support for IP multicast must be explicitly enabled. Legacy IP multicast uses reverse path forwarding (RPF) on routes in the unicast Routing Information Base (RIB) to build multicast distribution trees (MDTs).

MTR introduces a multicast topology that is completely independent from the unicast topology. MTR integration with multicast allows you to control the path of multicast traffic in the network.

The multicast topology maintains separate routing and forwarding tables. The following list summarizes MTR multicast support that is integrated into Cisco software:

- Conventional longest match support for multicast routes.
- RPF support for Protocol Independent Multicast (PIM).
- Border Gateway Protocol (BGP) MDT subaddress family identifier (SAFI) support for Inter-AS VPNs (SAFI number 66).
- Support for static multicast routes integrated into the **ip route topology** command (modifying the **ip mroute** command).

As in pre-MTR software, you enable multicast support by configuring the **ip multicast-routing** command in global configuration mode. You enable MTR support for multicast by configuring the **ip multicast rpf multitopology** command. After the device enters global address family configuration mode, you then enter the **topology** command with the **base** keyword; global topology configuration parameters are applied in this mode.

MTR Traffic Classification

Multitopology Routing (MTR) cannot be enabled on a device until traffic classification is configured, even if only one class-specific topology is configured. Traffic classification is used to configure topology-specific forwarding behaviors when multiple topologies are configured on the same device. Traffic classification must be applied consistently throughout the network. Class-specific packets are associated with the corresponding topology table forwarding entries.

Traffic classification is configured when you use the modular quality of service (QoS) CLI (MQC). MTR traffic classification is similar to QoS traffic classification. However, there is an important distinction. MTR traffic classification is defined globally for each topology, rather than at the interface level as in QoS.

A subset of differentiated services code point (DSCP) bits is used to encode classification values in the IP packet header. You configure a class map to define the traffic class by entering the **class-map** *class-map-name* command in global configuration mode. Only the **match-any** keyword is supported for MTR. You associate the traffic class with a policy by configuring the **policy-map type class-routing ipv4 unicast** command in global configuration mode. You activate the policy for the topology by configuring the **service-policy type class-routing** command in global address family configuration mode. Then you associate the service policy with all interfaces on the device.

You can configure MTR traffic classification and IP Differentiated Services or IP Precedence-based traffic classification in the same network. However, MTR requires exclusive use of some subset of the DSCP bits in the IP packet header for specific topology traffic. In a network where MTR and QoS traffic classification are configured, you must carefully coordinate simultaneous configuration.

Routing Protocol Support for MTR

You must enable IP routing on the device for Multitopology Routing (MTR) to operate. MTR supports static and dynamic routing in Cisco software. You can enable dynamic routing per topology to support interdomain and intradomain routing. Route calculation and forwarding are independent for each topology. MTR support is integrated into Cisco software for the following protocols:

- Border Gateway Protocol (BGP)
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Integrated Intermediate System-to-Intermediate System (IS-IS)
- Open Shortest Path First (OSPF)

You apply the per-topology configuration in router address family configuration mode of the global routing process (router configuration mode). The address family and subaddress family are specified when the device enters address family configuration mode. You specify the topology name and topology ID by entering the **topology** command in address family configuration mode.

You configure each topology with a unique topology ID under the routing protocol. The topology ID is used to identify and group Network Layer Reachability Information (NLRI) for each topology in updates for a

given protocol. In OSPF, EIGRP, and IS-IS, you enter the topology ID during the first configuration of the **topology** command for a class-specific topology. In BGP, you configure the topology ID by entering the **bgp tid** command under the topology configuration.

You can configure class-specific topologies with different metrics than the base topology. Interface metrics configured on the base topology can be inherited by the class-specific topology. Inheritance occurs if no explicit inheritance metric is configured in the class-specific topology.

You configure BGP support only in router configuration mode. You configure Interior Gateway Protocol (IGP) support in router configuration mode and in interface configuration mode.

By default, interfaces are not included in nonbase topologies. For routing protocol support for EIGRP, IS-IS, and OSPF, you must explicitly configure a nonbase topology on an interface. You can override the default behavior by using the **all-interfaces** command in address family topology configuration mode. The **all-interfaces** command causes the nonbase topology to be configured on all interfaces of the device that are part of the default address space or the virtual routing and forwarding (VRF) instance in which the topology is configured.

BGP Routing Protocol Support for MTR

BGP Network Scope

To implement Border Gateway Protocol (BGP) support for Multitopology Routing (MTR), the scope hierarchy is required, but the scope hierarchy is not limited to MTR use. The scope hierarchy introduces new configuration modes such as router scope configuration mode. The device enters router scope configuration mode when you configure the **scope** command in router configuration mode. When this command is entered, a collection of routing tables is created.

You configure BGP commands under the scope hierarchy for a single network (globally), or on a per-virtual routing and forwarding (VRF) basis; these configurations are referred to as scoped commands. The scope hierarchy can contain one or more address families.

MTR CLI Hierarchy Under BGP

The Border Gateway Protocol (BGP) CLI provides backward compatibility for pre-Multitopology Routing (MTR) BGP configuration and provides a hierarchical implementation of MTR. Router configuration mode is backward compatible with the pre-address family and pre-MTR configuration CLI. Global commands that affect all networks are configured in this configuration mode. For address family and topology configuration, you configure general session commands and peer templates to be used in address family configuration mode or in topology configuration mode.

After configuring any global commands, you define the scope either globally or for a specific virtual routing and forwarding (VRF) instance. The device enters address family configuration mode when you configure the **address-family** command in router scope configuration mode or in router configuration mode. Unicast is the default address family if no subaddress family identifier (SAFI) is specified. MTR supports only the IPv4 address family with a SAFI of unicast or multicast.

When the device enters address family configuration mode from router configuration mode, the software configures BGP to use pre-MTR-based CLI. This configuration mode is backward compatible with pre-existing address family configurations. Entering address family configuration mode from router scope configuration mode configures the device to use the hierarchical CLI that supports MTR. Address family configuration parameters that are not specific to a topology are entered in this address family configuration mode.

The device enters BGP topology configuration mode when you configure the **topology** command in address family configuration mode. You can configure up to 32 topologies (including the base topology) on a device. You configure the topology ID by entering the **bgp tid** command. All address family and subaddress family configuration parameters for the topology are configured here.

Note Configuring a scope for a BGP routing process removes CLI support for pre-MTR-based configuration.

The following example shows the hierarchy levels that are used when you configure BGP for MTR implementation:

```
router bgp <autonomous-system-number>
 ! Global commands

 scope {global | vrf <vrf-name>}
  ! Scoped commands

  address-family {<afi>} [<safi>]
   ! Address family specific commands

   topology {<topology-name> | base}
    ! topology specific commands
```

BGP Sessions for Class-Specific Topologies

Multitopology Routing (MTR) is configured under the Border Gateway Protocol (BGP) on a per-session basis. The base unicast and multicast topologies are carried in the global (default) session. A separate session is created for each class-specific topology that is configured under a BGP routing process. Each session is identified by its topology ID. BGP performs a best-path calculation individually for each class-specific topology. A separate Routing Information Base (RIB) and Forwarding Information Base (FIB) are maintained for each session.

