Configuring and Applying OER Policies

First Published: January 29, 2007
Last Updated: July 19, 2007

This module describes the Cisco IOS Optimized Edge Routing (OER) apply policy phase. In the apply policy phase, OER uses policies to map the measured performance metrics of traffic class entries in the Monitored Traffic Class (MTC) list, or exit links, against well-known or configured thresholds to determine if the traffic class entry performance or the link utilization is meeting specified levels of service, or if some action is required.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for Configuring and Applying OER Policies" section on page 73.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for Configuring and Applying OER Policies

Before implementing OER policies, you need to understand an overview of how OER works and how to set up OER network components. See the "Cisco IOS Optimized Edge Routing Overview" and "Setting Up OER Network Components" modules for more details. If you are following the OER performance loop, the OER profile and measure phases precede this phase. See the "Where to Go Next" section on page 71 for more details.

Information About Configuring and Applying OER Policies

To configure and apply OER policies, you should understand the following concepts:

- OER Apply Policy Phase Overview, page 2
- OER Policy Decision Point, page 3
- OER Traffic Class Performance Policies, page 5
- OER Link Policies, page 6
- Performance Routing Link Grouping, page 9
- OER Network Security Policies, page 10
- OER Policy Operational Options and Parameters, page 10
- OER Policy Application, page 12
- Priority Resolution for Multiple OER Policies, page 13

OER Apply Policy Phase Overview

The OER apply policy phase is the third step in the OER performance loop following after the profile phase that identifies the traffic classes, and the measure phase where each traffic class entry in the MTC list is monitored to determine performance metric measurements. The apply policy phase compares the measured performance metrics against well-known or configured thresholds to determine if the traffic is meeting specified levels of service, or if some action is required. If the performance metric does not conform to the threshold, a decision is made by OER to move the traffic class or exit into another state. For more details about the state transition decision, see the "OER Policy Decision Point" section on page 3.

An OER policy is a rule that defines an objective and contains the following attributes:

- A scope.
- An action.
- A triggering event or condition.

For example, a policy can be configured to maintain a delay of less than or equal to 100 milliseconds for packets sent to a specific traffic class entry. The scope is the network traffic sent to the specific traffic class entry, the action is a routing table change, and the triggering event is a measured delay of greater than 100 milliseconds for this traffic. The action may be not be executed until OER is configured to control the traffic in the OER control phase. By default, OER runs in an observe mode during the profile, measure, and apply policy phases.

In the OER apply policy phase you can configure and apply policies. Different types of OER policies can be configured—see Figure 1—and specific OER parameters and options can be included within a policy. In this document, a parameter is a configurable element that can be fine-tuned, and an option is a configurable element that is either enabled or disabled. After an OER policy is configured, the policy can be applied to learned traffic classes or configured traffic classes. OER policies can be applied globally—to all the traffic classes—or to just a specific set of traffic classes.

Figure 1   *OER Apply Policy Phase Structure*

In Figure 1 you can see that there are three types of OER policies plus some operational options and parameters that can be configured. Use the following links to review more information about each policy type, parameter, or option:

- OER Traffic Class Performance Policies, page 5
- OER Link Policies, page 6
- OER Network Security Policies, page 10
- OER Policy Operational Options and Parameters, page 10

After an OER policy is configured, you can see from Figure 1 that a policy can be applied to learned traffic classes or configured traffic classes on a global basis for all traffic classes or for a specific set of traffic classes. For more details about applying OER policies, see the "OER Policy Application" section on page 12.

When configuring multiple policy parameters for traffic classes, it is possible to have multiple overlapping policies. To resolve the potential conflict of which policy to run, OER uses its resolve function: a flexible mechanism that allows you to set the priority for most of the policy types. For more details about how OER resolves multiple policy conflicts, see the "Priority Resolution for Multiple OER Policies" section on page 13.

OER Policy Decision Point

When running an OER policy that compares the traffic class performance metrics with default or configured thresholds, a traffic class may change state. OER uses a policy decision point (PDP) that operates according to the traffic class state transition diagram shown in Figure 2. The state transition diagram in Figure 2 contains the following states:

- Default—A traffic class is placed in the default state when it is not under OER control. Traffic classes are placed in the default state when they are initially added to the central policy database, the MTC. A traffic class will transition into and out of the default state depending on performance measurements, timers, and policy configuration.

- Choose Exit—This is a temporary state in which the PDP compares the current state of the traffic class against its policy settings and chooses the optimal exit for the traffic class. OER will try to keep a traffic class flowing through its current exit but, as in the default state, performance measurements, timers, and policy configurations can cause the master controller to place a traffic class in this state for the duration of the exit link selection process. The traffic class remains in the choose exit state until it is moved to the new exit.

- Holddown—A traffic class is placed in the holddown state when the master controller requests a border router to forward the traffic class to be monitored using probes. Measurements are collected for the selected traffic class until the holddown timer expires unless the exit used by this traffic class is declared unreachable. If the exit is unreachable, the traffic class transitions back to the choose exit state.

Figure 2   **OER Traffic Class State Transition Diagram**

- In-Policy—After performance measurements are compared against default or user-defined policy settings and an exit selection is made, the traffic class enters an in-policy state. When a traffic class is in the in-policy state, the traffic class is forwarded through an exit that satisfies the default or user-defined settings. The master controller continues to monitor the traffic class, but no action is taken until the periodic timer expires, or an out-of-policy message is received from a measurement collector, when the traffic class transitions back to the choose exit state.

- Out-of-Policy (OOP)—A traffic class is placed in this state when there are no exits through which to forward the traffic class that conform to default or user-defined policies. While the traffic class is in this state, the backoff timer controls exiting from this state. Each time the traffic class enters this state, the amount of time the traffic class spends in this state increases. The timer is reset for a traffic class when the traffic class enters an in-policy state. If all exit links are out-of-policy, the master controller may select the best available exit.

OER Traffic Class Performance Policies

OER traffic class performance policies are a set of rules that govern performance characteristics for traffic classes that can be network addresses (prefixes) or application criteria such as protocol, port number, or DSCP value. Network addresses can refer to individual endpoints within a network (e.g. 10.1.1.1/32) or to entire subnets (e.g. 10.0.0.0/8). The major performance characteristics that can be managed within an OER policy are:

With the exception of reachability, none of these performance characteristics can be managed within the constructs of conventional routing protocol metrics. Cisco OER extends the concept of reachability (beyond ensuring that a particular route exists in the routing table) by automatically verifying that the destination can be reached through the indicated path. Using Cisco OER provides the network administrator with a new and powerful toolset for managing the flow of traffic.

Reachability

Reachability is specified as the relative percentage or the absolute maximum number of unreachable hosts, based on flows per million (fpm), that OER will permit from a traffic class entry. If the absolute number or relative percentage of unreachable hosts is greater than the user-defined or the default value, OER determines that the traffic class entry is out-of-policy and searches for an alternate exit link.

To configure parameters for reachability, use the **unreachable** command. This command has two keywords, **relative** and **threshold**. The **relative** keyword is used to configure the relative percentage of unreachable hosts. The relative unreachable host percentage is based on a comparison of short-term and long-term measurements. The short-term measurement reflects the percentage of hosts that are unreachable within a 5-minute period. The long-term measurement reflects the percentage of unreachable hosts within a 60-minute period. The following formula is used to calculate this value:

Relative percentage of unreachable hosts = ((short-term percentage - long-term percentage) / long-term percentage) * 100

The master controller measures the difference between these two values as a percentage. If the percentage exceeds the user-defined or default value, the traffic class entry is determined to be out-of-policy. For example, if 10 hosts are unreachable during the long-term measurement and 12 hosts are unreachable during short-term measurement, the relative percentage of unreachable hosts is 20 percent.

The **threshold** keyword is used to configure the absolute maximum number of unreachable hosts. The maximum value is based on the actual number of hosts that are unreachable based on fpm.

Delay

Delay (also referred as latency) is defined as the delay between when the packet was sent from the source device and when it arrived at a destination device. Delay can be measured as one-way delay or round-trip delay. The largest contributor to latency is caused by network transmission delay.

In Cisco IOS Release 12.4(6)T, 12.2(33)SRB, and later releases, support was introduced for defining delay performance characteristics with respect to voice traffic. Round-trip delay affects the dynamics of conversation and is used in Mean Opinion Score (MOS) calculations. One-way delay is used for diagnosing network problems. A caller may notice a delay of 200 milliseconds and try to speak just as

the other person is replying because of packet delay. The telephone industry standard specified in ITU-T G.114 recommends the maximum desired one-way delay be no more than 150 milliseconds. Beyond a one-way delay of 150 milliseconds, voice quality is affected. With a round-trip delay of 300 milliseconds or more, users may experience annoying talk-over effects.

Packet Loss

Packet loss can occur due an interface failing, a packet being routed to the wrong destination, or congestion in the network.

Packet loss for voice traffic leads to the degradation of service in which a caller hears the voice sound with breaks. Although average packet loss is low, voice quality may be affected by a short series of lost packets.

Jitter

Support for jitter was introduced in Cisco IOS Release 12.4(6)T, 12.2(33)SRB, and later releases. Jitter means interpacket delay variance. When multiple packets are sent consecutively from source to destination, for example, 10 ms apart, and if the network is behaving ideally, the destination should be receiving them 10 ms apart. But if there are delays in the network (like queuing, arriving through alternate routes, and so on) the arrival delay between packets might be greater than or less than 10 ms. Using this example, a positive jitter value indicates that the packets arrived more than 10 ms apart. If the packets arrive 12 ms apart, then positive jitter is 2 ms; if the packets arrive 8 ms apart, then negative jitter is 2 ms. For delay-sensitive networks like VoIP, both positive and negative jitter values are undesirable; a jitter value of 0 is ideal.

Mean Opinion Score (MOS)

Support for MOS was introduced in Cisco IOS Release 12.4(6)T, 12.2(33)SRB, and later releases. With all the factors affecting voice quality, many people ask how voice quality can be measured. Standards bodies like the ITU have derived two important recommendations: P.800 (MOS) and P.861 (Perceptual Speech Quality Measurement [PSQM]). P.800 is concerned with defining a method to derive a Mean Opinion Score of voice quality. MOS scores range between 1 representing the worst voice quality, and 5 representing the best voice quality. A MOS of 4 is considered "toll-quality" voice.

In Cisco IOS Release 12.4(4)T and prior releases, only reachability, delay, and loss performance characteristics could be used. In Cisco IOS Release 12.4(6)T, 12.2(33)SRB, and later releases, jitter and MOS performance characteristic can be configured in an OER policy as well as delay and packet loss to determine the quality of a phone call over an IP network.

OER Link Policies

OER link policies are a set of rules that are applied against OER-managed external link (an external link is an interface on a border router on the network edge). Link policies define the desired performance characteristics of the links. Instead of defining the performance of an individual traffic class entry that uses the link (as in traffic class performance policies), link policies are concerned with the performance of the link as a whole. In Cisco IOS Release 12.4(6)T and prior releases, link policies are applied only to exit (egress) links, but in Cisco IOS Release 12.4(9)T, 12.2(33)SRB, and later releases, support for selected entrance (ingress) link policies was introduced. The following performance characteristics are managed by link policies:

- Traffic Load (Utilization)
- Range
- Cost

Traffic Load

A traffic load (also referred to as utilization) policy consists of an upper threshold on the amount of traffic that a specific link can carry. Cisco IOS OER supports per traffic class load distribution. Every 20 seconds, by default, the border router reports the link utilization to the master controller, after an external interface is configured for a border router. In Cisco IOS Release 12.4(6)T and prior releases, only exit link traffic load thresholds can be configured as an OER policy, but in Cisco IOS Release 12.4(9)T, 12.2(33)SRB, and later releases, entrance link traffic load thresholds can be configured. If the exit or entrance link utilization is above the configured threshold, or the default threshold of 75 percent, the exit or entrance link is in an OOP state and OER starts the monitoring process to find an alternative link for the traffic class. The link utilization threshold can be manually configured either as an absolute value in kilobytes per second (kbps) or as a percentage. A load utilization policy for an individual interface is configured on the master controller under the border router configuration.

Tip   When configuring load distribution, we recommend that you set the interface load calculation on external interfaces to 30-second intervals with the **load-interval** interface configuration command. The default calculation interval is 300 seconds. The load calculation is configured under interface configuration mode on the border router. This configuration is not required, but it is recommended to allow Cisco IOS OER to respond as quickly as possible to load distribution issues.

Range

A range policy is defined to maintain all links within a certain utilization range, relative to each other in order to ensure that the traffic load is distributed. For example, if a network has multiple exit links, and there is no financial reason to choose one link over another, the optimal choice is to provide an even load distribution across all links. The load-sharing provided by traditional routing protocols is not always evenly distributed, because the load-sharing is flow-based rather than performance- or policy-based. Cisco OER range functionality allows you to configure OER to maintain the traffic utilization on a set of links within a certain percentage range of each other. If the difference between the links becomes too great, OER will attempt to bring the link back to an in-policy state by distributing traffic classes among the available links. The master controller sets the maximum range utilization to 20 percent for all OER-managed links by default, but the utilization range can be configured using a maximum percentage value. In Cisco IOS Release 12.4(6)T and prior releases, only an exit link utilization range can be configured as an OER policy, but in Cisco IOS Release 12.4(9)T, 12.2(33)SRB, and later releases, an entrance link utilization range can be configured.

Cost

OER support for cost-based optimization was introduced in Cisco IOS Release 12.3(14)T and 12.2(33)SRB. Cost-based optimization allow you to configure policies based on the monetary cost (ISP service level agreements [SLAs]) of each exit link in your network. To implement OER cost-based optimization the OER master controller is configured to send traffic over exit links that provide the most cost-effective bandwidth utilization, while still maintaining the desired performance characteristics. Cost-based optimization supports two billing models: fixed-rate billing or tier-based billing.

Fixed-rate billing is used when the ISP bills one flat rate for network access regardless of bandwidth usage. If fixed-rate billing only is configured on the exit links, all exits are considered equal with regard to cost-optimization and other policy parameters (such as delay, loss, and utilization) that are used to determine if the prefix or exit link is in-policy.

If multiple exit links are configured with tiered and fixed policies, then exit links with fixed policies have the highest priority with regard to cost optimization. If the fixed exit links are at maximum utilization, then the tiered exit links will be used.

Tier-based billing is used when the ISP bills at a tiered rate based on the percentage of exit link utilization. Each cost tier is configured separately with an associated monetary cost and a percentage of bandwidth utilization that activates the tier is defined. An allowance is made for bursting in the algorithm used to determine the tier-based billing. Bursting is defined as short periods of high bandwidth usage that would be expensive under fixed-rate billing.

The specific details of tier-based billing models vary by ISP. However, most ISPs use some variation of the following algorithm to calculate what an enterprise should pay in a tiered billing plan:

- Gather periodic measurements of egress and ingress traffic carried on the enterprise connection to the ISP network and aggregate the measurements to generate a rollup value for a rollup period.

- Generate one or more rollup values per billing period.

- Rank the rollup values for the billing period into a stack from the largest value to the smallest.

- Discard the top 5 percent of the rollup values from the stack to accommodate bursting.

- Apply the highest remaining rollup value in the stack to a tiered structure to determine a tier associated with the rollup value.

- Charge the customer based on a set cost associated with the determined tier.

Note A billing policy must be configured and applied to prefixes in order for the master controller to perform cost-based optimization.

At the end of each billing cycle the top n percent of samples, or rollup values, are discarded. The remaining highest value is the sustained utilization. Based on the number of samples discarded, the billing cycle is divided into three periods: the initial period, the middle period, and the last period.

The initial period is when the number of samples measured is less than the number of discards +1. For example, if the discard percentage is 7 percent, billing month is 30 days long, and sample period is 24 hours, then there are 30 samples at the end of the month. The number of discard samples is two (7 percent of 30). In this case, days one, two, and three are in the initial period. During this period, target the lowest tier for each ISP at the start of each respective billing period and "walk up" the tiers until the current total amount of traffic is allocated across the links.

The middle period is after the initial period until the number of samples yet to be measured or collected is less than the number of discards. Using the same example as before, the middle period occurs from day four through day 28. During this period, set the target tier to the sustained utilization tier, which is the tier in which (discard +1) the highest sample so far measured falls.