Topology Translation Using BGP

Depending on the design and policy requirements for your network, you might need to install routes from a class-specific topology on one device in a class-specific topology on a neighboring device. Topology translation functionality using the Border Gateway Protocol (BGP) provides support for this operation. Topology translation is BGP neighbor-session based. You configure the **neighbor translate-topology** command by using the IP address and topology ID from the neighbor.

The topology ID identifies the class-specific topology of the neighbor. The routes in the class-specific topology of the neighbor are installed in the local class-specific Routing Information Base (RIB). BGP performs a best-path calculation on all installed routes and installs these routes into the local class-specific RIB. If a duplicate route is translated, BGP selects and installs only one instance of the route per standard BGP best-path calculation behavior.

Topology Import Using BGP

Importing topologies using the Border Gateway Protocol (BGP) is similar to topology translation. The difference is that routes are moved between class-specific topologies on the same device. You configure this function by entering the **import topology** command and specify the name of the class-specific topology or base topology. Best-path calculations are run on the imported routes before they are installed into the topology

Routing Information Base (RIB). This **import topology** command also includes a **route-map** keyword to allow you to filter routes that are moved between class-specific topologies.

Interface Configuration Support for MTR

The configuration of a Multitopology Routing (MTR) topology in interface configuration mode allows you to enable or disable MTR on a per-interface basis. By default, a class-specific topology does not include any interfaces.

You can include or exclude individual interfaces by configuring the **topology** interface configuration command. You specify the address family and the topology (base or class-specific) when entering this command. The subaddress family can be specified. If no subaddress family is specified, the unicast subaddress family is used by default.

You can include globally all interfaces on a device in a topology by entering the **all-interfaces** command in routing topology configuration mode. Per-interface topology configuration applied with the **topology** command overrides global interface configuration.

The interface configuration support for MTR has these characteristics:

- Per-interface routing configuration: Interior Gateway Protocol (IGP) routing and metric configurations can be applied in interface topology configuration mode. Per-interface metrics and routing behaviors can be configured for each IGP.
- Open Shortest Path First (OSPF) interface topology configuration: Interface mode OSPF configurations for a class-specific topology are applied in interface topology configuration mode. In this mode, you can configure an interface cost or disable OSPF routing without removing the interface from the global topology configuration.
- Enhanced Interior Gateway Routing Protocol (EIGRP) interface topology configuration: Interface mode EIGRP configurations for a class-specific topology are applied in interface topology configuration mode. In this mode, you can configure various EIGRP features.
- Intermediate System-to-Intermediate System (IS-IS) interface topology configuration: Interface mode IS-IS configurations for a class-specific topology are applied in interface topology configuration mode. In this mode, you can configure an interface cost or disable IS-IS routing without removing the interface from the global topology configuration.

MTR Deployment Models

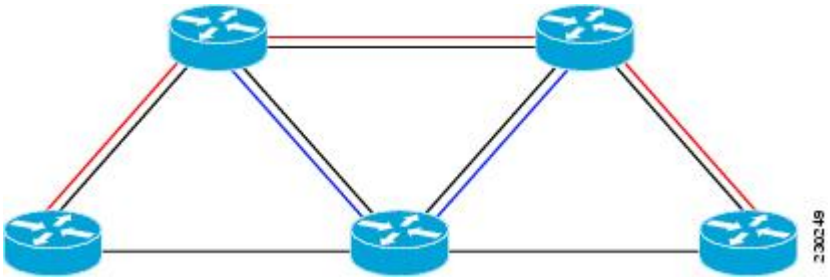
The base topology is the superset of all topologies in the network. It is defined by Network Layer Reachability Information (NLRI) for all reachable devices regardless of the deployment model that is used. Multitopology Routing (MTR) can be deployed using the service separation MTR model, or it can deployed using the overlapping MTR model. Each model represents a different approach to deploying MTR. However, these models are not mutually exclusive. Any level of variation of a combined model can be deployed.

Service Separation MTR Model

The figure below shows the service separation model where no topologies except for the base topology (shown in black) overlap with each other. In the service separation model, each class of traffic is constrained to its own exclusive topology. This model restricts the given class of traffic to a subset of the network. This model

is less configuration intensive than the overlapping MTR model because no topology-specific metrics need to be configured.

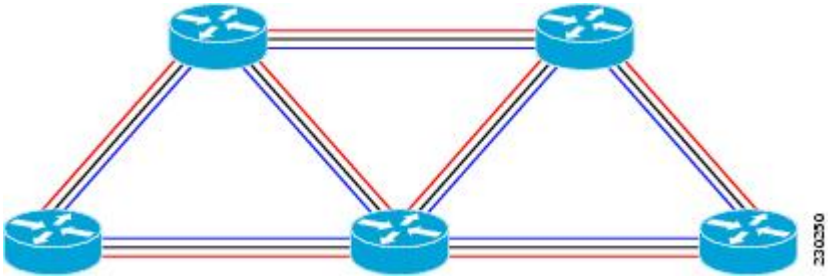
Figure 6: Service-Separation MTR Model



Overlapping MTR Model

In the overlapping Multitopology Routing (MTR) model, all topologies are configured to run over all devices in the network. This model provides the highest level of redundancy. All classes of traffic can use all links. Per-topology metrics are then configured to bias different classes of traffic to use different parts of the network. The redundancy that this model provides, however, makes it more configuration intensive than the service separation MTR model. In the figure below, all topologies are configured to run over all network devices. In this model, per-topology metrics are configured to bias the preferred routes for each topology.

Figure 7: Overlapping MTR Model



MTR Deployment Configuration

Multitopology Routing (MTR) supports both full and incremental deployment configurations. To support these options, MTR provides two different, configurable forwarding rules: strict forwarding mode for full deployment and incremental forwarding mode for an incremental deployment.

Strict Forwarding Mode for Full Deployment of MTR

Strict forwarding mode is the default forwarding mode in Multitopology Routing (MTR). In this mode, the device looks for a forwarding route only in the class-specific Forwarding Information Base (FIB). If no forwarding route is found, the device drops the received packet. In this mode, the device performs a longest match lookup for the topology FIB entry. This mode is designed for full deployment, where MTR is enabled on every device in the network or every device in the topology. Strict forwarding mode should be enabled

after an incremental deployment transition has been completed or when all devices in the network or topology are MTR enabled. You can enable strict forwarding mode after incremental forwarding mode by entering the **no forward-base** command in address family topology configuration mode.

Incremental Forwarding Mode for Incremental Deployment of MTR

Incremental forwarding mode is designed to support transitional or incremental deployment of Multitopology Routing (MTR), where devices in the network are not MTR enabled. In this mode, the device looks for a forwarding entry first in the class-specific Forwarding Information Base (FIB). If an entry is not found, the device looks for the longest match in the base topology FIB. If an entry is found in the base topology FIB, the device forwards the packet on the base topology. If a forwarding entry is not found in the base topology FIB, the device drops the packet.

This mode is designed to preserve connectivity during an incremental deployment of MTR and is recommended for use only during migration (the transition from a non-MTR to an MTR-enabled network). Class-specific traffic for a given destination is forwarded over contiguous segments of the class-specific topology containing that destination; otherwise, it is forwarded over the base topology.

This forwarding mode can be enabled to support mixed networks where some devices are not configured to run MTR. You enable incremental forwarding mode by entering the **forward-base** command in address family topology configuration mode.

Guidelines for Enabling and Disabling MTR

The section provides guidelines and procedures for enabling or disabling Multitopology Routing (MTR) in a production network. These guidelines assume that all participating networking devices are running a software image that supports MTR. The guidelines are designed to prevent major traffic interruptions due to misconfiguration and to minimize temporary transitional effects that can occur when you introduce or remove a topology from a network. The following guidelines must be implemented in the order that they are described:

First, create a class-specific topology on all networking devices and enable incremental forwarding mode by entering the **forward-base** command in address family topology configuration mode. Configure incremental forwarding whenever a topology is introduced or removed from the network. The topology is defined as a global container at this stage. No routing or forwarding can occur within the topology. Routing protocol support should not be configured.

Second, configure classification rules for the class-specific topology. You must consistently apply classification on all devices in the topology; each device has identical classifier configuration. You activate the topology when you attach a valid classification configuration to the global topology configuration. You can use **ping** and **traceroute** commands to verify reachability for interfaces and networking devices that are in the same topology and configured with identical classification.

Third, configure routing protocol support and static routing. Configure the devices in the topology one at a time. This configuration should include an interface, router process, and routing protocol-specific metrics and filters.

Enable routing in the topology by using a physical pattern in a contiguous manner relative to a single starting point. For example, configure all interfaces on a single device, and then all interfaces on each adjacent device. Follow this pattern until the task is complete. The starting point can be on the edge or core of the network. This recommendation is designed to increase the likelihood that class-specific traffic is forwarded on the same paths in the incremental topology as it is on the full topology when MTR is completely deployed.

If your network design requires strict forwarding mode, you should disable incremental forwarding only after you configure routing on all devices in a given topology. At this stage, MTR is fully operational. Class-specific

traffic is forwarded only over devices within the topology. Traffic that is not classified or destined for the topology is dropped.

When disabling a topology, reenable incremental forwarding mode. Remove custom route configuration, such as route summarization and default routes before disabling a topology, and reapply custom route configuration only after the topology is reenabled. This recommendation is designed to prevent traffic interruption because some destinations might be obscured during the transition. Custom route configuration is most useful when all of the more-specific routes are available in the routing table of the topology.

Note These guideliens apply only when a given classifier is enabled or disabled for a given topology. All other MTR configuration, including interface and routing protocol-specific configuration (other than the topology ID) can be modified dynamically as necessary.

How to Configure Multitopology Routing

Configuring a Multicast Topology for MTR

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip multicast-routing** [**vrf** *name*]
4. **ip multicast rpf multitopology**
5. **global-address-family ipv4** [**multicast** | **unicast**]
6. **topology** {**base** | *topology-name*}
7. **route-replicate from** {**multicast** | **unicast**} [**topology** {**base** | *name*}] *protocol* [**route-map** *name* | **vrf** *name*]
8. **use-topology unicast** {**base** | *topology-name*}
9. **shutdown**
10. **end**
11. **show topology** [**cache** [*topology-id*] | **ha** [**detail** | **interface** | **lock** | **router**] [**all** | **ipv4** | **ipv6** | **vrf** *vpn-instance*]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip multicast-routing** [**vrf** *name*] **Example:** `Device(config)# ip multicast-routing`	Enables IP multicast routing.
Step 4	**ip multicast rpf multitopology** **Example:** `Device(config)# ip multicast rpf multitopology`	Enables Multitopology Routing (MTR) support for IP multicast routing.
Step 5	**global-address-family ipv4** [**multicast** | **unicast**] **Example:** `Device(config)# global-address-family ipv4 multicast`	Enters global address family configuration mode to configure the global topology. • The address family for the class-specific topology is specified in this step. The subaddress family can be specified. Unicast is the default if no subaddress family is entered.
Step 6	**topology** {**base** | *topology-name*} **Example:** `Device(config-af)# topology base`	Configures the global topology instance and enters address family topology configuration mode. • Only the **base** keyword can be accepted for a multicast topology.
Step 7	**route-replicate from** {**multicast** | **unicast**} [**topology** {**base** | *name*}] *protocol* [**route-map** *name* | **vrf** *name*] **Example:** `Device(config-af-topology)# route-replicate from unicast topology VOICE ospf route-map map1`	(Optional) Replicates (copies) routes from another multicast topology Routing Information Base (RIB). • The *protocol* argument is configured to specify the protocol that is the source of the route. Routes can be replicated from the unicast base topology or a class-specific topology. **Note** However, route replication cannot be configured from a class-specific topology that is configured to forward the base topology (incremental forwarding). You can replicate routes from a multicast RIB to a multicast RIB or replicate routes from a unicast RIB to a multicast RIB, but you cannot replicate routes from a multicast RIB to a unicast RIB. • Replicated routes can be filtered through a route map before they are installed into the multicast RIB.

	Command or Action	Purpose
Step 8	**use-topology unicast** {**base** | *topology-name*} **Example:** `Device(config-af-topology)# use-topology unicast VIDEO`	(Optional) Configures a multicast topology to perform reverse path forwarding (RPF) computations using a unicast topology RIB. • The base or a class-specific unicast topology can be configured. When this command is configured, the multicast topology uses routes in the specified unicast topology table to build multicast distribution trees. **Note** This multicast RIB is not used when this command is enabled, even if the multicast RIB is populated and supported by a routing protocol.
Step 9	**shutdown** **Example:** `Device(config-af-topology)# shutdown`	(Optional) Temporarily disables a topology instance without removing the topology configuration (while other topology parameters are configured and other devices are configured with MTR).
Step 10	**end** **Example:** `Device(config-af-topology)# end`	(Optional) Exits address family topology configuration mode and enters privileged EXEC mode.
Step 11	**show topology** [**cache** [*topology-id*] | **ha** [**detail** | **interface** | **lock** | **router**] [**all** | **ipv4** | **ipv6** | **vrf** *vpn-instance*]] **Example:** `Device# show topology detail`	(Optional) Displays information about class-specific and base topologies.

What to Do Next

The topology is not activated until classification is configured. See the "QoS-MQC Support for MTR" feature module to configure classification for a class-specific topology.