The period after the middle period until the end of billing period is the last period. During this period, if you used links at the maximum link capacity for the remainder of the billing period and sustained utilization did not change, then set the target to the maximum allowable link utilization. Maximum link utilization is configurable where most likely values are 75 to 90 percent. Otherwise, set the target to sustained utilization tier.

During any sample period, if the cumulative usage is more than targeted cumulative usage, then bump up to the next tier for the remainder of sample period. If rollup is enabled, then replace the sample values with rollup values, and replace the number of samples with the number of rollups in the cost optimization algorithm.

Performance Routing Link Grouping

In Cisco IOS Release 12.4(15)T the ability to define a group of exit links as a preferred set of links, or a fallback set of links for OER to use when optimizing traffic classes specified in an OER policy, was introduced. OER currently selects the best link for a traffic class based on the preferences specified in a policy and the traffic class performance—using parameters such as reachability, delay, loss, jitter or MOS—on a path out of the specified link. Bandwidth utilization, cost, and the range of links can also be considered in selecting the best link. Link grouping introduces a method of specifying preferred links for one or more traffic classes in an OER policy so that the traffic classes are routed through the best link from a list of preferred links, referred to as the primary link group. A fallback link group can also be specified in case there are no links in the primary group that satisfy the specified policy and performance requirements. If no primary group links are available, the traffic classes are routed through the best link from the fallback group. To identify the best exit, OER probes links from both the primary and fallback groups.

Primary and fallback link groups can be configured at the master controller and are identified using a unique name. Link groups provide a method of grouping links such as high bandwidth links to be used, for example, by video traffic, by configuring an OER policy to specify that the best link is to be selected from the link group that consists of only high bandwidth links. The traffic classes specified in a policy can be configured with only one primary link group and one fallback link group. The priority of a link group can vary between policies, a link group might be a primary link group for one policy, and a fallback link group for another policy.

See Figure 3 for an example of how to implement link grouping. Three link groups, ISP1, ISP2, and ISP3 represent different Internet Service Providers (ISPs) and all three ISPs have links to interfaces on the three border routers shown in Figure 3. ISP1 links are the most expensive links, but they have the best Service Level Agreement (SLA) guarantees. ISP3 links are best effort links, and these links are the cheapest links. ISP2 links are not as good as the ISP1 links, but the ISP2 links are more reliable than the ISP3 links. The cost of the ISP2 links is higher than the ISP3 links, but lower than ISP1 links. In this situation, each ISP is created as a link group and associated with an interface on each border router shown in Figure 3.

Figure 3   Link Group Diagram
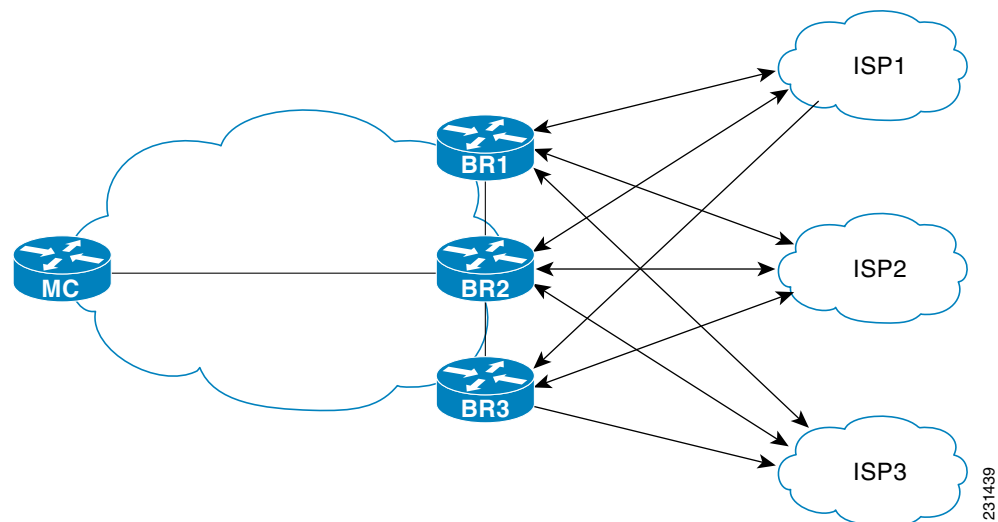
Assuming four types of traffic class, video, voice, FTP, and data, each traffic class can be routed through a border router interface belonging to an appropriate link group. Video and voice traffic classes need the best links so the ISP1 link group is configured as the primary link group, with ISP2 as the fallback group. FTP traffic needs reliable links but the cost might be a factor so ISP2 is assigned as the primary group, and ISP3 is the fallback link group. Note that although ISP1 provides the most reliable links, it may be too expensive for file transfer traffic. For data traffic, ISP3 is a good choice as a primary link group, with ISP2 as the fallback group.

Spillover

Performance routing link groups can be used to support spillover. Spillover is when there are two paths through the network—traffic engineering (TE) tunnels, for example—to the same provider edge (PE) router, but the tunnels take different paths across the network and the traffic is sent through one tunnel until it reaches a traffic load threshold when it spills over to the second tunnel. Using OER link groups one tunnel is created as a primary link group and the second tunnel is the fallback link group. When the first tunnel goes out of policy, OER switches to the fallback tunnel link group, which provides the spillover capacity until the traffic load on the first tunnel drops below the threshold. The tunnels must be established before the OER link groups are configured.

OER Network Security Policies

The ability to configure network security policies either to prevent unauthorized use of the network or to mitigate attacks inside and outside the network was introduced in Cisco IOS Release 12.4(6)T and 12.2(33)SRB. You can configure OER to use black hole or sinkhole routing techniques to limit the impact of attacks against your network. Black hole routing refers to the process of forwarding packets to a null interface, meaning that the packets are dropped into a "black hole." Sinkhole routing directs packets to a next hop where the packets can be stored, analyzed, or dropped. Another term for sinkhole routing is honey-pot routing.

OER Policy Operational Options and Parameters

In addition to the specific types of OER policies, there are some OER policy operational parameters or options that can be configured. The operational parameters are timers and the operational options consist of different operational modes. For more details, see the following sections:

OER Timers Parameters

Three types of timers can be configured as OER policy operational parameters:

Backoff Timer

The backoff timer is used to adjust the transition period that the master controller holds an out-of-policy traffic class entry. The master controller waits for the transition period before making an attempt to find an in-policy exit. A minimum, a maximum, and an optional step timer value can be configured.

Holddown Timer

The holddown timer is used to configure the traffic class entry route dampening timer to set the minimum period of time that a new exit must be used before an alternate exit can be selected. To prevent the traffic class entry from flapping because of rapid state changes, the master controller does not move the traffic class entry to a different exit even if it goes out-of-policy during the holddown timer period. OER does not implement policy changes while a traffic class entry is in the holddown state. A traffic class entry will remain in a holddown state for the default or configured time period. When the holddown timer expires, OER will select the best exit based on performance and policy configuration. However, an immediate route change will be triggered if the current exit for a traffic class entry becomes unreachable.

Periodic Timer

The periodic timer is used to find a better path for a traffic class entry, even if the traffic class entry is in-policy on the current exit. When the periodic timer expires, the master controller evaluates current exit links for the traffic class entry and, if a better exit exists based on the current measurements and priorities, the traffic class entry is moved to a new in-policy exit link.

When adjusting OER timers note that a newly configured timer setting will immediately replace the existing setting if the value of the new setting is less than the time remaining. If the value is greater than the time remaining, the new setting will be applied when the existing timer expires or is reset.

Note   Overly aggressive timer settings can keep an exit link or traffic class entry in an out-of-policy state.

OER Mode Options

Three types of mode options can be configured as OER policy operational options:

- Mode Monitor, page 11
- Mode Route, page 11
- Mode Select-Exit, page 12

Mode Monitor

The mode monitor option enables the configuration of OER monitoring settings. Monitoring is defined here as the act of measurement performed periodically over a set interval of time where the measurements are compared against a threshold. OER measures the performance of traffic classes using active and passive monitoring techniques but it also measures, by default, the utilization of exit links. For more details about mode monitoring options, see the "Measuring the Traffic Class Performance and Link Utilization Using OER" module.

Mode Route

The mode route option specifies one of three OER route control policy settings. Mode route control enables OER to control routes automatically, mode route metric specifies OER route protocol-related settings, and mode route observe offers route control advice, but does not take any action. Observe mode monitoring is enabled by default when OER is enabled. In observe mode, the master controller monitors traffic classes and exit links based on default and user-defined policies and then reports the status of the network and the decisions that should be made but does not implement any changes. Observe mode is used to verify the effect of OER features before OER is actively deployed on your network. For more details about the mode route control and mode route metric options, see the "Using OER to Control the Traffic Classes and Verify the Network Performance" module.

Mode Select-Exit

The mode select-exit option enables the exit selection settings. The definition of an in-policy traffic class entry is that the measured performance metrics are do not exceed a default or configured threshold while the traffic class traffic is on the current path. In this situation, OER does not search for an alternate exit link because the current network path keeps the traffic class entry in-policy. This type of configuration would be activated by using the **mode select-link good** command which is the default if the **mode** command is not specified. There are other deployment scenarios, where OER selects the best performance path. This type of configuration can be activated by using the **mode select-link best** command. In this type of situation, OER measures alternate path performance metrics while the traffic class entry is in-policy on the current path. OER moves the current path if a better performance path is found. After the first selection of the best path, however, OER does not initiate another search unless the periodic timer is configured. When the periodic timer expires, the master controller evaluates current exit links for the traffic class entry and, if a better exit exists based on the current measurements and priorities, the traffic class entry is moved to a new in-policy exit link. Use the periodic timer with the **mode select-link best** command if you have a deployment scenario where you need OER to select the best performance path at any given time.

There is one further use of the mode select-exit option. If OER does not find an in-policy exit for a traffic class entry when the **mode select-link good** command is operational, OER transitions the traffic class entry to an uncontrolled state. If OER does not find an in-policy exit for a traffic class entry when the **mode select-link best** command is operational, OER selects the best of the OOP exit links for the traffic class entry.

OER Policy Application

OER policies can be applied to learned or configured traffic classes. OER policies can be applied on a global basis when the policy is configured directly under OER master controller configuration mode. All traffic classes inherit global policies. If, however, you want to apply a policy to a subset of the traffic classes, then a specific policy can be configured. A specific OER policy applies only to the specific traffic classes that match a prefix list or access list. Specific policies inherit global policies unless the same policy is overwritten by the specific policy. In Cisco IOS Release 12.4(6)T and earlier releases, OER policies applied only to prefixes, but in Cisco IOS Release 12.4(9)T, 12.2(33)SRB, and later releases, OER policies can apply to traffic classes that define an application traffic class and may include prefixes, protocols, port numbers, and DSCP values. To apply specific policies to learned or configured traffic classes, OER map configuration is used.

OER Map Configuration for OER Policies

An OER map may appear to be similar to a route map but there are significant differences. An OER map is designed to select learned or configured traffic classes using a match clause and then to apply OER policy configurations using a set clause. The OER map can be optionally configured with a sequence number like a route map, but only the OER map with the lowest sequence number is evaluated. The operation of an OER map differs from a route map at this point. There are two important distinctions:

- Only a single match clause may be configured for each sequence. An error message will be displayed on the console if you attempt to configure multiple match clauses for a single OER map sequence.

- An OER map is not configured with permit or deny statements. However, a permit or deny sequence can be configured for an IP traffic flow by configuring a permit or deny statement in an IP prefix list and then applying the prefix list to the OER map.

The OER map applies the configuration of the set clause after a successful match occurs. An OER set clause can be used to set policy parameters such as the backoff timer, packet delay, holddown timer, packet loss, mode settings, periodic timer, resolve settings, unreachable hosts, and traceroute reporting.

Policies applied by an OER map take effect immediately. The OER map configuration can be viewed in the output of the **show running-config** command. OER policy configuration can be viewed in the output of the **show oer master policy** command. These policies are applied only to traffic classes that match or pass through the OER map.

Policy Rules Configuration to Apply an OER Policy

The **policy-rules** OER master controller configuration command was introduced in Cisco IOS Release 12.3(11)T, 12.2(33)SRB, and later releases. This command allows you to select an OER map using a sequence number and apply the configuration under OER master controller configuration mode, providing an improved method to switch between predefined OER maps. Only one OER map is used at a time for policy configuration, but many OER maps can be defined. In Cisco IOS Release 12.3(8)T, only one OER map could be defined to apply a policy to traffic classes.

Priority Resolution for Multiple OER Policies

When configuring multiple policy criteria for a single traffic class entry, or a set of traffic classes, it is possible to have multiple overlapping policies. To resolve the potential conflict of which policy to run, OER uses its resolve function: a flexible mechanism that allows you to set the priority for an OER policy. Each policy is assigned a unique value, and the policy with the lowest value is selected as the highest priority policy. By default, OER assigns the highest priority to delay policies, followed by utilization policies. Assigning a priority value to any policy will override the default settings. To configure the policy conflict resolution, use the **resolve** command in OER master controller configuration mode, or the **set resolve** command in OER map configuration mode.

Variance Setting for OER Policy Conflict Resolution

When configuring OER resolve settings, you can also set an allowable variance for the defined policy. Variance configures the average delay, as a percentage, that all traffic classes for one exit, or the specific policy traffic classes for an exit, can vary from the defined policy value and still be considered equivalent. For example, if the delay on the best exit link (best exit in terms of delay) for a traffic class entry is 80 milliseconds (ms) and a 10 percent variance is configured, then any other exit links with a delay between 80 and 88 ms for the same traffic class entry are considered equivalent to the best exit link.

To illustrate how variance is used by OER consider three exit links with the following performance values for delay and jitter for a traffic class entry:

- Exit A—Delay is 80 ms, jitter is 3ms
- Exit B—Delay is 85 ms, jitter is 1ms
- Exit C—Delay is 100 ms, jitter is 5ms

The following OER policy conflict resolution is configured and applied to the traffic class entry:

```
delay priority 1 variance 10
jitter priority 2 variance 10
```

OER determines the best exit by looking at the policy with the lowest priority value, which in this example is the delay policy. Exit A has the lowest delay value, but Exit B has a delay value of 85 which is within a 10 percent variance of the delay value at Exit A. Exit A and Exit B can therefore be considered equal in terms of delay values. Exit C is now eliminated because the delay values are too high. The next priority policy is jitter, and Exit B has the lowest jitter value. OER will select Exit B as the only best exit for the traffic class entry because Exit A has a jitter value that is not within 10 percent variance of the Exit B jitter value.

> **Note** Variance cannot be configured for cost or range policies.

How to Configure and Apply OER Policies

This section contains the following optional tasks:

Configuring and Applying an OER Policy to Learned Traffic Classes

Perform this task at the master controller to configure and apply an OER policy to learned traffic classes. After configuring the router as an OER master controller using the **oer master** command, most of the commands in this task are all optional. Each step configures a performance policy that applies to learned traffic classes on a global basis. In this example, OER is configured to select the first in-policy exit.

Cisco IOS OER Timers Adjustments

When adjusting OER timers note that a newly configured timer setting will immediately replace the existing setting if the value of the new setting is less than the time remaining. If the value is greater than the time remaining, the new setting will be applied when the existing timer expires or is reset.

> **Note** Overly aggressive timer settings can keep an exit link or traffic class entry in an out-of-policy state.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **oer master**
4. **backoff** *min-timer max-timer* [*step-timer*]
5. **delay** {**relative** *percentage* | **threshold** *maximum*}

6. **holddown** *timer*

7. **loss** {**relative** *average* | **threshold** *maximum*}

8. **periodic** *timer*

9. **unreachable** {**relative** *average* | **threshold** *maximum*}

10. **mode select-exit** {**best** | **good**}

11. **end**

12. **show oer master policy** [*sequence-number* | *policy-name* | **default**]

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		
		• Enter your password if prompted.

Step 2	`configure terminal`
	
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`oer master`
	
	Example:
	`Router(config)# oer master`
		Enters OER master controller configuration mode.