Configuring MTR Traffic Classification

Before You Begin

Note Following the correct order of the commands in this task is very important. Ensure that all configuration that affects traffic classification is complete before entering the **service-policy type class-routing** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map match-any** *class-map-name*
4. **match** [**ip**] **dscp** *dscp-value* [*dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value*]
5. **exit**
6. **policy-map type class-routing ipv4 unicast** *policy-map-name*
7. **class** {*class-name* | **class-default**}
8. **select-topology** *topology-name*
9. **exit**
10. **exit**
11. **global-address-family ipv4** [**multicast** | **unicast**]
12. **service-policy type class-routing** *policy-map-name*
13. **end**
14. **show topology detail**
15. **show policy-map type class-routing ipv4 unicast** [**interface** [*type number*]]
16. **show mtm table**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**class-map match-any** *class-map-name* **Example:** `Device(config)# class-map match-any VOICE-CLASS`	Creates a class map to be used for matching packets to a specified class and enters quality of service (QoS) class-map configuration mode. • The Multitopology Routing (MTR) traffic class is defined using this command. **Note** The **match-any** keyword must be entered when configuring classification for MTR.

	Command or Action	Purpose
Step 4	**match** [**ip**] **dscp** *dscp-value* [*dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value*] **Example:** `Device(config-cmap)# match ip dscp 9`	Identifies a differentiated services code point (DSCP) value as a match criterion. • Use the *dcsp-value* argument to define a specific metric value. • Do not use the DSCP values 48 and 16. See the "Restrictions for QoS-MQC Support for MTR" section for more information.
Step 5	**exit** **Example:** `Device(config-cmap)# exit`	Exits QoS class-map configuration mode.
Step 6	**policy-map type class-routing ipv4 unicast** *policy-map-name* **Example:** `Device(config)# policy-map type class-routing ipv4 unicast VOICE-CLASS-POLICY`	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy and enters QoS policy-map configuration mode.
Step 7	**class** {*class-name* | **class-default**} **Example:** `Device(config-pmap)# class VOICE-CLASS`	Specifies the name of the class whose policy you want to create or change or specifies the default class and enters policy-map class configuration mode. • The class map is referenced. • For a class map to be referenced in a class-routing policy map, you must first define it by using the **class-map** command as shown in Step 3.
Step 8	**select-topology** *topology-name* **Example:** `Device(config-pmap-c)# select-topology VOICE`	Attaches the policy map to the topology.
Step 9	**exit** **Example:** `Device(config-pmap-c)# exit`	Exits QoS policy-map class configuration mode.
Step 10	**exit** **Example:** `Device(config-pmap)# exit`	Exits QoS policy-map configuration mode.

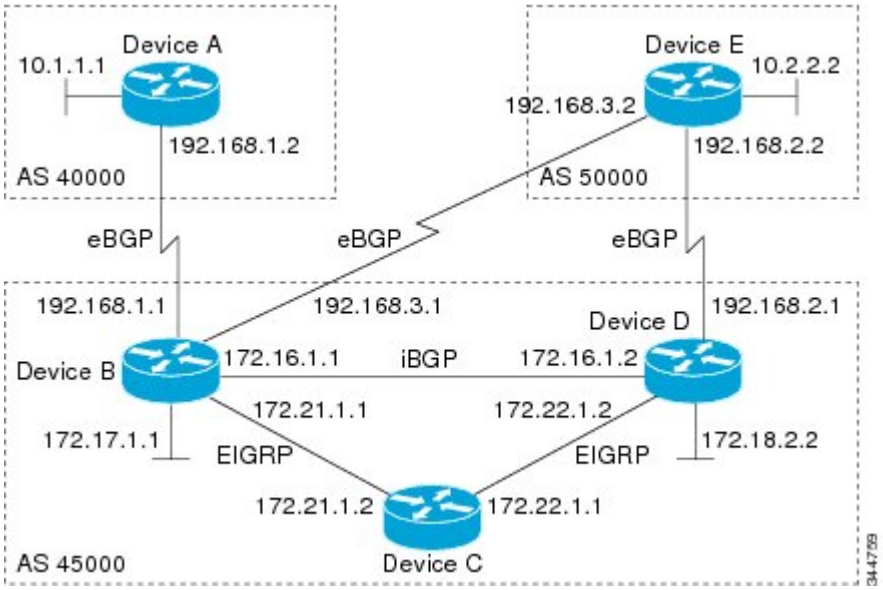
	Command or Action	Purpose
Step 11	**global-address-family ipv4** [**multicast** | **unicast**] **Example:** `Device(config)# global-address-family ipv4`	Enters global address family configuration mode to configure MTR.
Step 12	**service-policy type class-routing** *policy-map-name* **Example:** `Device(config-af)# service-policy type class-routing VOICE-CLASS-POLICY`	Attaches the service policy to the policy map for MTR traffic classification and activates MTR. • The *policy-map-name* argument must match the value configured in step 6. **Note** Traffic classification is enabled after this command is entered. Ensure that all configuration that affects traffic classification is complete before entering this command.
Step 13	**end** **Example:** `Device(config-af)# end`	Exits global address family configuration mode and returns to privileged EXEC mode.
Step 14	**show topology detail** **Example:** `Device# show topology detail`	(Optional) Displays detailed information about class-specific and base topologies.
Step 15	**show policy-map type class-routing ipv4 unicast** [**interface** [*type number*]] **Example:** `Device# show policy-map type class-routing ipv4 unicast`	(Optional) Displays the class-routing policy map configuration. • If you specify the **interface** keyword without the argument, statistics for all interfaces are displayed.
Step 16	**show mtm table** **Example:** `Device# show mtm table`	(Optional) Displays information about the DSCP values assigned to each topology.

Activating an MTR Topology by Using BGP

Perform this task to activate a Multitopology Routing (MTR) topology inside an address family by using the Border Gateway Protocol (BGP). This task is configured on Device B in the figure below and must also be configured on Device D and Device E. In this task, a scope hierarchy is configured to apply globally, and a neighbor is configured in router scope configuration mode. Under the IPv4 unicast address family, an MTR

topology that applies to video traffic is activated for the specified neighbor. There is no interface configuration mode for BGP topologies.