Step 4	`backoff` *min-timer max-timer* [*step-timer*] **Example:** `Router(config-oer-mc)# backoff 400 4000 400`	(Optional) Sets the backoff timer to adjust the time period for policy decisions. • The *min-timer* argument is used to set the minimum transition period in seconds. • The *max-timer* argument is used to set the maximum length of time OER holds an out-of-policy traffic class entry when there are no links that meet the policy requirements of the traffic class entry. • The *step-timer* argument allows you to optionally configure OER to add time each time the minimum timer expires until the maximum time limit has been reached.

	Command or Action	Purpose
Step 5	**delay** {**relative** *percentage* | **threshold** *maximum*} **Example:** Router(config-oer-mc)# delay relative 80	(Optional) Sets the delay threshold as a relative percentage or as an absolute value. • The **relative** keyword is used to configure a relative delay percentage. The relative delay percentage is based on a comparison of short-term and long-term measurements. • The **threshold** keyword is used to configure the absolute maximum delay period in milliseconds. • If the configured delay threshold is exceeded, then the prefix is out-of-policy. • The example sets a delay threshold of 80 percent based on a relative average.
Step 6	**holddown** *timer* **Example:** Router(config-oer-mc)# holddown 600	(Optional) Configures the traffic class entry route dampening timer to set the minimum period of time that a new exit must be used before an alternate exit can be selected. • OER does not implement route changes while a traffic class entry is in the holddown state. • When the holddown timer expires, OER will select the best exit based on performance and policy configuration. • OER starts the process of finding an alternate path if the current exit for a traffic class entry becomes unreachable. • The example sets the traffic class entry route dampening timer to 600 seconds.
Step 7	**loss** {**relative** *average* | **threshold** *maximum*} **Example:** Router(config-oer-mc)# loss relative 20	(Optional) Sets the relative or maximum packet loss limit that OER will permit for a traffic class entry. • The **relative** keyword sets a relative percentage of packet loss based on a comparison of short-term and long-term packet loss percentages. • The **threshold** keyword sets the absolute packet loss based on packets per million. • The example configures the master controller to search for a new exit link when the relative percentage of packet loss is equal to or greater than 20 percent.

	Command or Action	Purpose
Step 8	**periodic** *timer* **Example:** `Router(config-oer-mc)# periodic 300`	(Optional) Configures OER to periodically select the best exit link when the periodic timer expires. • When this command is enabled, the master controller will periodically evaluate and then make policy decisions for traffic classes. • The example sets the periodic timer to 300 seconds. When the timer expires, OER will select either the best exit or the first in-policy exit. **Note** The **mode select-exit** command is used to determine if OER selects the first in-policy exit or the best available exit when this timer expires. For more details, see the *"OER Mode Options" section on page 11.*
Step 9	**unreachable** {**relative** *average* | **threshold** *maximum*} **Example:** `Router(config-oer-mc)# unreachable relative 10`	(Optional) Sets the maximum number of unreachable hosts. • This command is used to specify the relative percentage or the absolute maximum number of unreachable hosts, based on flows per million (fpm), that OER will permit for a traffic class entry. If the absolute number or relative percentage of unreachable hosts is greater than the user-defined or the default value, OER determines that the traffic class entry is OOP and searches for an alternate exit link. • The **relative** keyword is used to configure the relative percentage of unreachable hosts. The relative unreachable host percentage is based on a comparison of short-term and long-term measurements. • The **threshold** keyword is used to configure the absolute maximum number of unreachable hosts based on fpm. • The example configures OER to search for a new exit link for a traffic class entry when the relative percentage of unreachable hosts is equal to or greater than 10 percent.
Step 10	**mode select-exit** {**best** | **good**}} **Example:** `Router(config-oer-mc)# mode select-exit good`	Enables the exit link selection based on performance or policy. • The **select-exit** keyword is used to configure the master controller to select either the best available exit when the **best** keyword is entered or the first in-policy exit when the **good** keyword is entered. **Note** Only the syntax that is applicable to this task is displayed. For more details, see the *Cisco IOS Optimized Edge Routing Command Reference*, Release 12.4T.

	Command or Action	Purpose
Step 11	**end** **Example:** `Router(config-oer-mc)# end`	Exits OER master controller configuration mode and enters privileged EXEC mode.
Step 12	**show oer master policy** [*sequence-number* | *policy-name* | **default**] **Example:** `Router# show oer master policy`	Displays policy settings on an OER master controller. • The output of this command displays default policies and, optionally, policies configured with an OER map. • The *sequence-number* argument is used to display policy settings for the specified OER map sequence. • The *policy-name* argument is used to display policy settings for the specified OER policy map name. • The **default** keyword is used to display only the default policy settings. • The example displays the default policy settings and policy settings updated by the configuration in this task.

Examples

This example shows output from the **show oer master policy** command. Default policy settings are displayed except where the configuration in this task has overwritten specific policy settings.

```
Router# show oer master policy

Default Policy Settings:
  backoff 400 4000 400
  delay relative 80
  holddown 600
  periodic 300
  probe frequency 56
  mode route observe
  mode monitor both
  mode select-exit good
  loss relative 20
  unreachable relative 10
  resolve delay priority 11 variance 20
  resolve utilization priority 12 variance 20
 *tag 0
```

Configuring and Applying an OER Policy to Configured Traffic Classes

Perform this task at the master controller to configure and apply an OER policy to specified configured traffic classes. This task contains two targeted policies that work differently for different traffic class entries from the MTC list. The policies are configured using an OER map. This task contains both prefix list and access list configuration with different criteria in the set clauses. OER timers are also modified in this OER map configuration.

Note   Policies applied in an OER map can override global policy configurations.

Cisco IOS OER Timers Adjustments

When adjusting OER timers note that a newly configured timer setting will immediately replace the existing setting if the value of the new setting is less than the time remaining. If the value is greater than the time remaining, the new setting will be applied when the existing timer expires or is reset.

Note Overly aggressive timer settings can keep an exit link or prefix in an out-of-policy state.

Prefix List Use with OER

IP prefix lists are used to manually select prefixes for OER monitoring and the prefix list syntax operates in a slightly different way with OER than in regular routing. The **ge** keyword is not used and the **le** keyword is used by OER to specify two types of prefixes: exact prefixes, and inclusive prefixes.

A master controller can monitor and control an exact prefix of any length including the default route. If an exact prefix is specified, OER monitors only the exact prefix.

A master controller can monitor and control an inclusive prefix using the **le** keyword and the *le-value* argument set to 32. OER monitors the configured prefix and any more specific prefixes (for example, configuring the 10.0.0.0/8 le 32 prefix would include the 10.1.0.0/16 and the 10.1.1.0/24 prefixes) over the same exit and records the information in the routing information base (RIB).

Note Use the inclusive prefix option with caution in a typical OER deployment because of the potential increase in the amount of prefixes being monitored and recorded.

Prerequisites

This task requires the master controller and border routers to be running Cisco IOS Release 12.4(6)T, 12.2(33)SRB, or later releases.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*} [**le** *le-value*]
4. **ip access list** {**standard** | **extended**} *access-list-name*
5. [*sequence-number*] **permit udp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**dscp** *dscp-value*] [
6. **exit**
7. **oer-map** *map-name sequence-number*
8. **match ip address prefix-list** *prefix-list-name*
9. **set backoff** *min-timer max-timer* [*step-timer*]
10. **set delay** {**relative** *percentage* | **threshold** *maximum*}
11. **set loss** {**relative** *average* | **threshold** *maximum*}
12. **set periodic** *timer*
13. **set unreachable** {**relative** *average* | **threshold** *maximum*}

14. **exit**

15. **oer-map** *map-name sequence-number*

16. **match ip address** {**access-list** *access-list-name* | **prefix-list** *prefix-list-name*}

17. **set active probe** *probe-type ip-address* [**target-port** *number*] [**codec** *codec-name*]

18. **set probe frequency** *seconds*

19. **set jitter threshold** *maximum*

20. **set mos threshold** *minimum* **percent** *percent*

21. **set mode select-exit** {**best** | **good**}

22. **end**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		
		• Enter your password if prompted.

Step 2	`configure terminal`
	
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`ip prefix-list` *list-name* [`seq` *seq-value*] {`deny` *network***/***length* | `permit` *network***/***length*} [`le` *le-value*] **Example:** `Router(config)# ip prefix-list OER seq 10 permit 10.4.9.0/24`	Creates an IP prefix list. • IP prefix lists are used to manually select prefixes for monitoring by the master controller. • A master controller can monitor and control an exact prefix of any length including the default route. If an exact prefix is specified, OER monitors only the exact prefix. • A master controller can monitor and control an inclusive prefix using the **le** keyword set to 32. OER monitors the configured prefix and any more specific prefixes (for example, configuring the 10.0.0.0/8 le 32 prefix would include the 10.1.0.0/16 and the 10.1.1.0/24 prefixes) over the same exit and records the information in the routing information base (RIB). • The prefixes specified in the IP prefix list are imported into the OER map with the **match ip address** (OER) command. • The example creates an exact IP prefix list that permits prefixes only from the 10.4.9.0/24 subnet. **Note** Only the syntax applicable to OER is shown. For more details, see the *Cisco IOS IP Routing Protocols Command Reference*, Release 12.4T.

	Command or Action	Purpose
Step 4	`ip access-list {`**`standard`** `	` **`extended`**`}` *`access-list-name`*    **Example:**   `Router(config)# ip access-list extended VOICE_ACCESS_LIST`	Defines an IP access list by name. • OER supports only named access lists. • The example creates an extended IP access list named VOICE_ACCESS_LIST.

Step 5	`[`*`sequence-number`*`]` **`permit udp`** *`source source-wildcard`* `[`*`operator`* `[`*`port`*`]]` *`destination destination-wildcard`* `[`*`operator`* `[`*`port`*`]]` `[`**`dscp`** *`dscp-value`*`]`
	
	 Example:
	 `Router(config-ext-nacl)# permit udp any range 16384 32767 10.20.20.0 0.0.0.15 range 16384 32767`
		Sets conditions to allow a packet to pass a named IP access list.
		
		 • The example is configured to identify all UDP traffic ranging from a destination port number of 16384 to 32767 from any source to a destination prefix of 10.20.20.0/24. This specific UDP traffic is to be optimized.
		
		 Note Only the syntax applicable to this task is shown. For more details, see the *Cisco IOS IP Application Services Command Reference*, Release 12.4T.

Step 6	**`exit`** **Example:** `Router(config-ext-nacl)# exit`	Exits extended access list configuration mode and returns to global configuration mode.
Step 7	**`oer-map`** *`map-name sequence-number`* **Example:** `Router(config)# oer-map FINANCE 10`	Enters OER map configuration mode to configure an OER map to apply policies to selected IP prefixes. • Only one match clause can be configured for each OER map sequence. • Permit sequences are first defined in an IP prefix list and then applied with the **match ip address** (OER) command in Step 8. • The example creates an OER map named FINANCE.
Step 8	**`match ip address {`**`access-list`** *`access-list-name`* `	` **`prefix-list`** *`prefix-list-name`*`}`    **Example:**   `Router(config-oer-map)# match ip address prefix-list OER`	References an extended IP access list or IP prefix list as match criteria in an OER map. • Only a single match clause can be configured for each OER map sequence. • The example configures the prefix list named OER as match criteria in an OER map.

	Command or Action	Purpose
Step 9	**set backoff** *min-timer max-timer* [*step-timer*] **Example:** Router(config-oer-map)# set backoff 400 4000 400	Creates a set clause entry to configure the backoff timer to adjust the time period for traffic class entry policy decisions. • The *min-timer* argument is used to set the minimum transition period in seconds. • The *max-timer* argument is used to set the maximum length of time OER holds an out-of-policy traffic class entry when there are no OER controlled in-policy traffic classes. • The *step-timer* argument allows you to optionally configure OER to add time each time the minimum timer expires until the maximum time limit has been reached. • The example creates a set clause to configure the minimum timer to 400 seconds, the maximum timer to 4000 seconds, and the step timer to 400 seconds for traffic that is matched in the same OER map sequence.
Step 10	**set delay** {**relative** *percentage* | **threshold** *maximum*} **Example:** Router(config-oer-map)# set delay threshold 2000	Creates a set clause entry to configure the delay threshold. • The delay threshold can be configured as a relative percentage or as an absolute value for match criteria. • The **relative** keyword is used to configure a relative delay percentage. The relative delay percentage is based on a comparison of short-term and long-term measurements. • The **threshold** keyword is used to configure the absolute maximum delay period in milliseconds. • The example creates a set clause that sets the absolute maximum delay threshold to 2000 milliseconds for traffic that is matched in the same OER map sequence.

	Command or Action	Purpose

Step 11	`set loss {`**`relative`** `average |` **`threshold`** `maximum}`
	
	Example:
	`Router(config-oer-map)# set loss relative 20`
		Creates a set clause entry to configure the relative or maximum packet loss limit that the master controller will permit for an exit link.
		
		• This command is used within an OER map to configure the relative percentage or maximum number of packets that OER will permit to be lost during transmission on an exit link. If packet loss is greater than the user-defined or the default value, the master controller determines that the exit link is out-of-policy.
		
		• The **relative** keyword is used to configure the relative packet loss percentage. The relative packet loss percentage is based on a comparison of short-term and long-term packet loss.
		
		• The **threshold** keyword is used to configure the absolute maximum packet loss. The maximum value is based on the actual number of packets per million that have been lost.
		
		• The example creates a set clause that configures the relative percentage of acceptable packet loss to less than 20 percent for traffic that is matched in the same OER map sequence.

Step 12	`set periodic timer`
	
	Example:
	`Router(config-oer-map)# set periodic 300`
		Creates a set clause entry to configure the time period for the periodic timer.
		
		• When this command is enabled, the master controller will periodically evaluate and then make policy decisions for traffic classes, even if they are currently in-policy.
		
		• The **set mode select-exit** command in Step 21 is used to determine if OER selects the first in-policy exit or the best available exit when this timer expires.
		
		• The example creates a set clause that configures the periodic timer to 300 seconds for traffic that is matched in the same OER map sequence.

	Command or Action	Purpose
Step 13	**set unreachable** {**relative** *average* | **threshold** *maximum*} **Example:** Router(config-oer-map)# set unreachable relative 10	Creates a set clause entry to configure the maximum number of unreachable hosts. • This command is used to specify the relative percentage or the absolute maximum number of unreachable hosts, based on flows per million (fpm), that OER will permit for a traffic class entry. If the absolute number or relative percentage of unreachable hosts is greater than the user-defined or the default value, OER determines that the traffic class entry is OOP and searches for an alternate exit link. • The **relative** keyword is used to configure the relative percentage of unreachable hosts. The relative unreachable host percentage is based on a comparison of short-term and long-term measurements. • The **threshold** keyword is used to configure the absolute maximum number of unreachable hosts based on fpm. • The example creates a set clause entry that configures the master controller to search for a new exit link for a traffic class entry when the relative percentage of unreachable hosts is equal to or greater than 10 percent for traffic learned based on highest delay.
Step 14	**exit** **Example:** Router(config-oer-map)# exit	(Optional) Exits OER map configuration mode and returns to global configuration mode.
Step 15	**oer-map** *map-name sequence-number* **Example:** Router(config)# oer-map VOICE_MAP 10	Enters OER map configuration mode to configure an OER map to apply policies to selected IP traffic classes. • Only one match clause can be configured for each OER map sequence. • Deny sequences are first defined in an IP prefix list and then applied with the **match ip address** (OER) command in Step 16. • The example creates an OER map named VOICE_MAP.
Step 16	**match ip address** {**access-list** *access-list-name* | **prefix-list** *prefix-list-name*} **Example:** Router(config-oer-map)# match ip address access-list VOICE_ACCESS_LIST	References an extended IP access list or IP prefix list as match criteria in an OER map. • Only a single match clause can be configured for each OER map sequence. • The example configures the IP access list named VOICE_ACCESS_LIST as match criteria in an OER map.