Figure 8: BGP Network Diagram



SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **scope** {**global** | **vrf** *vrf-name*}
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
6. **neighbor** {*ip-address* | *peer-group-name*} **transport** {**connection-mode** {**active** | **passive**} | **path-mtu-discovery** | **multi-session** | **single-session**}
7. **address-family ipv4** [**mdt** | **multicast** | **unicast**]
8. **topology** {**base** | *topology-name*}
9. **bgp tid** *number*
10. **neighbor** *ip-address* **activate**
11. **neighbor** {*ip-address* | *peer-group-name*} **translate-topology** *number*
12. **end**
13. **clear ip bgp topology** {* | *topology-name*} {*as-number* | **dampening** [*network-address* [*network-mask*]] | **flap-statistics** [*network-address* [*network-mask*]] | **peer-group** *peer-group-name* | **table-map** | **update-group** [*number* | *ip-address*]} [**in** [**prefix-filter**] | **out** | **soft** [**in** [**prefix-filter**] | **out**]]
14. **show ip bgp topology** {* | *topology*} **summary**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router bgp** *autonomous-system-number* **Example:** `Device(config)# router bgp 45000`	Enters router configuration mode to create or configure a BGP routing process.
Step 4	**scope** {**global** | **vrf** *vrf-name*} **Example:** `Device(config-router)# scope global`	Defines the scope for the BGP routing process and enters router scope configuration mode. • BGP general session commands that apply to a single network, or a specified virtual and routing forwarding (VRF) instance, are entered in this configuration mode. • Use the **global** keyword to specify that BGP uses the global routing table. • Use the **vrf** *vrf-name* keyword and argument to specify that BGP uses a specific VRF routing table. The VRF must already exist.
Step 5	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number* **Example:** `Device(config-router-scope)# neighbor 172.16.1.2 remote-as 45000`	Adds the IP address of the neighbor in the specified autonomous system to the multiprotocol BGP neighbor table of the local device.
Step 6	**neighbor** {*ip-address* | *peer-group-name*} **transport** {**connection-mode** {**active** | **passive**} | **path-mtu-discovery** | **multi-session** | **single-session**} **Example:** `Device(config-router-scope)# neighbor 172.16.1.2 transport multi-session`	Enables a TCP transport session option for a BGP session. • Use the **connection-mode** keyword to specify the type of connection, either active or passive. • Use the **path-mtu-discovery** keyword to enable the TCP transport path maximum transmission unit (MTU) discovery. • Use the **multi-session** keyword to specify a separate TCP transport session for each address family.

	Command or Action	Purpose
		• Use the **single-session** keyword to specify that all address families use a single TCP transport session.
Step 7	**address-family ipv4** [**mdt** | **multicast** | **unicast**] **Example:** `Device(config-router-scope)# address-family ipv4`	Specifies the IPv4 address family and enters router scope address family configuration mode. • Use the **mdt** keyword to specify IPv4 multicast distribution tree (MDT) address prefixes. • Use the **multicast** keyword to specify IPv4 multicast address prefixes. • Use the **unicast** keyword to specify the IPv4 unicast address family. By default, the device is placed in address family configuration mode for the IPv4 unicast address family if the **unicast** keyword is not specified with the **address-family ipv4** command. • Nontopology-specific configuration parameters are configured in this configuration mode.
Step 8	**topology** {**base** | *topology-name*} **Example:** `Device(config-router-scope-af)# topology VIDEO`	Configures the topology instance in which BGP routes class-specific or base topology traffic, and enters router scope address family topology configuration mode.
Step 9	**bgp tid** *number* **Example:** `Device(config-router-scope-af-topo)# bgp tid 100`	Associates a BGP routing process with the specified topology ID. • Each topology must be configured with a unique topology ID.
Step 10	**neighbor** *ip-address* **activate** **Example:** `Device(config-router-scope-af-topo)# neighbor 172.16.1.2 activate`	Enables the BGP neighbor to exchange prefixes for the network service access point (NSAP) address family with the local device. **Note** If you have configured a peer group as a BGP neighbor, do not use this command because peer groups are automatically activated when any peer group parameter is configured.
Step 11	**neighbor** {*ip-address* | *peer-group-name*} **translate-topology** *number* **Example:** `Device(config-router-scope-af-topo)# neighbor 172.16.1.2 translate-topology 200`	(Optional) Configures BGP to install routes from a topology on another device to a topology on the local device. • The topology ID is entered for the *number* argument to identify the topology on the device.

	Command or Action	Purpose
Step 12	**end** **Example:** `Device(config-router-scope-af-topo)# end`	(Optional) Exits router scope address family topology configuration mode and returns to privileged EXEC mode.
Step 13	**clear ip bgp topology** {***** | *topology-name*} {*as-number* | **dampening** [*network-address* [*network-mask*]] | **flap-statistics** [*network-address* [*network-mask*]] | **peer-group** *peer-group-name* | **table-map** | **update-group** [*number* | *ip-address*]} [**in** [**prefix-filter**] | **out** | **soft** [**in** [**prefix-filter**] | **out**]] **Example:** `Device# clear ip bgp topology VIDEO 45000`	Resets BGP neighbor sessions under a specified topology or all topologies.
Step 14	**show ip bgp topology** {***** | *topology*} **summary** **Example:** `Device# show ip bgp topology VIDEO summary`	(Optional) Displays BGP information about a topology. • Most standard BGP keywords and arguments can be entered following the **topology** keyword. **Note** Only the syntax required for this task is shown. For more details, see the *Cisco IOS IP Routing: BGP Command Reference*.

What to Do Next

Repeat this task for every topology that you want to enable, and repeat this configuration on all neighbor devices that are to use the topologies.

If you want to import routes from one Multitopology Routing (MTR) topology to another on the same device, see the “Importing Routes from an MTR Topology by Using BGP” section.

Importing Routes from an MTR Topology by Using BGP

Perform this task to import routes from one Multitopology Routing (MTR) topology to another on the same device, when multiple topologies are configured on the same device. In this task, a prefix list is defined to permit prefixes from the 10.2.2.0 network, and this prefix list is used with a route map to filter routes moved from the imported topology. A global scope is configured, address family IPv4 is entered, the VIDEO topology is specified, the VOICE topology is imported, and the routes are filtered using the route map named 10NET.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *number*] {**deny** | **permit**} *network/length* [**ge** *ge-length*] [**le** *le-length*]
4. **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
5. **match ip address** {*access-list-number* [*access-list-number ...* | *access-list-name...*] | *access-list-name* [*access-list-number ...* | *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name...*]}
6. **exit**
7. **router bgp** *autonomous-system-number*
8. **scope** {**global** | **vrf** *vrf-name*}
9. **address-family ipv4** [**mdt** | **multicast** | **unicast**]
10. **topology** {**base** | *topology-name*}
11. **import topology** {**base** | *topology-name*} [**route-map** *map-name*]
12. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip prefix-list** *list-name* [**seq** *number*] {**deny** | **permit**} *network/length* [**ge** *ge-length*] [**le** *le-length*] **Example:** `Device(config)# ip prefix-list TEN permit 10.2.2.0/24`	Configures an IP prefix list. • In this example, prefix list TEN permits advertising of the 10.2.2.0/24 prefix depending on a match set by the **match ip address** command.
Step 4	**route-map** *map-name* [**permit** | **deny**] [*sequence-number*] **Example:** `Device(config)# route-map 10NET`	Creates a route map and enters route-map configuration mode. • In this example, the route map named 10NET is created.
Step 5	**match ip address** {*access-list-number* [*access-list-number ...* | *access-list-name...*] |	Configures the route map to match a prefix that is permitted by a standard access list, an extended access list, or a prefix list.