	Command or Action	Purpose
Step 17	`set active-probe` *probe-type ip-address* [`target-port` *number*] [`codec` *codec-name*] **Example:** `Router(config-oer-map)# set active-probe jitter 10.20.22.1 target-port 2000 codec g729a`	Creates a set clause entry to assign a target prefix for an active probe. • The **echo** keyword is used to specify the target IP address of a prefix to actively monitor using Internet Control Message Protocol (ICMP) echo (ping) messages. • The **jitter** keyword is used to specify the target IP address of a prefix to actively monitor using jitter messages. • The **tcp-conn** keyword is used to specify the target IP address of a prefix to actively monitor using Internet Control Message Protocol (ICMP) echo (ping) messages. • The **udp-echo** keyword is used to specify the target IP address of a prefix to actively monitor using Internet Control Message Protocol (ICMP) echo (ping) messages. • The example creates a set clause entry to specify the target IP address of a prefix and a specific port number to actively monitor using jitter.
Step 18	`set probe frequency` *seconds* **Example:** `Router(config-oer-map)# set probe frequency 10`	Creates a set clause entry to set the frequency of the OER active probe. • The *seconds* argument is used to set the time, in seconds, between the active probe monitoring of the specified IP prefixes. • The example creates a set clause to set the active probe frequency to 10 seconds.
Step 19	`set jitter threshold` *maximum* **Example:** `Router(config-oer-map)# set jitter threshold 20`	Creates a set clause entry to configure the jitter threshold value. • The **threshold** keyword is used to configure the maximum jitter value, in milliseconds. • The example creates a set clause that sets the jitter threshold value to 20 for traffic that is matched in the same OER map sequence.

Command or Action	Purpose
Step 20 **set mos** {**threshold** *minimum* **percent** *percent*} **Example:** `Router(config-oer-map)# set mos threshold 4.0 percent 30`	Creates a set clause entry to configure the MOS threshold and percentage values used to decide whether an alternate exit is be selected. • The **threshold** keyword is used to configure the minimum MOS value. • The **percent** keyword is used to configure the percentage of MOS values that are below the MOS threshold. • OER calculates the percentage of MOS values below the MOS threshold that are recorded in a five-minute period. If the percentage value exceeds the configured percent value or the default value, the master controller searches for alternate exit links. • The example creates a set clause that sets the threshold MOS value to 4.0 and the percent value to 30 percent for traffic that is matched in the same OER map sequence.
Step 21 **set mode select-exit** {**best** | **good**} **Example:** `Router(config-oer-map)# set mode select-exit best`	Creates a set clause entry to configure monitoring, control, or exit selection settings for matched traffic. • The **select-exit** keyword is used to configure the master controller to select either the best available exit when the **best** keyword is entered or the first in-policy exit when the **good** keyword is entered.
Step 22 **end** **Example:** `Router(config-oer-map)# end`	Exits OER map configuration mode and enters privileged EXEC mode.

Preventing OER Optimization of Learned Prefixes

Perform this task at the master controller to configure and apply an OER policy to prevent OER from attempting to optimize specified learned prefixes. This task is useful when you know a few prefixes that you want to exclude from the OER optimization, but these prefixes will be learned automatically by OER. In this task, an IP prefix list is configured with two entries for different prefixes that are not to be optimized. An OER map is configured with two entries in a sequence that will prevent OER from optimizing the prefixes specified in the prefix list, although the prefixes may be learned. If the sequence numbers of the OER map entries are reversed, OER will learn and attempt to optimize the prefixes.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* \| **permit** *network/length*} [**le** *le-value*]
4. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* \| **permit** *network/length*} [**le** *le-value*]
5. **oer-map** *map-name sequence-number*

6. **match ip address prefix-list** *prefix-list-name*

7. **oer-map** *map-name sequence-number*

8. **match oer learn** {**delay** | **inside** | **throughput**}

9. **end**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		
		• Enter your password if prompted.

Step 2	`configure terminal`
	
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`ip prefix-list` *list-name* [`seq` *seq-value*] {`deny` *network*`/`*length* | `permit` *network*`/`*length*} [`le` *le-value*] **Example:** `Router(config)# ip prefix-list DENY_LIST deny 10.1.1.0/24`	Creates an IP prefix list. • IP prefix lists are used to manually deny or permit prefixes for monitoring by the master controller. • The prefixes specified in the IP prefix list are imported into the OER map with the **match ip address** (OER) command. • The example creates an IP prefix list with an entry that denies prefixes only from the 10.1.1.0/24 subnet. **Note** Only the syntax applicable to OER is shown. For more details, see the *Cisco IOS IP Routing Protocols Command Reference*, Release 12.4T.
Step 4	`ip prefix-list` *list-name* [`seq` *seq-value*] {`deny` *network*`/`*length* | `permit` *network*`/`*length*} [`le` *le-value*] **Example:** `Router(config)# ip prefix-list DENY_LIST deny 172.20.1.0/24`	Creates an IP prefix list. • IP prefix lists are used to manually deny or permit prefixes for monitoring by the master controller. • The prefixes specified in the IP prefix list are imported into the OER map with the **match ip address** (OER) command. • The example creates an IP prefix entry that denies prefixes only from the 172.20.1.0/24 subnet. **Note** Only the syntax applicable to OER is shown. For more details, see the *Cisco IOS IP Routing Protocols Command Reference*, Release 12.4T.

	Command or Action	Purpose
Step 5	**oer-map** *map-name sequence-number* **Example:** Router(config)# oer-map DENY_MAP 10	Enters OER map configuration mode to configure an OER map to apply policies to selected IP prefixes. • Only one match clause can be configured for each OER map sequence. • Deny sequences are first defined in an IP prefix list and then applied with the **match ip address** (OER) command in Step 6. • The example creates an OER map named DENY_MAP with a sequence number of 10.
Step 6	**match ip address** {**access-list** *access-list-name* | **prefix-list** *prefix-list-name*} **Example:** Router(config-oer-map)# match ip address prefix-list DENY_LIST	References an extended IP access list or IP prefix list as match criteria in an OER map. • Only a single match clause can be configured for each OER map sequence. • The example configures the prefix list named OER as match criteria in an OER map.
Step 7	**exit** **Example:** Router(config-oer-map)# exit	Exits OER map configuration mode and returns to global configuration mode.
Step 8	**oer-map** *map-name sequence-number* **Example:** Router(config)# oer-map DENY_MAP 20	Enters an OER map entry. • Only one match clause can be configured for each OER map sequence. • Deny sequences are first defined in an IP prefix list and then applied with the **match ip address** (OER) command in Step 9. • The example creates an OER map entry for the OER map named DENY_MAP with a sequence number of 20.
Step 9	**match oer learn** {**delay** | **inside** | **throughput**} **Example:** Router(config-oer-map)# match oer learn throughput	Creates a match clause entry in an OER map to match OER learned prefixes. • OER can be configured to learn traffic classes that are inside prefixes or prefixes based on highest delay, or highest outbound throughput. • Only a single match clause can be configured for each OER map sequence. • The example creates a match clause entry that matches traffic classes that are learned on the basis of the highest throughput.
Step 10	**end** **Example:** Router(config-oer-map)# end	(Optional) Exits OER map configuration mode and returns to privileged EXEC mode.

Configuring and Applying an OER Policy to Learned Inside Prefixes

Perform this task to apply a policy to learned inside prefix traffic class entries from the MTC list. Support for optimizing inside prefixes was introduced in Cisco IOS Release 12.4(9)T and 12.2(33)SRB. The policy is configured using an OER map and contains some set clauses.

✎
Note   Policies applied in an OER map do not override global policy configurations.

OER Inside Prefixes

An OER inside prefix is defined as a public IP prefix assigned to a company. An OER outside prefix is defined as a public IP prefix assigned outside the company. Companies advertise the inside prefixes over the Internet using an Internet service provider (ISP) and receive advertisements for outside prefixes from an ISP.

Prerequisites

This task requires the master controller and border routers to be running Cisco IOS Release 12.4(9)T, 12.2(33)SRB, or later releases.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **oer-map** *map-name sequence-number*
4. **match oer learn** {**delay** | **inside** | **throughput**}
5. **set delay** {**relative** *percentage* | **threshold** *maximum*}
6. **set loss** {**relative** *average* | **threshold** *maximum*}
7. **set unreachable** {**relative** *average* | **threshold** *maximum*}
8. **end**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		
		• Enter your password if prompted.

Step 2	`configure terminal`
	
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

	Command or Action	Purpose
Step 3	**oer-map** *map-name sequence-number* **Example:** Router(config)# oer-map INSIDE_LEARN 10	Enters OER map configuration mode to configure an OER map to apply policies to selected IP prefixes. • Only one match clause can be configured for each OER map sequence. • Deny sequences are first defined in an IP prefix list and then applied with a **match** command. • The example creates an OER map named INSIDE_LEARN.
Step 4	**match oer learn** {**delay** | **inside** | **throughput**} **Example:** Router(config-oer-map)# match oer learn inside	Creates a match clause entry in an OER map to match OER learned prefixes. • Prefixes can be configured to learn prefixes that are inside prefixes or prefixes based on lowest delay, or highest outbound throughput. • Only a single match clause can be configured for each OER map sequence. • The example creates a match clause entry that matches traffic learned using inside prefixes.
Step 5	**set delay** {**relative** *percentage* | **threshold** *maximum*} **Example:** Router(config-oer-map)# set delay threshold 2000	Creates a set clause entry to configure the delay threshold. • The delay threshold can be configured as a relative percentage or as an absolute value for match criteria. • The **relative** keyword is used to configure a relative delay percentage. The relative delay percentage is based on a comparison of short-term and long-term measurements. • The **threshold** keyword is used to configure the absolute maximum delay period in milliseconds. • The example creates a set clause that sets the absolute maximum delay threshold to 2000 milliseconds for traffic that is matched in the same OER map sequence.

	Command or Action	Purpose
Step 6	**set loss** {**relative** *average* | **threshold** *maximum*} **Example:** Router(config-oer-map)# set loss relative 20	Creates a set clause entry to configure the relative or maximum packet loss limit that the master controller will permit for an exit link. • This command is used to configure an OER map to configure the relative percentage or maximum number of packets that OER will permit to be lost during transmission on an exit link. If packet loss is greater than the user-defined or the default value, the master controller determines that the exit link is out-of-policy. • The **relative** keyword is used to configure the relative packet loss percentage. The relative packet loss percentage is based on a comparison of short-term and long-term packet loss. • The **threshold** keyword is used to configure the absolute maximum packet loss. The maximum value is based on the actual number of packets per million that have been lost. • The example creates a set clause that configures the relative percentage of acceptable packet loss to less than 20 percent for traffic that is matched in the same OER map sequence.
Step 7	**set unreachable** {**relative** *average* | **threshold** *maximum*} **Example:** Router(config-oer-map)# set unreachable relative 10	Creates a set clause entry to configure the maximum number of unreachable hosts. • This command is used to specify the relative percentage or the absolute maximum number of unreachable hosts, based on flows per million (fpm), that OER will permit for a traffic class entry. If the absolute number or relative percentage of unreachable hosts is greater than the user-defined or the default value, OER determines that the traffic class entry is OOP and searches for an alternate exit link. • The **relative** keyword is used to configure the relative percentage of unreachable hosts. The relative unreachable host percentage is based on a comparison of short-term and long-term measurements. • The **threshold** keyword is used to configure the absolute maximum number of unreachable hosts based on fpm. • The example creates a set clause entry that configures the master controller to search for a new exit link for a traffic class entry when the relative percentage of unreachable hosts is equal to or greater than 10 percent for traffic learned based on highest delay.
Step 8	**end** **Example:** Router(config-oer-map)# end	(Optional) Exits OER map configuration mode and returns to privileged EXEC mode.

Configuring and Applying an OER Policy to Configured Inside Prefixes

Perform this task to apply a policy to configured inside prefix traffic class entries from the MTC list. Support for optimizing inside prefixes was introduced in Cisco IOS Release 12.4(9)T and 12.2(33)SRB. The policies are configured using an OER map. This task contains prefix list configuration with different criteria in the set clauses.

Note Policies applied in an OER map do not override global policy configurations.

OER Inside Prefixes

An OER inside prefix is defined as a public IP prefix assigned to a company. An OER outside prefix is defined as a public IP prefix assigned outside the company. Companies advertise the inside prefixes over the Internet using an Internet service provider (ISP) and receive advertisements for outside prefixes from an ISP.

Prerequisites

This task requires the master controller and border routers to be running Cisco IOS Release 12.4(9)T, 12.2(33)SRB, or later releases.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **oer-map** *map-name sequence-number*
4. **match ip address** {**access-list** *access-list-name* | **prefix-list** *prefix-list-name* [**inside**]}
5. **set delay** {**relative** *percentage* | **threshold** *maximum*}
6. **set loss** {**relative** *average* | **threshold** *maximum*}
7. **set unreachable** {**relative** *average* | **threshold** *maximum*}
8. **end**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		
		• Enter your password if prompted.

Step 2	`configure terminal`
	
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

	Command or Action	Purpose
Step 3	`oer-map map-name` *sequence-number* **Example:** `Router(config)# oer-map INSIDE_CONFIGURE 10`	Enters OER map configuration mode to create or configure an OER map. • OER map operation is similar to that of route maps. • Only a single match clause can be configured for each OER map sequence. • Common and deny sequences should be applied to lowest oer-map sequence for best performance. • The example creates an OER map named INSIDE_CONFIGURE.
Step 4	`match ip address` {**access-list** *access-list-name* | **prefix-list** *prefix-list-name* [**inside**] **Example:** `Router(config-oer-map)# match ip address prefix-list INSIDE_PREFIXES inside`	References an extended IP access list or IP prefix list as match criteria in an OER map. • Use the **inside** keyword to specify inside prefixes to support OER BGP inbound optimization that supports best entrance selection for traffic that originates from prefixes outside an autonomous system destined for prefixes inside the autonomous system. • The example creates a match clause entry using the prefix list INSIDE_PREFIXES that specifies inside prefixes.
Step 5	`set delay` {**relative** *percentage* | **threshold** *maximum*} **Example:** `Router(config-oer-map)# set delay threshold 2000`	Creates a set clause entry to configure the delay threshold. • The delay threshold can be configured as a relative percentage or as an absolute value for match criteria. • The **relative** keyword is used to configure a relative delay percentage. The relative delay percentage is based on a comparison of short-term and long-term measurements. • The **threshold** keyword is used to configure the absolute maximum delay period in milliseconds. • The example creates a set clause that sets the absolute maximum delay threshold to 2000 milliseconds for traffic that is matched in the same OER map sequence.

	Command or Action	Purpose
Step 6	**set loss** {**relative** *average* | **threshold** *maximum*} **Example:** Router(config-oer-map)# set loss relative 20	Creates a set clause entry to configure the relative or maximum packet loss limit that the master controller will permit for an exit link. • This command is used to configure an OER map to configure the relative percentage or maximum number of packets that OER will permit to be lost during transmission on an exit link. If packet loss is greater than the user-defined or the default value, the master controller determines that the exit link is out-of-policy. • The **relative** keyword is used to configure the relative packet loss percentage. The relative packet loss percentage is based on a comparison of short-term and long-term packet loss. • The **threshold** keyword is used to configure the absolute maximum packet loss. The maximum value is based on the actual number of packets per million that have been lost. • The example creates a set clause that configures the relative percentage of acceptable packet loss to less than 20 percent for traffic that is matched in the same OER map sequence.
Step 7	**set unreachable** {**relative** *average* | **threshold** *maximum*} **Example:** Router(config-oer-map)# set unreachable relative 10	Creates a set clause entry to configure the maximum number of unreachable hosts. • This command is used to specify the relative percentage or the absolute maximum number of unreachable hosts, based on flows per million (fpm), that OER will permit for a traffic class entry. If the absolute number or relative percentage of unreachable hosts is greater than the user-defined or the default value, OER determines that the traffic class entry is OOP and searches for an alternate exit link. • The **relative** keyword is used to configure the relative percentage of unreachable hosts. The relative unreachable host percentage is based on a comparison of short-term and long-term measurements. • The **threshold** keyword is used to configure the absolute maximum number of unreachable hosts based on fpm. • The example creates a set clause entry that configures the master controller to search for a new exit link for a traffic class entry when the relative percentage of unreachable hosts is equal to or greater than 10 percent for traffic learned based on highest delay.
Step 8	**end** **Example:** Router(config-oer-map)# end	Exits OER map configuration mode and returns to privileged EXEC mode.

Configuring Policy Rules for OER Maps

Perform this task to select an OER map and apply the configuration under OER master controller configuration mode. The **policy-rules** OER master controller configuration command was introduced in Cisco IOS Release 12.3(11)T, and this command provides an improved method to switch between predefined OER maps.