	Command or Action	Purpose
	access-list-name [*access-list-number ...* | *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name...*]} **Example:** `Device(config-route-map)# match ip address prefix-list TEN`	• In this example, the route map is configured to match prefixes permitted by prefix list TEN.
Step 6	**exit** **Example:** `Device(config-route-map)# exit`	Exits route-map configuration mode and returns to global configuration mode.
Step 7	**router bgp** *autonomous-system-number* **Example:** `Device(config)# router bgp 50000`	Enters router configuration mode to create or configure a Border Gateway Protocol (BGP) routing process.
Step 8	**scope** {**global** | **vrf** *vrf-name*} **Example:** `Device(config-router)# scope global`	Defines the scope to the BGP routing process and enters router scope configuration mode. • BGP general session commands that apply to a single network, or a specified virtual routing and forwarding (VRF) instance, are entered in this configuration mode. • Use the **global** keyword to specify that BGP uses the global routing table. • Use the **vrf** *vrf-name* keyword and argument to specify that BGP uses a specific VRF routing table. The VRF must already exist.
Step 9	**address-family ipv4** [**mdt** | **multicast** | **unicast**] **Example:** `Device(config-router-scope)# address-family ipv4`	Enters router scope address family configuration mode to configure an address family session under BGP. • Nontopology-specific configuration parameters are configured in this configuration mode.
Step 10	**topology** {**base** | *topology-name*} **Example:** `Device(config-router-scope-af)# topology VIDEO`	Configures the topology instance in which BGP routes class-specific or base topology traffic, and enters router scope address family topology configuration mode.
Step 11	**import topology** {**base** | *topology-name*} [**route-map** *map-name*]	(Optional) Configures BGP to move routes from one topology to another on the same device.

	Command or Action	Purpose
	Example: `Device(config-router-scope-af-topo)# import topology VOICE route-map 10NET`	• The **route-map** keyword can be used to filter routes that moved between topologies.
Step 12	**end** **Example:** `Device(config-router-scope-af-topo)# end`	(Optional) Exits router scope address family topology configuration mode and returns to privileged EXEC mode.

Configuring an MTR Topology in Interface Configuration Mode

Before You Begin

Define a topology globally before configuring the per-interface topology configuration.

Note Interfaces cannot be excluded from the base topology by design. However, an Interior Gateway Protocol (IGP) can be excluded from an interface in a base topology configuration.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **topology ipv4** [**multicast** | **unicast**] {*topology-name* [**disable**] | **base**}
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface Ethernet 0/0`	Specifies the interface type and number, and enters interface configuration mode.
Step 4	**topology ipv4** [**multicast** | **unicast**] {*topology-name* [**disable**] | **base**} **Example:** `Device(config-if)# topology ipv4 VOICE`	Enters interface topology configuration mode to configure a Multitopology Routing (MTR) topology name on an interface. • Use the **disable** keyword to disable the topology instance on the interface. This form is used to exclude a topology configuration from an interface. • If the **no** form of this command is used, the topology interface configuration is removed. • If the **no** form of this command is used with the **disable** keyword, the topology instance is enabled on the interface.
Step 5	**end** **Example:** `Device(config-if-topology)# end`	Exits interface topology configuration mode and returns to privileged EXEC mode.

Enabling and Monitoring MTR Topology Statistics Accounting

Enabling Topology Statistics Accounting for MTR

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **global-address-family ipv4** [**multicast** | **unicast**]
4. **topology accounting**
5. **exit**
6. **interface** *type number*
7. **ip topology-accounting**
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**global-address-family ipv4** [**multicast**	**unicast**] **Example:** `Device(config)# global-address-family ipv4`	Enters global address family configuration mode.
Step 4	**topology accounting** **Example:** `Device(config-af)# topology accounting`	Enables topology accounting on all interfaces in the global address family for all IPv4 unicast topologies in the default virtual routing and forwarding (VRF) instance.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Device(config-af)# exit`	Exits global address family configuration mode.
Step 6	**interface** *type number* **Example:** `Device(config)# interface FastEthernet 1/10`	Specifies the interface type and number, and enters interface configuration mode.
Step 7	**ip topology-accounting** **Example:** `Device(config-if)# ip topology-accounting`	Enables topology accounting for all IPv4 unicast topologies in the VPN VRF associated with the specified interface. • This topology accounting is supported only for the default VRF.
Step 8	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Monitoring Interface and Topology IP Traffic Statistics for MTR

Use any of the following commands in any order to monitor interface and topology IP traffic statistics for Multitopology Routing (MTR).

SUMMARY STEPS

1. **enable**
2. **show ip interface** [*type number*] [**topology** {*name* | **all** | **base**}] [**stats**]
3. **show ip traffic** [**topology** {*name* | **all** | **base**}]
4. **clear ip interface** *type number* [**topology** {*name* | **all** | **base**}] [**stats**]
5. **clear ip traffic** [**topology** {*name* | **all** | **base**}]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**show ip interface** [*type number*] [**topology** {*name* | **all** | **base**}] [**stats**] **Example:** `Device# show ip interface FastEthernet 1/10 stats`	(Optional) Displays IP traffic statistics for all interfaces or statistics related to the specified interface. • If you specify an interface type and number, information for that specific interface is displayed. If you specify no optional arguments, information for all the interfaces is displayed. • If the **topology** *name* keyword and argument are used, statistics are limited to the IP traffic for that specific topology. • The **base** keyword displays the IPv4 unicast base topology.
Step 3	**show ip traffic** [**topology** {*name* | **all** | **base**}] **Example:** `Device# show ip traffic topology VOICE`	(Optional) Displays global IP traffic statistics (an aggregation of all the topologies when MTR is enabled) or statistics related to a particular topology. • The **base** keyword is reserved for the IPv4 unicast base topology.
Step 4	**clear ip interface** *type number* [**topology** {*name* | **all** | **base**}] [**stats**] **Example:** `Device# clear ip interface FastEthernet 1/10 topology all`	(Optional) Resets interface-level IP traffic statistics. • If the **topology** keyword and a related keyword are not used, only the interface-level aggregate statistics are reset. • If all topologies need to be reset, use the **all** keyword as the topology name.
Step 5	**clear ip traffic** [**topology** {*name* | **all** | **base**}] **Example:** `Device# clear ip traffic topology all`	(Optional) Resets IP traffic statistics. • If no topology name is specified, global statistics are cleared.

Testing Network Connectivity for MTR

SUMMARY STEPS

1. **enable**
2. **ping** [**vrf** *vrf-name* | **topology** *topology-name*] *protocol* [*target-address*] [*source-address*]
3. **traceroute** [**vrf** *vrf-name* | **topology** *topology-name*] [*protocol*] *destination*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**ping** [**vrf** *vrf-name* | **topology** *topology-name*] *protocol* [*target-address*] [*source-address*] **Example:** `Device# ping topology VOICE ip`	Configures the device to transmit ping messages to the target host in a topology. • An extended ping is configured by entering this command with only the topology name.
Step 3	**traceroute** [**vrf** *vrf-name* | **topology** *topology-name*] [*protocol*] *destination* **Example:** `Device# traceroute VOICE`	Configures the device to trace the specified host in a topology. • An extended trace is configured by entering this command with only the topology name. • If the **vrf** *vrf-name* keyword and argument are used, the **topology** option is not displayed because only the default virtual routing and forwarding (VRF) instance is supported. The **topology** *topology-name* keyword and argument and the differentiated services code point (DSCP) option in the extended traceroute system dialog are displayed only if there is a topology configured on the device.

Configuration Examples for Multitopology Routing

Examples Multicast Topology for MTR

Examples: Route Replication Configuration

The following example shows how to enable multicast support for Multitopology Routing (MTR) and to configure a separate multicast topology:

```
ip multicast-routing
ip multicast rpf multitopology
!
global-address-family ipv4 multicast
 topology base
 end
```

The following example shows how to configure the multicast topology to replicate Open Shortest Path First (OSPF) routes from the VOICE topology. The routes are filtered through the VOICE route map before they are installed in the multicast routing table.

```
ip multicast-routing
ip multicast rpf multitopology
!
access-list 1 permit 192.168.1.0 0.0.0.255
!
route-map VOICE
 match ip address 1
 exit
!
global-address-family ipv4 multicast
 topology base
 route-replicate from unicast topology VOICE ospf route-map VOICE
```

Example: Using a Unicast RIB for Multicast RPF Configuration

The following example shows how to configure the multicast topology to perform reverse path forwarding (RPF) calculations on routes in the VIDEO topology Routing Information Base (RIB) to build multicast distribution trees:

```
ip multicast-routing
ip multicast rpf multitopology
!
global-address-family ipv4 multicast
 topology base
 use-topology unicast VIDEO
 end
```

Example: Multicast Verification

The following example shows that the multicast topology is configured to replicate routes from the Routing Information Base (RIB) of the VOICE topology:

```
Device# show topology detail

Topology: base
  Address-family: ipv4
  Associated VPN VRF is default
  Topology state is UP
  Associated interfaces:
    Ethernet0/0, operation state: UP
    Ethernet0/1, operation state: DOWN
    Ethernet0/2, operation state: DOWN
    Ethernet0/3, operation state: DOWN
    Loopback0, operation state: UP

Topology: VIDEO
  Address-family: ipv4
  Associated VPN VRF is default
  Topology state is UP
  Topology fallback is enabled
  Topology maximum route limit 1000, warning limit 90% (900)
  Associated interfaces:
Topology: VOICE
  Address-family: ipv4
  Associated VPN VRF is default
  Topology state is UP
  Topology is enabled on all interfaces
  Associated interfaces:
    Ethernet0/0, operation state: UP
    Ethernet0/1, operation state: DOWN
```

```
    Ethernet0/2, operation state: DOWN
    Ethernet0/3, operation state: DOWN
    Loopback0, operation state: UP
Topology: base
  Address-family: ipv4 multicast
  Associated VPN VRF is default
  Topology state is DOWN
  Multicast multi-topology mode is enabled.
  Route Replication Enabled:
    from unicast topology VOICE all route-map VOICE
  Associated interfaces:
```

Examples: MTR Traffic Classification

The following example shows how to configure classification and activate Multitopology Routing (MTR) for two topologies:

```
global-address-family ipv4
 topology VOICE
  all-interfaces
  exit
 topology VIDEO
  forward-base
  maximum routes 1000 90
  exit
 exit
class-map match-any VOICE-CLASS
 match ip dscp 9
 exit
class-map match-any VIDEO-CLASS
 match ip dscp af11
 exit
policy-map type class-routing ipv4 unicast MTR
 class VOICE-CLASS
  select-topology VOICE
  exit
 class VIDEO-CLASS
  select-topology VIDEO
  exit
 exit
global-address-family ipv4
 service-policy type class-routing MTR
end
```

The following example shows how to display detailed information about the VOICE and VIDEO topologies:

```
Device# show topology detail

Topology: base
  Address-family: ipv4
  Associated VPN VRF is default
  Topology state is UP
  Associated interfaces:
    Ethernet0/0, operation state: UP
    Ethernet0/1, operation state: DOWN
    Ethernet0/2, operation state: DOWN
    Ethernet0/3, operation state: DOWN
    Loopback0, operation state: UP

Topology: VIDEO
  Address-family: ipv4
  Associated VPN VRF is default
  Topology state is UP
  Topology fallback is enabled
  Topology maximum route limit 1000, warning limit 90% (900)
  Associated interfaces:
Topology: VOICE
  Address-family: ipv4
  Associated VPN VRF is default
```

```
  Topology state is UP
  Topology is enabled on all interfaces
  Associated interfaces:
    Ethernet0/0, operation state: UP
    Ethernet0/1, operation state: DOWN
    Ethernet0/2, operation state: DOWN
    Ethernet0/3, operation state: DOWN
    Loopback0, operation state: UP
Topology: base
  Address-family: ipv4 multicast
  Associated VPN VRF is default
  Topology state is DOWN
  Multicast multi-topology mode is enabled.
  Route Replication Enabled:
    from unicast topology VOICE all route-map BLUE
  Associated interfaces:
    Ethernet0/0, operation state: UP
    Ethernet0/1, operation state: DOWN
    Ethernet0/2, operation state: DOWN
    Ethernet0/3, operation state: DOWN
    Loopback0, operation state: UP
```

The following example shows how to display the classification values for the VOICE and VIDEO topologies:

```
Device# show mtm table

MTM Table for VRF: default, ID:0
Topology                Address Family   Associated VRF         Topo-ID
base                    ipv4              default                 0
VOICE                    ipv4             default                 2051
Classifier: ClassID:3
DSCP: cs1
DSCP: 9
VIDEO                    ipv4             default                 2054
Classifier: ClassID:4
DSCP: af11
```

Examples Activating an MTR Topology by Using BGP

Example: BGP Topology Translation Configuration

The following example shows how to configure the Border Gateway Protocol (BGP) in the VIDEO topology and how to configure topology translation with the 192.168.2.2 neighbor:

```
router bgp 45000
 scope global
  neighbor 172.16.1.1 remote-as 50000
  neighbor 192.168.2.2 remote-as 55000
  neighbor 172.16.1.1 transport multi-session
  neighbor 192.168.2.2 transport multi-session
   address-family ipv4
    topology VIDEO
     bgp tid 100
     neighbor 172.16.1.1 activate
     neighbor 192.168.2.2 activate
     neighbor 192.168.2.2 translate-topology 200
     end
clear ip bgp topology VIDEO 50000
```