Prerequisites

- At least one OER map must be configured before you can enable policy-rule support.
- This task requires the master controller and border routers to be running Cisco IOS Release 12.3(11)T, 12.2(33)SRB, or later release.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **oer master**
4. **policy-rules** *map-name*
5. **end**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		
		- Enter your password if prompted.

Step 2	`configure terminal`
	
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`oer master`
	
	Example:
	`Router(config)# oer master`
		Enters OER master controller configuration mode to configure global prefix and exit link policies.

	Command or Action	Purpose
Step 4	**policy-rules** *map-name* **Example:** Router(config-oer-mc)# policy-rules RED	Applies a configuration from an OER map to a master controller configuration in OER master controller configuration mode. • Reentering this command with a new OER map name will immediately overwrite the previous configuration. This behavior is designed to allow you to quickly select and switch between predefined OER maps. • The example applies the configuration from the OER map named RED.
Step 5	**end** **Example:** Router(config-oer-mc)# end	Exits OER master controller configuration mode and enters privileged EXEC mode.

Configuring Multiple OER Policy Conflict Resolution

Perform this task to use the OER resolve function to assign a priority to an OER policy to avoid any conflict over which policy to run first. Each policy is assigned a unique value, and the policy with the highest value is selected as the highest priority. By default, a delay policy has the highest priority and a traffic load (utilization) policy has the second highest priority. Assigning a priority value to any policy will override default settings.

SUMMARY STEPS

1. **enable**

2. **configure terminal**

3. **oer master**

4. **resolve** {**cost priority** *value* | **delay priority** *value* **variance** *percentage* | **loss priority** *value* **variance** *percentage* | **range priority** *value* | **utilization priority** *value* **variance** *percentage*}

5. Repeat Step 4 to assign a priority for each required OER policy.

6. **end**

DETAILED STEPS

|	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose

Step 3	`oer master`
	
	Example:
	`Router(config)# oer master`
		Enters OER master controller configuration mode.

Step 4	`resolve {cost priority value | delay priority value variance percentage | loss priority value variance percentage | range priority value | utilization priority value variance percentage}`
	
	Example:
	`Router(config-oer-mc)# resolve loss priority 2 variance 10`
		Sets policy priority or resolves policy conflicts.
		
		• This command is used to set priority when multiple policies are configured for the same prefix. When this command is configured, the policy with the highest priority will be selected to determine the policy decision.
		
		• The **priority** keyword is used to specify the priority value. Setting the number 1 assigns the highest priority to a policy. Setting the number 10 assigns the lowest priority.
		
		• Each policy must be assigned a different priority number.
		
		• The **variance** keyword is used to set an allowable variance for a user-defined policy. This keyword configures the allowable percentage that an exit link or prefix can vary from the user-defined policy value and still be considered equivalent.
		
		• The example sets the priority for loss policies to 2 with a 10 percent variance.
		
		Note Variance cannot be configured for range or cost policies.
		
		Note Support for **jitter** and **mos** policies was introduced in Cisco IOS Release 12.4(6)T and 12.2(33)SRB. For more details, see the *Cisco IOS Optimized Edge Routing Command Reference*, Release 12.4T.

Step 5	Repeat Step 4 to assign a priority for each required OER policy.	—

Step 6	`end`
	
	Example:
	`Router(config-oer-mc)# end`
		Exits OER master controller configuration mode, and enters privileged EXEC mode.

Configuring an Exit Link Load Balancing OER Policy

Perform this task at the master controller to configure a load balancing policy for traffic class flows over the border router exit links. In this example, range and exit utilization policies are given priority when OER chooses the best exit selection for traffic class flows. Best route selection for performance policies is disabled. The external Ethernet interfaces on border router 1 and border router 2—BR1 and BR2 in Figure 4—are both configured with a maximum utilization threshold of 70 percent and a range of utilization between the two exit links is set to 30 percent. After an external interface is configured for the border routers, OER automatically monitors the utilization of external links on a border router every

5 minutes. The utilization is reported back to the master controller and, if the utilization exceeds 70 percent, OER selects another exit link for traffic class flows on that link. To complete the load balancing, the utilization range between the two exit links must not be greater than 30 percent, otherwise OER will move some of the traffic classes from one exit link to another to balance the traffic load between the two exit links.

Figure 4   *Network diagram for OER Exit Link Load Balancing*
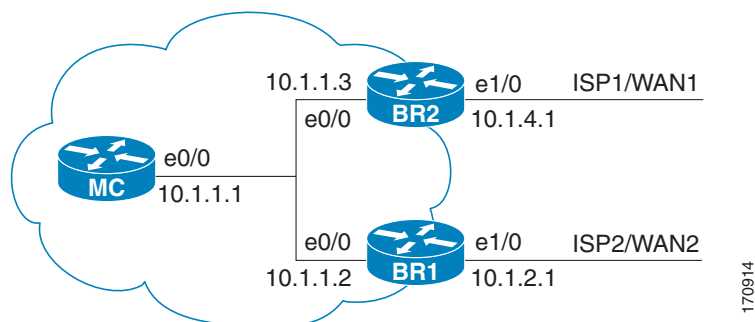
Traffic can also be load balanced over entrance links, for more details see the "Using OER to Control Traffic Classes and Verify the Network Performance" module.

SUMMARY STEPS

1. **enable**

2. **configure terminal**

3. **oer master**

4. **max-range-utilization percent** *maximum*

5. **mode select-exit** {**best** | **good**}

6. **resolve range priority** *value*

7. **resolve utilization priority** *value* **variance** *percentage*

8. **no resolve delay**

9. **no resolve loss**

10. **border** *ip-address* [**key-chain** *key-chain-name*]

11. **interface** *type number* **external**

12. **max-xmit-utilization** {**absolute** *kbps* | **percentage** *value*}

13. **exit**

14. **exit**

15. Repeat Step 10 through Step 14 to set a utilization threshold for each external link.

16. **keepalive** *timer*

17. **end**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		
		• Enter your password if prompted.

Step 2	`configure terminal`
	
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`oer master`
	
	Example:
	`Router(config)# oer master`
		Enters OER master controller configuration mode to configure a router as a master controller and to configure global operations and policies.

Step 4	`max-range-utilization percent` *maximum* **Example:** `Router(config-oer-mc)# max-range-utilization percent 30`	Sets the maximum utilization range for all OER-managed exit link.s. • Use the **percent** keyword and *maximum* argument to specify the maximum utilization range between all the exit links. • In this example, the utilization range between all the exit links on the border routers must be within 30 percent.
Step 5	`mode select-exit` {**best** | **good**} **Example:** `Router(config-oer-mc)# mode select-exit best`	Creates a set clause entry to configure exit selection settings. • Use the **select-exit** keyword to configure the master controller to select either the best available exit when the **best** keyword is entered or the first in-policy exit when the **good** keyword is entered. • In this example, OER will select the best available exit. **Note** Only the syntax relevant to this task is displayed. For more details, see the *Cisco IOS Optimized Edge Routing Command Reference*, Release 12.4T.

	Command or Action	Purpose
Step 6	`resolve range priority` *value* **Example:** `Router(config-oer-mc)# resolve range priority 1`	Sets policy priority or resolves policy conflicts. • This command is used to set the priorities when multiple policies are configured for the same prefix. When this command is configured, the policy with the highest priority will be selected to determine the policy decision. • The **priority** keyword is used to specify the priority value. Setting the number 1 assigns the highest priority to a policy. Setting the number 10 assigns the lowest priority. • Each policy must be assigned a different priority number. • In this example, the priority for range policies is set to 1. **Note** Only the syntax relevant to this task is displayed. For more details, see the *Cisco IOS Optimized Edge Routing Command Reference*, Release 12.4T.
Step 7	`resolve utilization priority` *value* `variance` *percentage* **Example:** `Router(config-oer-mc)# resolve utilization priority 2 variance 25`	Sets policy priority or resolves policy conflicts. • This command is used to set the priorities when multiple policies are configured for the same prefix. When this command is configured, the policy with the highest priority will be selected to determine the policy decision. • The **priority** keyword is used to specify the priority value. Setting the number 1 assigns the highest priority to a policy. Setting the number 10 assigns the lowest priority. • Each policy must be assigned a different priority number. • The **variance** keyword is used to set an allowable variance for a user-defined policy. This keyword configures the allowable percentage that an exit link or prefix can vary from the user-defined policy value and still be considered equivalent. • In this example, the priority for utilization policies is set to 2 with a 25 percent variance. **Note** Only the syntax relevant to this task is displayed. For more details, see the *Cisco IOS Optimized Edge Routing Command Reference*, Release 12.4T.

Step 8	`no resolve delay`
	
	Example:
	`Router(config-oer-mc)# no resolve delay`
		Disables any priority for delay performance policies.
		
		Note Only the syntax relevant to this task is displayed. For more details, see the *Cisco IOS Optimized Edge Routing Command Reference*, Release 12.4T.

	Command or Action	Purpose

Step 9	`no resolve loss`
	
	Example:
	`Router(config-oer-mc)# no resolve loss`
		Disables any priority for loss performance policies.
		
		Note Only the syntax relevant to this task is displayed. For more details, see the *Cisco IOS Optimized Edge Routing Command Reference*, Release 12.4T.

Step 10	`border ip-address [key-chain key-chain-name]`
	
	Example:
	`Router(config-oer-mc)# border 10.1.1.2 key-chain border1_OER`
		Enters OER-managed border router configuration mode to establish communication with a border router.
		
		• An IP address is configured to identify the border router.
		
		• At least one border router must be specified to create an OER-managed network. A maximum of ten border routers can be controlled by a single master controller.
		
		• The value for the *key-chain-name* argument must match a valid the key-chain name configured on the border router.
		
		Note The **key-chain** keyword and *key-chain-name* argument must be entered when a border router is initially configured. However, this keyword is optional when reconfiguring an existing border router.

Step 11	`interface type number external`
	
	Example:
	`Router(config-oer-mc-br)# interface Ethernet 1/0 external`
		Configures a border router interface as an OER-managed external interface.
		
		• External interfaces are used to forward traffic and for active monitoring.
		
		• A minimum of two external border router interfaces are required in an OER-managed network. At least one external interface must be configured on each border router. A maximum of 20 external interfaces can be controlled by single master controller.
		
		Tip Configuring an interface as an OER-managed external interface on a router enters OER border exit interface configuration mode. In this mode, you can configure maximum link utilization or cost-based optimization for the interface.
		
		Note Entering the **interface** command without the **external** or **internal** keyword places the router in global configuration mode and not OER border exit configuration mode. The **no** form of this command should be applied carefully so that active interfaces are not removed from the router configuration.

Command or Action	Purpose

Step 12 `max-xmit-utilization {`**absolute** `kbps |` **percentage** `value}`
 	
Example:
`Router(config-oer-mc-br-if)#`
`max-xmit-utilization percentage 70`
	Configures the maximum utilization on a single OER managed exit link.
	
	• Use the **absolute** keyword and *kbps* argument to specify the absolute maximum utilization on an OER managed exit link in kbps.
	
	• Use the **percentage** keyword and *value* argument to specify percentage utilization of an exit link.

Step 13 `exit` **Example:** `Router(config-oer-mc-br-if)# exit`	Exits OER-managed border exit interface configuration mode and returns to OER-managed border router configuration mode.
Step 14 `exit` **Example:** `Router(config-oer-mc-br)# exit`	Exits OER-managed border router configuration mode and returns to OER master controller configuration mode.
Step 15 Repeat Step 10 through Step 14 with appropriate changes to set a utilization threshold for each external link.	—
Step 16 `keepalive` *timer* **Example:** `Router(config-oer-mc)# keepalive 10`	(Optional) Configures the length of time that an OER master controller will maintain connectivity with an OER border router after no keepalive packets have been received. • The example sets the keepalive timer to 10 seconds. The default keepalive timer is 60 seconds.
Step 17 `end` **Example:** `Router(config-oer-mc-learn)# end`	Exits OER Top Talker and Top Delay learning configuration mode and returns to privileged EXEC mode.

Implementing Performance Routing Link Groups

Perform this task on a master controller to set up some performance routing link groups by identifying an exit link on a border router as a member of a link group, and to create an OER map to specify link groups for traffic classes defined in an OER policy. In this task, a link group is set up for video traffic and a set of high bandwidth exit links are identified as members of the video link group which is identified as a primary link group. A fallback link group is also specified.

An OER policy is created using an OER map where the primary and fall link groups are specified for traffic classes matching the OER map criteria. OER probes both the primary and fallback group links and selects the best link in the primary link group for the traffic class specified in this task. If none of the primary links are within policy, OER selects the bast link from the fallback group. For more details about link groups, see the "Performance Routing Link Grouping" section on page 9.

Prerequisites

This task requires the master controller and border routers to be running Cisco IOS Release 12.4(15)T, or later release.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **oer master**
4. **border** *ip-address* [**key-chain** *key-chain-name*]
5. **interface** *type number* **external**
6. **link-group** *link-group-name* [*link-group-name* [*link-group-name*]]
7. **exit**
8. Repeat Step 5 through Step 7 with appropriate changes to set up link groups for all the external interface.
9. **interface** *type number* **internal**
10. **exit**
11. **ip access-list** {**standard** | **extended**} *access-list-name*
12. [*sequence-number*] **permit udp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**dscp** *dscp-value*]
13. Repeat Step 12 for every required access list entry.
14. **exit**
15. **oer-map** *map-name sequence-number*
16. **match traffic-class access-list** *access-list-name*
17. **set link-group** *link-group-name* [**fallback** *link-group-name*]
18. **end**
19. **show oer master link-group** [*link-group-name*]

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		
		• Enter your password if prompted.

Step 2	`configure terminal`
	
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

	Command or Action	Purpose

Step 3	`oer master`
	
	Example:
	`Router(config)# oer master`
		Enters OER master controller configuration mode to configure a router as a master controller.
		
		• A master controller and border router process can be enabled on the same router (for example, in a network that has a single router with two exit links to different service providers).
		
		Note Only the syntax used in this context is displayed. For more details, see the *Cisco IOS Optimized Edge Routing Command Reference*, Release 12.4T

Step 4	`border` *ip-address* [`key-chain` *key-chain-name*] **Example:** `Router(config-oer-mc)# border 192.168.1.2 key-chain border1_OER`	Enters OER-managed border router configuration mode to establish communication with a border router. • An IP address is configured to identify the border router. • At least one border router must be specified to create an OER-managed network. A maximum of ten border routers can be controlled by a single master controller. • The value for the *key-chain-name* argument must match the key-chain name configured when the border router is set up. **Note** The **key-chain** keyword and *key-chain-name* argument must be entered when a border router is initially configured. However, this keyword is optional when reconfiguring an existing border router.

Step 5	`interface` *type number* `external`
	
	Example:
	`Router(config-oer-mc-br)# interface Serial 2/0 external`
		Configures a border router interface as an OER-managed external interface.
		
		• External interfaces are used to forward traffic and for active monitoring.
		
		• A minimum of two external border router interfaces are required in an OER-managed network. At least one external interface must be configured on each border router. A maximum of 20 external interfaces can be controlled by single master controller.
		
		Tip Configuring an interface as an OER-managed external interface on a router enters OER border exit interface configuration mode. In this mode, you can configure maximum link utilization or cost-based optimization for the interface.
		
		Note Entering the **interface** command without the **external** or **internal** keyword places the router in global configuration mode and not OER border exit configuration mode. The **no** form of this command should be applied carefully so that active interfaces are not removed from the router configuration.

	Command or Action	Purpose
Step 6	**link-group** *link-group-name* [*link-group-name* [*link-group-name*]] **Example:** Router(config-oer-mc-br-if)# link-group VIDEO	Configures an OER border router exit interface as a member of a link group. • Use the *link-group-name* to specify the link group name for the interface. • Up to three link groups can be specified for each interface. • In this example, the Serial 2/0 external interface is configured as a member of the link group named VIDEO. **Note** The **link-group** command associates a link group with an interface. Another step, Step 17, uses the **set link-group** command to identify the link group as a primary or fallback group for traffic classes defined in an OER map.
Step 7	**exit** **Example:** Router(config-oer-mc-br-if)# exit	Exits OER-managed border exit interface configuration mode and returns to OER-managed border router configuration mode.
Step 8	Repeat Step 5 through Step 7 with appropriate changes to set up link groups for all the external interface.	—
Step 9	**interface** *type number* **internal** **Example:** Router(config-oer-mc-br)# interface FastEthernet 0/1 internal	Configures a border router interface as an OER controlled internal interface. • Internal interfaces are used for passive monitoring only. Internal interfaces do not forward traffic. • At least one internal interface must be configured on each border router. **Note** Support to configure a VLAN interface as an internal interface was introduced in Cisco IOS Release 12.3(14)T and 12.2(33)SRB.
Step 10	**exit** **Example:** Router(config-oer-mc-br)# exit	Exits OER-managed border configuration mode and returns to global configuration mode.
Step 11	**ip access-list** {**standard**	**extended**} *access-list-name* **Example:** Router(config)# ip access-list extended ACCESS_VIDEO	Defines an IP access list by name and enters extended named access list configuration mode. • OER supports only named access lists. • The example creates an extended IP access list named ACCESS_VIDEO.

	Command or Action	Purpose
Step 12	[*sequence-number*] **permit udp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**dscp** *dscp-value*] **Example:** Router(config-ext-nacl)# permit tcp any any 500	Sets conditions to allow a packet to pass a named IP access list. • The example is configured to identify all TCP traffic from any destination or source and from destination port number of 500. This specific TCP traffic is to be optimized. **Note** Only the syntax applicable to this task is shown. For more details, see the *Cisco IOS IP Application Services Command Reference*, Release 12.4T.
Step 13	Repeat Step 12 for more access list entries, as required.	—
Step 14	**exit** **Example:** Router(config-ext-nacl)# exit	(Optional) Exits extended named access list configuration mode and returns to global configuration mode.
Step 15	**oer-map** *map-name sequence-number* **Example:** Router(config)# oer-map VIDEO_MAP 10	Enters OER map configuration mode to configure an OER map. • Only one match clause can be configured for each OER map sequence. • Permit sequences are first defined in an IP prefix list and then applied with the **match ip address** (OER) command in Step 16. • The example creates an OER map named VIDEO_MAP.
Step 16	**match traffic-class access-list** *access-list-name* **Example:** Router(config-oer-map)# traffic-class access-list ACCESS_VIDEO	Manually configures an access list as match criteria used to create traffic classes using an OER map. • Each access list entry must contain a destination prefix and may include other optional parameters. • The example defines a traffic class using the criteria defined in the access list named ACCESS_VIDEO.
Step 17	**set link-group** *link-group-name* [**fallback** *link-group-name*] Example: Router(config-oer-map)# set link-group video fallback voice	Specifies a link group for traffic classes defined in an OER map to create an OER policy. • Use the *link-group-name* to specify the primary link group name for the policy. • Use the **fallback** keyword to specify the fallback link group name for the policy. • The example specifies the VIDEO link group as the primary link group for the traffic class matching the access list ACCESS_VIDEO. The link group VOICE is specified as the fallback link group.

	Command or Action	Purpose

Step 18	`end`
	
	Example:
	`Router(config-oer-map)# end`
		(Optional) Exits OER map configuration mode and returns to privileged EXEC mode.

Step 19	`show oer master link-group` [*link-group-name*] **Example:** `Router# show oer master link-group`	Displays information about configured OER link groups. • Use the optional *link-group-name* argument to display information for the specified OER link group. • If the *link-group-name* argument is not specified, information about all OER link groups is displayed. • The example displays information about all configured link groups.

Examples

The example output from the **show oer master link-group** command displays information about performance routing link groups configured using OER. In this example, the VIDEO link group is shown with other configured link groups.

```
Router# show oer master link-group

link group video
  Border          Interface        Exit id
  192.168.1.2     Serial2/0        1
 link group voice
  Border          Interface        Exit id
  192.168.1.2     Serial2/0        1
  192.168.1.2     Serial3/0        2
  192.168.3.2     Serial4/0        4
 link group data
  Border          Interface        Exit id
  192.168.3.2     Serial3/0        3
```

Configuring OER Cost-Based Policies

Perform this task to configure cost-based optimization. Cost-based optimization is configured on a master controller using the **cost-minimization** command in OER border exit interface configuration mode (under the external interface configuration). Cost-based optimization supports tiered and fixed billing methods.

Prerequisites

This task requires the master controller and border routers to be running Cisco IOS Release 12.3(14)T, 12.2(33)SRB, or later releases.

SUMMARY STEPS

1. **enable**

2. **configure terminal**

3. **oer master**

4. **border** *ip-address* [**key-chain** *key-chain-name*]

5. **interface** *type number* **external**

6. **cost-minimization** {**calc** {**combined** | **separate** | **sum**} | **discard** [**daily**] {**absolute** *number* | **percent** *percentage*} | **end day-of-month** *day* [**offset** *hh*:*mm*] | **fixed fee** [*cost*] | **nickname** *name* | **sampling period** *minutes* [**rollup** *minutes*] | **summer-time** *start end* [*offset*] | **tier** *percentage fee*}

7. Repeat Step 6 to configure additional cost-based optimization policies, if required.

8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**oer master** **Example:** Router(config)# oer master	Enters OER master controller configuration mode to configure global prefix and exit link policies.
Step 4	**border** *ip-address* [**key-chain** *key-chain-name*] **Example:** Router(config-oer-mc)# border 10.100.1.1 key-chain OER	Enters OER-managed border router configuration mode to establish communication with a border router. **Note** The **key-chain** keyword is required only for initial border router configuration.
Step 5	**interface** *type number* **external** **Example:** Router(config-oer-mc-br)# interface ethernet 0/0 external	Enters OER border exit interface configuration mode to configure a border router interface as an external interface. • At least one external interface must be configured on each border router.

	Command or Action	Purpose
Step 6	**cost-minimization** {**calc** {**combined**	**separate**	**sum**}	**discard** [**daily**] {**absolute** *number*	**percent** *percentage*}	**end day-of-month** *day* [**offset** *hh:mm*]	**fixed fee** [*cost*]	**nickname** *name*	**sampling period** *minutes* [**rollup** *minutes*]	**summer-time** *start end* [*offset*]	**tier** *percentage fee*} **Example:** Router(config-oer-mc-br-if)# cost-minimization end day-of-month 30 offset 3:00	Configures cost-based optimization policies on a master controller. • Cost-based optimization supports fixed or tier-based billing, inbound and outbound cost measurements, and very granular sampling. • The **calc** keyword is used to configure how the fee is calculated. You can configure the master controller to combine ingress and egress samples, either by first adding and then combining or by analyzing ingress and egress samples separately. • The **discard** keyword is used to configure the number of samples that are removed for bursty link usage. It is specified as a percentage or as an absolute value. If a sampling rollup is configured, the discard values also applies to the rollup. If the **daily** keyword is entered, samples are analyzed and discarded on a daily basis. At the end of the billing cycle, monthly sustained usage is calculated by averaging daily sustained utilization. • The **end** keyword is used to configure the last day of the billing cycle. Entering the offset keyword allows you to adjust the end of the cycle to compensate for a service provider in a different zone. • The **fixed** keyword is configured when the service provider bills for network access over the specified exit link at a flat rate. The **fee** keyword is optionally used to specify the exit link cost. • The **nickname** keyword is used to apply label that identifies the service provider. • The **sampling** keyword is used to configure the time intervals at which link utilization samples are gathered. By default, the link is sampled every five minutes. • The **rollup** keyword is used to reduce the number of samples by aggregating them. All samples collected during the rollup period are averaged to calculate rollup utilization. **Note** The minimum number that can be entered for the rollup period must be equal to or greater than the number that is entered for the sampling period. • In this example, the billing end date is set to 30, and a a three-hour offset is applied.
Step 7	Repeat Step 6 to configure additional cost-based optimization policies, if required.	—

	Command or Action	Purpose
Step 8	**end** **Example:** Router(config-oer-mc-br-if)# end	Exits OER border exit interface configuration mode and enters privileged EXEC mode.

Configuring OER Network Security Policies

Perform one of the following two optional tasks to help prevent and mitigate attacks on your network. The first task uses the black hole routing technique, and the second task uses the sinkhole routing technique.

- Configuring Black Hole Routing Using an OER Map, page 50
- Configuring Sinkhole Routing Using an OER Map, page 52

Configuring Black Hole Routing Using an OER Map

Perform this task to configure an OER map to filter packets to be forwarded to a null interface, meaning that the packets are discarded in a "black hole." The prefix list is configured after an IP prefix is identified as the source of the attack on the network. Some protocols such as BGP allow the redistribution of back hole routes, but other protocols do not.

Prerequisites

This task requires the master controller and border routers to be running Cisco IOS Release 12.4(9)T, 12.2(33)SRB, or later releases.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*} [**le** *le-value*]
4. **oer-map** *map-name sequence-number*
5. **match ip address** {**access-list** *access-list-name* | **prefix-list** *prefix-list-name*}
6. **set interface null0**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network*/*length* | **permit** *network*/*length*} [**le** *le-value*] **Example:** Router(config)# ip prefix-list BLACK_HOLE_LIST seq 10 permit 10.20.21.0/24	Creates an IP prefix list. • IP prefix lists are used to manually select prefixes for monitoring by the OER master controller. • A master controller can monitor and control an exact prefix of any length including the default route. If an exact prefix is specified, OER monitors only the exact prefix. • A master controller can monitor and control an inclusive prefix using the **le** keyword set to 32. OER monitors the configured prefix and any more specific prefixes (for example, configuring the 10.0.0.0/8 le 32 prefix would include the 10.1.0.0/16 and the 10.1.1.0/24 prefixes) over the same exit and records the information in the routing information base (RIB). • The prefixes specified in the IP prefix list are imported into an OER map using the **match ip address** (OER) command. • The example creates an IP prefix list named BLACK_HOLE_LIST that permits prefixes from the 10.20.21.0/24 subnet.
Step 4	**oer-map** *map-name* *sequence-number* **Example:** Router(config)# oer-map BLACK_HOLE_MAP 10	Enters OER map configuration mode to configure an OER map to apply policies to selected IP prefixes. • Only one match clause can be configured for each OER map sequence. • Deny sequences are first defined in an IP prefix list and then applied with the **match ip address** (OER) command in the previous step. • The example creates an OER map named BLACK_HOLE_MAP.

	Command or Action	Purpose
Step 5	`match ip address {access-list access-list-name	prefix-list prefix-list-name}`  **Example:** `Router(config-oer-map)# match ip address prefix-list BLACK_HOLE_LIST`	References an extended IP access list or IP prefix as match criteria in an OER map. • Only a single match clause can be configured for each OER map sequence. • The example configures the IP prefix list named BLACK_HOLE_LIST as match criteria in an OER map.

Step 6	`set interface null0`
	
	Example:
	`Router(config-oer-map)# set interface null0`
		Creates a set clause entry to forward packets to the null interface, meaning that they are discarded.
		
		• The example creates a set clause entry to specify that the packets matching the prefix list, BLACK_HOLE_LIST, are discarded.

Step 7	`end`
	
	Example:
	`Router(config-oer-map)# end`
		(Optional) Exits OER map configuration mode and returns to privileged EXEC mode.

Configuring Sinkhole Routing Using an OER Map

Perform this task to configure an OER map to filter packets to be forwarded to a next hop. The next hop is a router where the packets can be stored, analyzed, or discarded (the sinkhole analogy). The prefix list is configured after an IP prefix is identified as the source of an attack on the network.

Prerequisites

This task requires the master controller and border routers to be running Cisco IOS Release 12.4(9)T, 12.2(33)SRB, or later releases.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*} [**le** *le-value*]
4. **oer-map** *map-name sequence-number*
5. **match ip address** {**access-list** *access-list-name* | **prefix-list** *prefix-list-name*}
6. **set next-hop** *ip-address*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network*/*length* | **permit** *network*/*length*} [**le** *le-value*] **Example:** Router(config)# ip prefix-list SINKHOLE_LIST seq 10 permit 10.20.21.0/24	Creates an IP prefix list. • IP prefix lists are used to manually select prefixes for monitoring by the OER master controller. • A master controller can monitor and control an exact prefix of any length including the default route. If an exact prefix is specified, OER monitors only the exact prefix. • A master controller can monitor and control an inclusive prefix using the **le** keyword set to 32. OER monitors the configured prefix and any more specific prefixes (for example, configuring the 10.0.0.0/8 le 32 prefix would include the 10.1.0.0/16 and the 10.1.1.0/24 prefixes) over the same exit and records the information in the routing information base (RIB). • The prefixes specified in the IP prefix list are imported into an OER map using the **match ip address** (OER) command. • The example creates an IP prefix list named SINKHOLE_LIST that permits prefixes from the 10.20.21.0/24 subnet.
Step 4	**oer-map** *map-name* *sequence-number* **Example:** Router(config-oer-mc)# oer-map SINKHOLE_MAP 10	Enters OER map configuration mode to configure an OER map to apply policies to selected IP prefixes. • Only one match clause can be configured for each OER map sequence. • Deny sequences are first defined in an IP prefix list and then applied with the **match ip address** (OER) command in the previous step. • The example creates an OER map named SINKHOLE_MAP.
Step 5	**match ip address** {**access-list** *access-list-name* | **prefix-list** *prefix-list-name*} **Example:** Router(config-oer-map)# match ip address prefix-list SINKHOLE_LIST	References an extended IP access list or IP prefix as match criteria in an OER map. • Only a single match clause can be configured for each OER map sequence. • The example configures the IP prefix list named SINKHOLE_LIST as match criteria in an OER map.

	Command or Action	Purpose
Step 6	**set next-hop** *ip-address* **Example:** Router(config-oer-map)# set next-hop 10.20.21.6	Creates a set clause entry specifying that packets are forwarded to the next hop. • The example creates a set clause entry to specify that the packets matching the prefix list, SINKHOLE_LIST, are forwarded to the next hop at 10.20.21.6.
Step 7	**end** **Example:** Router(config)# end	(Optional) Exits OER map configuration mode and returns to privileged EXEC mode.

Configuring OER Voice Traffic Optimization Using Active Probes

Support for optimizing voice traffic using OER was introduced in 12.4(6)T. Configuring OER to optimize voice traffic using active probes involves several decisions and subsequent branching tasks. The first step is to identify the traffic to be optimized and decide whether to use a prefix list or an access list. Use a prefix list to identify all traffic, including voice traffic, with a specific set of destination prefixes. Use an access list to identify only voice traffic with a specific destination prefix and carried over a specific protocol.

The second step in optimizing voice traffic is to configure active probing using the **active-probe** or **set active-probe** command to specify the type of active probe to be used. In Cisco IOS Release 12.4(6)T, 12.2(33)SRB, the ability to set a forced target assignment for the active probe was introduced.

The final step in optimizing voice traffic is to configure an OER policy to set the performance metrics that you want OER to apply to the identified traffic.

Perform one of the first two optional tasks, depending on whether you want to use a prefix list or an access list to identify the traffic to be optimized. The third task can be used with traffic identified using an access list, and it also demonstrates how to use a forced target assignment. For an example configuration that can be used with traffic identified using a prefix list, see the "Optimizing Only Voice Traffic Using Active Probes" section on page 69.

- Identifying Traffic for OER Using a Prefix List, page 54
- Identifying Voice Traffic to Optimize Using an Access List, page 55
- Configuring OER Voice Probes with a Target Assignment, page 57

Identifying Traffic for OER Using a Prefix List

Before traffic can be measured using OER, it must be identified. Perform this task to use a prefix list to identify the traffic that OER will probe.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*} [**le** *le-value*]
4. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		
		• Enter your password if prompted.