Example: BGP Global Scope and VRF Configuration

The following example shows how to configure a global scope for a unicast topology and also for a multicast topology. After the device exits the router scope configuration mode, a scope is configured for the virtual routing and forwarding (VRF) instance named DATA.

```
router bgp 45000
 scope global
  bgp default ipv4-unicast
  neighbor 172.16.1.2 remote-as 45000
  neighbor 192.168.3.2 remote-as 50000
  address-family ipv4 unicast
   topology VOICE
   bgp tid 100
   neighbor 172.16.1.2 activate
   exit
  address-family ipv4 multicast
   topology base
    neighbor 192.168.3.2 activate
    exit
   exit
  exit
 scope vrf DATA
  neighbor 192.168.1.2 remote-as 40000
  address-family ipv4
   neighbor 192.168.1.2 activate
   end
```

Examples: BGP Topology Verification

The following example shows summary output for the **show ip bgp topology** command. Information is displayed about Border Gateway Protocol (BGP) neighbors configured to use the Multitopology Routing (MTR) topology named VIDEO.

```
Device# show ip bgp topology VIDEO summary

BGP router identifier 192.168.3.1, local AS number 45000
BGP table version is 1, main routing table version 1
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.16.1.2      4 45000     289     289        1    0    0 04:48:44        0
192.168.3.2     4 50000       3       3        1    0    0 00:00:27        0
```

The following partial output displays BGP neighbor information under the VIDEO topology:

```
Device# show ip bgp topology VIDEO neighbors 172.16.1.2

BGP neighbor is 172.16.1.2,  remote AS 45000, internal link
  BGP version 4, remote router ID 192.168.2.1
  BGP state = Established, up for 04:56:30
  Last read 00:00:23, last write 00:00:21, hold time is 180, keepalive interval is 60
seconds
  Neighbor sessions:
    1 active, is multisession capable
  Neighbor capabilities:
    Route refresh: advertised and received(new)
  Message statistics, state Established:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                0          0
    Keepalives:           296        296
    Route Refresh:          0          0
    Total:                297        297
```

```
  Default minimum time between advertisement runs is 0 seconds
 For address family: IPv4 Unicast topology VIDEO
  Session: 172.16.1.2 session 1
  BGP table version 1, neighbor version 1/0
  Output queue size : 0
  Index 1, Offset 0, Mask 0x2
1 update-group member
  Topology identifier: 100
.
.
.
  Address tracking is enabled, the RIB does have a route to 172.16.1.2
  Address tracking requires at least a /24 route to the peer
  Connections established 1; dropped 0
  Last reset never
  Transport(tcp) path-mtu-discovery is enabled
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Minimum incoming TTL 0, Outgoing TTL 255
Local host: 172.16.1.1, Local port: 11113
Foreign host: 172.16.1.2, Foreign port: 179
.
.
.
```

Example: Importing Routes from an MTR Topology by Using BGP

The following example shows how to configure an access list to be used by a route map named VOICE to filter routes imported from the Multitopology Routing (MTR) topology named VOICE. Only routes with the prefix 192.168.1.0 are imported.

```
access-list 1 permit 192.168.1.0 0.0.0.255
route-map BLUE
 match ip address 1
 exit
router bgp 50000
 scope global
  neighbor 10.1.1.2 remote-as 50000
  neighbor 172.16.1.1 remote-as 60000
   address-family ipv4
    topology VIDEO
     bgp tid 100
     neighbor 10.1.1.2 activate
     neighbor 172.16.1.1 activate
     import topology VOICE route-map VOICE
     end
clear ip bgp topology VIDEO 50000
```

Example: MTR Topology in Interface Configuration Mode

The following example shows how to disable the VOICE topology on Ethernet interface 0/0:

```
interface Ethernet 0/0
 topology ipv4 VOICE disable
```

Examples: Monitoring Interface and Topology IP Traffic Statistics for MTR

In the following example, the **show ip interface** command displays IP traffic statistics for Fast Ethernet interface 1/10:

```
Device# show ip interface FastEthernet 1/10 stats
```

```
FastEthernet1/10
 5 minutes input rate 0 bits/sec, 0 packet/sec,
 5 minutes output rate 0 bits/sec, 0 packet/sec,
 201 packets input, 16038 bytes
 588 packets output, 25976 bytes
```

In this example, the **show ip traffic** command displays statistics related to a particular topology:

```
Device# show ip traffic topology VOICE

  Topology: VOICE
  5 minute input rate 0 bits/sec, 0 packet/sec,
  5 minute output rate 0 bits/sec, 0 packet/sec,
  100 packets input, 6038 bytes,
  88 packets output, 5976 bytes.
```

Examples: Testing Network Connectivity for MTR

The following example shows how to send a ping to the 10.1.1.2 neighbor in the VOICE topology:

```
Device# ping topology VOICE ip 10.1.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

The following example shows how to trace the 10.1.1.4 host in the VOICE topology:

```
Device# traceroute VOICE ip 10.1.1.4
Type escape sequence to abort.
Tracing the route to 10.1.1.4
  1 10.1.1.2 4 msec *  0 msec
  2 10.1.1.3 4 msec *  2 msec
  3 10.1.1.4 4 msec *  4 msec
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Multitopology Routing (MTR) commands	Cisco IOS Multitopology Routing Command Reference

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for MTR Support for Multicast

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Multi-Topology Routing

Feature Name	Releases	Feature Information
MTR Support for Multicast	15.0(1)SY	This feature provides MTR support for multicast and allows the user to control the path of multicast traffic in the network. The following commands were introduced or modified: **clear ip route multicast**, **ip multicast rpf multitopology**, **show ip route multicast**, **use-topology**.

Glossary

base topology—The entire network for which the usual set of routes are calculated. This topology is the same as the default global routing table that exists without Multitopology Routing (MTR) being used.

class-specific topology—New topologies that are defined over and above the existing base topology; each class-specific topology is represented by its own Routing Information Base (RIB) and Forwarding Information Base (FIB).

classification—Selection and matching of traffic that needs to be provided with a different treatment based on its mark. Classification is a read-only operation.

DSCP—differentiated services code point. Six bits in the Type of Service (ToS) field. Two bits are used for Explicit Congestion Notification, which are used to mark the packet.

incremental forwarding mode—Incremental forwarding mode is designed to support transitional or incremental deployment of MTR, where devices are in the network that are not MTR enabled. In this mode, the device looks for a forwarding entry first in the class-specific FIB. If an entry is not found, the device then looks for the longest match in the base topology FIB. If an entry is found in the base topology FIB, the packet is forwarded on the base topology. If a forwarding entry is not found in the base topology FIB, the packet is dropped.

marking—Setting a value in the packet or frame. Marking is a read and write operation.

multitopology—Multitopology means that each topology routes and forward a subset of the traffic as defined by the classification criteria.

NLRI—Network Layer Reachability Information.

strict forwarding mode—Strict forwarding mode is the default forwarding mode for MTR. Only routes in the topology-specific routing table are considered. Among these, the longest match for the destination address is used. If no route containing the destination address can be found in the topology specific table, the packet is dropped.

TID—Topology Identifier. Each topology is configured with a unique topology ID. The topology ID is configured under the routing protocol and is used to identify and group NLRI for each topology in updates for a given protocol.