Step 2	`configure terminal`
	
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`ip prefix-list` *list-name* [`seq` *seq-value*] {`deny` *network*/*length* | `permit` *network*/*length*} [`le` *le-value*] **Example:** `Router(config)# ip prefix-list TRAFFIC_PFX_LIST seq 10 permit 10.20.21.0/24`	Creates an IP prefix list. • IP prefix lists are used to manually select prefixes for monitoring by the OER master controller. • A master controller can monitor and control an exact prefix of any length including the default route. If an exact prefix is specified, OER monitors only the exact prefix. • A master controller can monitor and control an inclusive prefix using the **le** keyword set to 32. OER monitors the configured prefix and any more specific prefixes (for example, configuring the 10.0.0.0/8 le 32 prefix would include the 10.1.0.0/16 and the 10.1.1.0/24 prefixes) over the same exit and records the information in the routing information base (RIB). • The prefixes specified in the IP prefix list are imported into an OER map using the **match ip address** (OER) command. • The example creates an IP prefix list named TRAFFIC_PFX_LIST that permits prefixes from the 10.20.21.0/24 subnet.

Step 4	`exit`
	
	Example:
	`Router(config)# exit`
		(Optional) Exits global configuration mode and returns to privileged EXEC mode.

Identifying Voice Traffic to Optimize Using an Access List

Perform this task to use an access list to identify the voice traffic. Before voice traffic can be optimized, it must be identified. Voice traffic that has to be optimized must be configured because OER does not "learn" about voice traffic on IP networks during an OER learn phase.

IP Protocol Stack for Voice

Voice traffic uses a variety of protocols and streams on the underlying IP network. Figure 5 is a representation of the protocol options available for carrying voice traffic over IP. Most signaling traffic for voice is carried over TCP. Most voice calls are carried over User Datagram Protocol (UDP) and Real-Time Protocol (RTP). You can configure your voice devices to use a specific range of destination port numbers over UDP to carry voice call traffic.

Figure 5   Protocol Stack Options Available for Voice Traffic
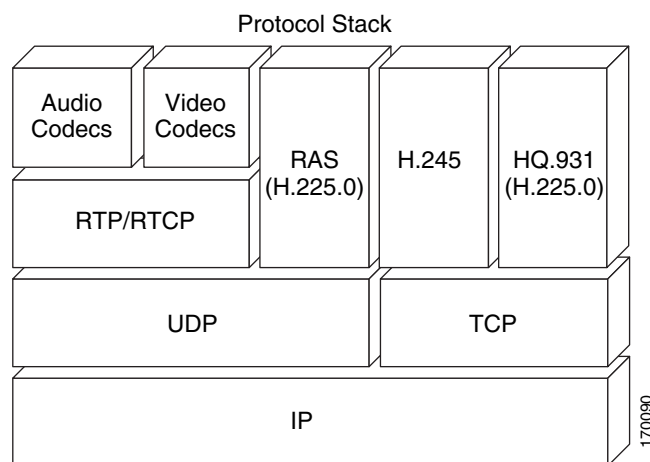
Prerequisites

This task requires the master controller and border routers to be running Cisco IOS Release 12.4(6)T, 12.2(33)SRB, or later release.

SUMMARY STEPS

1. **enable**

2. **configure terminal**

3. **ip access list** {**standard** | **extended**} *access-list-name*

4. [*sequence-number*] **permit udp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]]

5. **end**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		
		• Enter your password if prompted.

Step 2	`configure terminal`
	
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`ip access-list` {`standard` | `extended`} *access-list-name* **Example:** `Router(config)# ip access-list extended VOICE_ACCESS_LIST`	Defines an IP access list by name. • OER supports only named access lists. • The example creates an extended IP access list named VOICE_ACCESS_LIST.
Step 4	[*sequence-number*] **permit udp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] **Example:** `Router(config-ext-nacl)# permit udp any range 16384 32767 10.20.20.0 0.0.0.15 range 16384 32767`	Sets conditions to allow a packet to pass a named IP access list. • The example is configured to identify all UDP traffic ranging from a destination port number of 16384 to 32767 from any source to a destination prefix of 10.20.20.0/24. This specific UDP traffic is to be optimized. • Only the syntax applicable to this task is shown. For more details, see the *Cisco IOS IP Application Services Command Reference*, Release 12.4T.

Step 5	`end`
	
	Example:
	`Router(config-ext-nacl)# end`
		(Optional) Exits extended access list configuration mode and returns to privileged EXEC mode.

Configuring OER Voice Probes with a Target Assignment

After identifying the traffic (in this example, voice traffic identified using an access list) to be optimized, perform this task to configure the OER jitter probes and assign the results of the jitter probes to optimize the identified traffic. In this task, the OER active voice probes are assigned a forced target for OER instead of the usual longest match assigned target. Before configuring the OER jitter probe on the source device, the IP SLAs Responder must be enabled on the target device (the operational target). The IP SLAs Responder is available only on Cisco IOS software-based devices. Start this task at the network device that runs the IP SLAs Responder.

Note The device that runs the IP SLAs Responder does not have to be configured for OER.

Note Policies applied in an OER map do not override global policy configurations.

Prerequisites

- Before configuring this task, perform the "Identifying Voice Traffic to Optimize Using an Access List" section on page 55.
- This task requires the master controller and border routers to be running Cisco IOS Release 12.4(6)T, 12.2(33)SRB, or later releases.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla monitor responder**
4. **exit**
5. Move to the network device that is the OER master controller.
6. **enable**
7. **configure terminal**
8. **oer-map** *map-name sequence-number*
9. **match ip address** {**access-list** *access-list-name* | **prefix-list** *prefix-list-name*}
10. **set active probe** *probe-type ip-address* [**target-port** *number*] [**codec** *codec-name*]
11. **set probe frequency** *seconds*
12. **set jitter threshold** *maximum*
13. **set mos threshold** *minimum* **percent** *percent*
14. **set resolve** {**cost priority** *value* | **delay priority** *value* **variance** *percentage* | **jitter priority** *value* **variance** *percentage* | **loss priority** *value* **variance** *percentage* | **mos priority** *value* **variance** *percentage* | **range priority** *value* | **utilization priority** *value* **variance** *percentage*}
15. **set resolve mos priority** *value* **variance** *percentage*
16. **set delay** {**relative** *percentage* | **threshold** *maximum*}
17. **exit**
18. **oer master**
19. **policy-rules** *map-name*
20. **end**
21. **show oer master active-probes forced**
22. **show oer master policy** [*sequence-number* | *policy-name* | **default**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**ip sla monitor responder** **Example:** Router(config)# ip sla monitor responder	Enables the IP SLAs Responder.
Step 4	**exit** **Example:** Router(config)# exit	Exits global configuration mode and returns to privileged EXEC mode.
Step 5	Move to the network device that is the OER master controller.	—
Step 6	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 7	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 8	**oer-map** *map-name sequence-number* **Example:** Router(config)# oer-map TARGET_MAP 10	Enters OER map configuration mode to configure an OER map to apply policies to selected IP prefixes. • Only one match clause can be configured for each OER map sequence. • Deny sequences are first defined in an IP prefix list and then applied with the **match ip address** (OER) command in Step 9. • The example creates an OER map named TARGET_MAP.
Step 9	**match ip address** {**access-list** *access-list-name* | **prefix-list** *prefix-list-name*} **Example:** Router(config-oer-map)# match ip address access-list VOICE_ACCESS_LIST	References an extended IP access list or IP prefix as match criteria in an OER map. • Only a single match clause can be configured for each OER map sequence. • The example configures the IP access list named VOICE_ACCESS_LIST as match criteria in an OER map. The access list was created in the "Identifying Voice Traffic to Optimize Using an Access List" task.

	Command or Action	Purpose
Step 10	**set active-probe** *probe-type ip-address* [**target-port** *number*] [**codec** *codec-name*] **Example:** Router(config-oer-map)# set active-probe jitter 10.20.22.1 target-port 2000 codec g729a	Creates a set clause entry to assign a target prefix for an active probe. • Use the *probe-type* argument to specify one four probe types: echo, jitter, tcp-conn, or udp-echo. • The *ip-address* argument to specify the target IP address of a prefix to be monitored using the specified type of probe. • The **target-port** keyword and *number* argument are used to specify the destination port number for the active probe. • The **codec** keyword and *codec-name* argument are used only with the jitter probe type. Specifies the codec value used for Mean Opinion Score (MOS) calculation. The codec values must be one of the following: g711alaw, g711ulaw, or g729a. • The example creates a set clause entry to specify the target IP address of a prefix and a specific port number to actively monitor using jitter.
Step 11	**set probe frequency** *seconds* **Example:** Router(config-oer-map)# set probe frequency 10	Creates a set clause entry to set the frequency of the OER active probe. • The *seconds* argument is used to set the time, in seconds, between the active probe monitoring of the specified IP prefixes. • The example creates a set clause to set the active probe frequency to 10 seconds.
Step 12	**set jitter threshold** *maximum* **Example:** Router(config-oer-map)# set jitter threshold 20	Creates a set clause entry to configure the jitter threshold value. • The **threshold** keyword is used to configure the maximum jitter value, in milliseconds. • The example creates a set clause that sets the jitter threshold value to 20 for traffic that is matched in the same OER map sequence.

	Command or Action	Purpose
Step 13	**set mos** {**threshold** *minimum* **percent** *percent*} **Example:** `Router(config-oer-map)# set mos threshold 4.0 percent 30`	Creates a set clause entry to configure the MOS threshold and percentage values used to decide whether an alternate exit is be selected. • The **threshold** keyword is used to configure the minimum MOS value. • The **percent** keyword is used to configure the percentage of MOS values that are below the MOS threshold. • OER calculates the percentage of MOS values below the MOS threshold that are recorded in a five-minute period. If the percentage value exceeds the configured percent value or the default value, the master controller searches for alternate exit links. • The example creates a set clause that sets the threshold MOS value to 4.0 and the percent value to 30 percent for traffic that is matched in the same OER map sequence.
Step 14	**set resolve** {**cost priority** *value* | **delay priority** *value* **variance** *percentage* | **jitter priority** *value* **variance** *percentage* | **loss priority** *value* **variance** *percentage* | **mos priority** *value* **variance** *percentage* | **range priority** *value* | **utilization priority** *value* **variance** *percentage*} **Example:** `Router(config-oer-map)# set resolve jitter priority 1 variance 10`	Creates a set clause entry to configure policy priority or resolve policy conflicts. • This command is used to set priority for a policy type when multiple policies are configured for the same prefix. When this command is configured, the policy with the highest priority will be selected to determine the policy decision. • The **priority** keyword is used to specify the priority value. Configuring the number 1 assigns the highest priority to a policy. Configuring the number 10 assigns the lowest priority. • Each policy must be assigned a different priority number. • The **variance** keyword is used to set an allowable variance for a user-defined policy. This keyword configures the allowable percentage that an exit link or prefix can vary from the user-defined policy value and still be considered equivalent. • Variance cannot be configured for cost or range policies. • The example creates set clause that configures the priority for jitter policies to 1 for voice traffic. The variance is configured to allow a 10 percent difference in jitter statistics before a prefix is determined to be out-of-policy.

	Command or Action	Purpose
Step 15	**set resolve mos priority** *value* **variance** *percentage* **Example:** Router(config-oer-map)# set resolve mos priority 2 variance 15	Creates a set clause entry to configure policy priority or resolve policy conflicts. • The example creates set clause that configures the priority for MOS policies to 2 for voice traffic. The variance is configured to allow a 15 percent difference in MOS values before a prefix is determined to be out-of-policy. **Note** Only the syntax applicable to this task is used in this example. For more details, see Step 14.
Step 16	**set delay** {**relative** *percentage* │ **threshold** *maximum*} **Example:** Router(config-oer-map)# set delay threshold 100	Creates a set clause entry to configure the delay threshold. • The delay threshold can be configured as a relative percentage or as an absolute value for match criteria. • The **relative** keyword is used to configure a relative delay percentage. The relative delay percentage is based on a comparison of short-term and long-term measurements. • The **threshold** keyword is used to configure the absolute maximum delay period in milliseconds. • The example creates a set clause that sets the absolute maximum delay threshold to 100 milliseconds for traffic that is matched in the same OER map sequence.
Step 17	**exit** **Example:** Router(config-oer-map)# exit	Exits OER map configuration mode and returns to global configuration mode.
Step 18	**oer master** **Example:** Router(config)# oer master	Enters OER master controller configuration mode to configure a router as a master controller. • A master controller and border router process can be enabled on the same router (for example, in a network that has a single router with two exit links to different service providers). **Note** Only the syntax used in this context is displayed. For more details, see the *Cisco IOS Optimized Edge Routing Command Reference*, Release 12.4T.
Step 19	**policy-rules** *map-name* **Example:** Router(config-oer-mc)# policy-rules TARGET_MAP	Applies a configuration from an OER map to a master controller configuration in OER master controller configuration mode. • Reentering this command with a new OER map name will immediately overwrite the previous configuration. This behavior is designed to allow you to quickly select and switch between predefined OER maps. • The example applies the configuration from the OER map named TARGET_MAP.

	Command or Action	Purpose

Step 20	`end`
	
	Example:
	`Router(config-oer-mc)# end`
		Exits OER master controller configuration mode and enters privileged EXEC mode.

Step 21	`show oer master active-probes [appl	forced]`  **Example:** `Router# show oer master active-probes forced`	Displays connection and status information about active probes on an OER master controller. • The output from this command displays the active probe type and destination, the border router that is the source of the active probe, the target prefixes that are used for active probing, and whether the probe was learned or configured. • The **appl** keyword is used to filter the output to display information about applications optimized by the master controller. • The **forced** keyword is used to show any forced targets that are assigned. • The example displays connection and status information about the active probes generated for voice traffic configured with a forced target assignment.
Step 22	`show oer master policy [sequence-number	policy-name	default]`  **Example:** `Router# show oer master policy TARGET_MAP`	Displays policy settings on an OER master controller. • The output of this command displays default policy and policies configured with an OER map. • The *sequence-number* argument is used to display policy settings for the specified OER map sequence. • The *policy-name* argument is used to display policy settings for the specified OER policy map name. • The **default** keyword is used to display only the default policy settings. • The example displays the policy settings configured for the TARGET_MAP policy.

Examples

This example shows output from the **show oer master active-probes forced** command. The output is filtered to display only connection and status information about the active probes generated for voice traffic configured with a forced target assignment.

```
Router# show oer master active-probes forced

OER Master Controller active-probes
Border   = Border Router running this Probe
Policy   = Forced target is configure under this policy
Type     = Probe Type
Target   = Target Address
TPort    = Target Port
N - Not applicable
```

```
The following Forced Probes are running:

Border          State    Policy              Type      Target          TPort
10.20.20.2      ACTIVE   40                  jitter    10.20.22.1      3050
10.20.21.3      ACTIVE   40                  jitter    10.20.22.4      3050
```

What to do Next

For further configuration examples of OER voice traffic optimization, see the "Configuring OER Voice Traffic Optimization Using Active Probes: Examples" section on page 69.

Configuration Examples for Configuring and Applying OER Policies

The following examples in this section show various OER policy configurations:

Configuring and Applying an OER Policy to Learned Traffic Classes: Example

The following example uses learned traffic classes and overwrites many of the default policy settings and configures the master controller to move traffic classes to the best available exit link when any of the configured or default policy settings exceed their thresholds:

```
enable
configure terminal
oer master
 backoff 200 2000 200
 delay threshold 2000
 holddown 400
 loss threshold 1500
 periodic 180
 unreachable threshold 1000
 mode select-exit best
 end
```

Configuring and Applying an OER Policy to Configured Traffic Classes: Example

The following example uses traffic classes filtered by a prefix list and an access list and overwrites some of the default policy settings. The policies are configured using two OER maps that apply to different traffic classes that represent voice traffic. The master controller is configured to move traffic classes to the first in-policy exit link when any of the configured or default policy settings exceed their thresholds. To run this task, both the master controller and border routers must be running Cisco IOS Release 12.4(9)T, 12.2(33)SRB, or later releases.

```
enable
configure terminal
ip prefix-list CONFIG_TRAFFIC_CLASS seq 10 permit 10.1.5.0/24
ip access-list extended VOICE_TRAFFIC_CLASS
 permit udp any range 16384 32767 10.1.5.0 0.0.0.15 range 16384 32767 dscp ef
 exit
oer-map CONFIG_MAP 10
 match ip address prefix-list CONFIG_TRAFFIC_CLASS
 set backoff 100 1000 100
 set delay threshold 1000
 set loss relative 25
 set periodic 360
 set unreachable relative 20
 exit
oer-map VOICE_MAP 10
 match ip address access-list VOICE_TRAFFIC_CLASS
 set active-probe jitter 10.1.5.1 target-port 2000 codec g729a
 set probe-frequency 20
 set jitter threshold 30
 set mos threshold 4.0 percent 25
 set mode select-exit good
 end
```

Preventing OER Optimization of Learned Prefixes: Example

The following example shows how to configure OER to prevent specified prefixes being optimized. In this example, an IP prefix list is created with two entries for different prefixes that are not to be optimized. An OER map is configured with two entries in a sequence that will prevent OER from optimizing the prefixes specified in the prefix list, although the prefixes may be learned. If the sequence numbers of the OER map entries are reversed, OER will learn and attempt to optimize the prefixes.

```
enable
configure terminal
ip prefix-list DENY_PREFIX deny 172.17.10.0/24
ip prefix-list DENY_PREFIX deny 172.19.10.0/24
oer-map DENY_PREFIX_MAP 10
 match ip address prefix-list DENY_PREFIX
 exit
oer-map DENY_PREFIX_MAP 20
 match oer learn throughput
 end
```

Configuring and Applying an OER Policy to Learned Inside Prefixes: Example

The following example shows how to apply an OER policy to learned inside prefixes:

```
enable
configure terminal
oer-map INSIDE_LEARN 10
```

```
 match oer learn inside
 set delay threshold 2000
 set loss relative 20
 set unreachable relative 90
 end
```

Configuring and Applying an OER Policy to Configured Inside Prefixes: Example

The following example shows how to create an OER map named INSIDE_CONFIGURE and apply an OER policy to manually configured inside prefixes:

```
enable
configure terminal
 oer-map INSIDE_CONFIGURE 10
 match ip address prefix-list INSIDE_PREFIXES inside
 set delay threshold 2000
 set loss relative 20
 set unreachable relative 80
 end
```

Configuring Policy Rules for OER Maps: Example

The following example shows how to configure the **policy-rules** command to apply the OER map configuration named BLUE under OER master controller mode:

```
enable
configure terminal
oer-map BLUE 10
 match oer learn delay
 set loss relative 90
 exit
oer master
 policy-rules BLUE
 exit
```

Configuring Multiple OER Policy Conflict Resolution: Example

The following example configures an OER resolve policy that sets delay to the highest priority, followed by loss, and then utilization. The delay policy is configured to allow a 20 percent variance, the loss policy is configured to allow a 30 percent variance, and the utilization policy is configured to allow a 10 percent variance.

```
enable
configure terminal
oer master
 resolve delay priority 1 variance 20
 resolve loss priority 2 variance 30
 resolve utilization priority 3 variance 10
 end
```

Configuring an Exit Link Load Balancing OER Policy: Example

The following example configures an OER load balancing policy for traffic class flows over the border router exit links. This example task is performed at the master controller and configures an exit link utilization range and an exit link utilization threshold with policy priorities set for utilization and range policies. Performance policies, delay and loss, are disabled. OER uses both the utilization and range thresholds to load balance the traffic flow over the exit links.

```
enable
configure terminal
oer master
 max-range-utilization percentage 25
 mode select-exit best
 resolve range priority 1
 resolve utilization priority 2 variance 15
 no resolve delay
 no resolve loss
 border 10.1.4.1
 interface Ethernet 1/0 external
 max-xmit-utilization absolute 10000
 exit
 exit
 border 10.1.2.1
 interface Ethernet 1/0 external
 max-xmit-utilization absolute 10000
 end
```

Implementing Performance Routing Link Groups: Example

The following example shows how to implement link groups. In this example, an OER map named VIDEO_MAP is created to configure OER to define a traffic class that matches an access list named ACCESS_VIDEO. The traffic class is configured to use a link group named VIDEO as the primary link group, and a fallback group named VOICE. The VIDEO link group may be a set of high bandwidth links that are preferred for video traffic.

```
enable
configure terminal
border 10.1.4.1
 interface serial 2/0 external
  link-group VIDEO
  exit
 interface serial 3/0 external
  link-group VOICE
  exit
 interface Ethernet 1/0 internal
 exit
ip access-list extended ACCESS_VIDEO
 permit tcp any 10.1.1.0 0.0.0.255 eq 500
 permit tcp any 172.17.1.0 0.0.255.255 eq 500
 permit tcp any 172.17.1.0 0.0.255.255 range 700 750
 permit tcp 192.168.1.1 0.0.0.0 10.1.2.0 0.0.0.255 eq 800 any any dscp ef
 exit
oer-map VIDEO_MAP 10
 match traffic-class access-list ACCESS_VIDEO
 set link-group VIDEO fallback VOICE
 end
```

Configuring OER Cost-Based Policies: Example

The following example shows how to configure cost-based optimization on a master controller. Cost optimization configuration is applied under the external interface configuration. In this example, a policy for a tiered billing cycle is configured that sets a tiered fee of 1000 at 100 percent utilization, a tiered fee of 900 at 90 percent utilization, and a tiered fee of 800 at 80 percent utilization. Calculation is configured separately for egress and ingress samples. The time interval between sampling is set to 10 minutes and these samples are configured to be rolled up every 60 minutes.

```
enable
configure terminal
oer master
 border 10.5.5.55 key-chain key
 interface Ethernet 0/0 external
 cost-minimization nickname ISP1
 cost-minimization end day-of-month 30 180
 cost-minimization calc separate
 cost-minimization sampling 10 rollup 60
 cost-minimization tier 100 fee 1000
 cost-minimization tier 90 fee 900
 cost-minimization tier 80 fee 800
 exit
```

Configuring OER Network Security Policies: Examples

Black Hole Routing Example

The following example creates an OER map named BLACK_HOLE_MAP that matches traffic defined in the IP prefix list named PREFIX_BLACK_HOLE. The OER map filters packets to be forwarded to a null interface, meaning that the packets are discarded in a "black hole." The prefix list is configured after an IP prefix is identified as the source of the attack on the network.

```
enable
configure terminal
ip prefix-list PREFIX_BLACK_HOLE seq 10 permit 10.1.5.0/24
oer-map BLACK_HOLE_MAP 10
 match ip address prefix-list PREFIX_BLACK_HOLE
 set interface null0
 end
```

Sink Hole Routing Example

The following example creates an OER map named SINK_HOLE_MAP that matches traffic defined in the IP prefix list named PREFIX_SINK_HOLE. The OER map filters packets to be forwarded to a next hop. The next hop is a router where the packets can be stored, analyzed, or discarded (the sinkhole analogy). The prefix list is configured after an IP prefix is identified as the source of an attack on the network.

```
enable
configure terminal
ip prefix-list PREFIX_SINK_HOLE seq 10 permit 10.1.5.0/24
oer-map SINK_HOLE_MAP 10
 match ip address prefix-list PREFIX_SINK_HOLE
 set next-hop 10.1.1.3
 end
```

Configuring OER Voice Traffic Optimization Using Active Probes: Examples

Voice packets traveling through an IP network are no different from data packets. In the plain old telephone system (POTS), voice traffic travels over circuit-switched networks with predetermined paths and each phone call is given a dedicated connection for the duration of the call. Voice traffic using POTS has no resource contention issues, but voice traffic over an IP network has to contend with factors such as delay, jitter, and packet loss, which can affect the quality of the phone call.

The following examples show both how to use an access list to identify only voice traffic to be optimized by OER and to use a prefix list to identify traffic that includes voice traffic to be optimized by OER.

Optimizing Only Voice Traffic Using Active Probes

Figure 6 shows that voice traffic originating at the remote office and terminating at the headquarters has to be optimized to select the best path out of the remote office network. Degradation in voice (traffic) quality is less likely to be introduced within the network, so probing the edge of the network gives a measurement that is close to probing the final destination.

Figure 6   OER Network Topology Optimizing Voice Traffic Using Active Probes
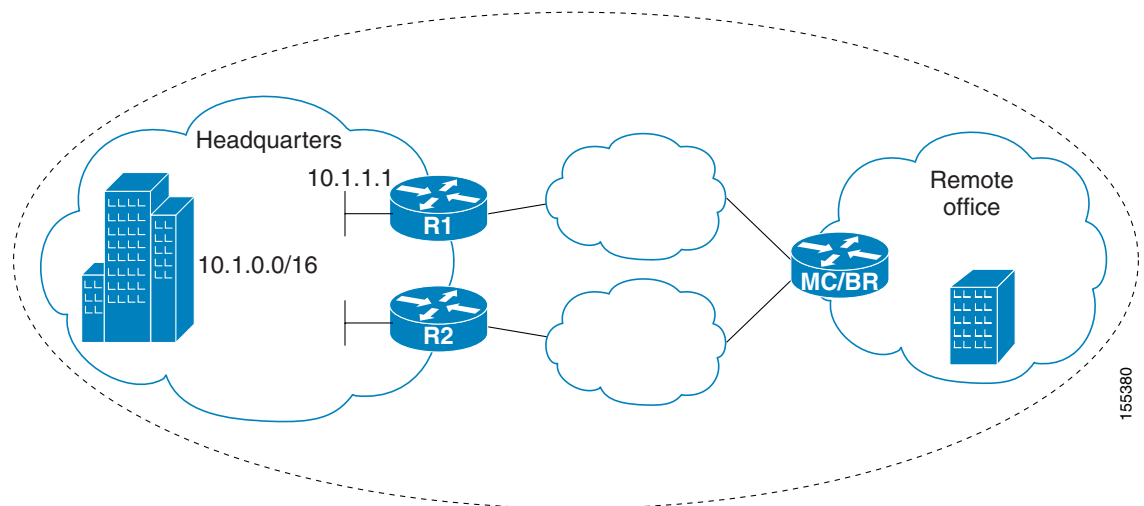
This configuration optimizes voice traffic to use the best performance path, whereas all other traffic destined to the same network—10.1.0.0/16—will follow the best path as indicated by a traditional routing protocol, for example BGP, that is configured on the device. As part of this optimization, OER will use policy based routing (PBR) to set the best exit link for voice traffic within a device.

The following configuration is performed on the edge router R1 in Figure 6 in the headquarters network to enable the IP SLAs Responder.

```
enable
configure terminal
 ip sla responder
 exit
```

The following configuration is performed on the edge router MC/BR (which is both an OER master controller and border router) in Figure 6 in the remote office network to optimize voice traffic using active probes.

```
enable
configure terminal
ip access-list extended Voice_Traffic
 10 permit udp any 10.1.0.0 0.0.255.255 range 16384 32767
 exit
oer-map Voice_MAP 10
 match ip address access-list Voice_Traffic
 set active-probe jitter 10.1.1.1 target-port 1025 codec g711alaw
 set delay threshold 300
 set mos threshold 3.76 percent 30
 set jitter threshold 15
 set loss relative 5
 resolve mos priority 1
 resolve jitter priority 2
 resolve delay priority 3
 resolve loss priority 4
```

Optimizing Traffic (Including Voice Traffic) Using Active Probes

Figure 7 shows that traffic originating in the headquarters network and destined for the remote office network has to be optimized based on voice traffic metrics. Voice traffic is one of the most important traffic classes that travel from the headquarters to the remote office network, so the voice traffic must be prioritized to be optimized. Degradation in voice packet quality is less likely to be introduced within the network, so probing the edge of the network gives a measurement that is close to probing the final destination.

Figure 7   OER Network Topology for Optimizing All Traffic Using Active Probes
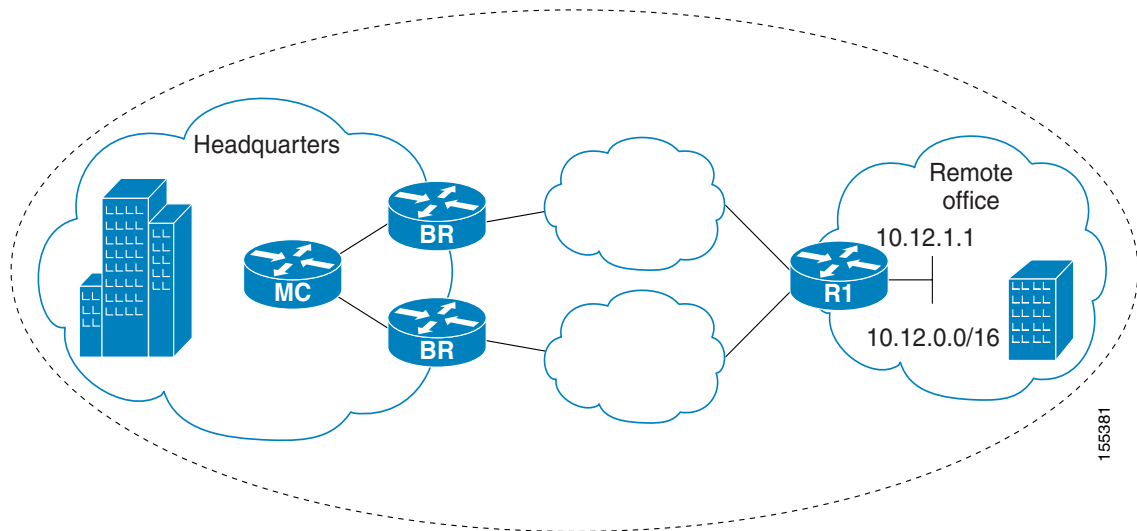
This configuration optimizes all traffic, including voice traffic, destined for the 10.12.0.0/16 network. The OER optimization is based on the measurement of voice performance metrics with threshold values using active probes. As part of the optimization, OER will introduce a BGP or a static route into the headquarters network. For more details about BGP and static route optimization, see the Using OER to Control Traffic Classes and Verify the Route Control Changes module.

The following configuration is performed on router R1 in Figure 7 in the remote office network to enable the IP SLAs Responder.

```
enable
configure terminal
 ip sla responder
 exit
```

The following configuration is performed on one of the BR routers in Figure 7 in the headquarters network to optimize all traffic (including voice traffic) using active probes.

```
enable
configure terminal
 ip prefix-list All_Traffic_Prefix permit 10.12.0.0/16
 oer-map Traffic_MAP 10
 match ip address prefix-list All_Traffic_Prefix
 set active-probe jitter 10.12.1.1 target-port 1025 codec g711alaw
! port 1025 for the target probe is an example.
 set delay threshold 300
 set mos threshold 3.76 percent 30
 set jitter threshold 15
 set loss relative 5
 resolve mos priority 1
 resolve jitter priority 2
 resolve delay priority 3
 resolve loss priority 4
```

Where to Go Next

This module covered the OER apply policy phase and it has assumed that you started with the "Cisco IOS Optimized Edge Routing Overview" and the "Setting Up OER Network Components" module. The apply policy phase is the third phase in the OER performance loop. To learn more about the other OER phases, read through the other modules in the following list:

- Using OER to Profile the Traffic Classes
- Measuring the Traffic Class Performance and Link Utilization Using OER
- Configuring and Applying OER Policies
- Using OER to Control Traffic Classes and Verify the Route Control Changes

After you understand the various OER phases, review the OER solutions modules that are listed under "Related Documents" section on page 71.

Additional References

The following sections provide references related to configuring and applying OER policies.

Related Documents

Related Topic	Document Title
Cisco OER technology overview	"Cisco IOS Optimized Edge Routing Overview" module
Concepts and configuration tasks required to set up OER network components.	"Setting Up OER Network Components" module

Related Topic	Document Title
OER solution module: voice traffic optimization using OER active probes.	"OER Voice Traffic Optimization Using Active Probes" module
OER solution module: configuring VPN IPsec/GRE tunnel interfaces as OER-managed exit links.	"Configuring VPN IPsec/GRE Tunnel Interfaces As OER-Managed Exit Links" module
Cisco OER commands: complete command syntax, command mode, command history, defaults, usage guidelines and examples	• *Cisco IOS Optimized Edge Routing Command Reference*, Release 12.4T • *Cisco IOS Optimized Edge Routing Command Reference*, Release 12.2 SR
IP Routing Protocol commands	• *Cisco IOS IP Routing Protocols Command Reference*, Release 12.4T • *Cisco IOS IP Routing Protocols Command Reference*, Release 12.2SR
IP Routing Protocol configuration tasks	*Cisco IOS IP Routing Protocols Configuration Guide*, Release 12.4

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and technical documentation. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for Configuring and Applying OER Policies

Table 1 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.3(8)T, 12.2(33)SRB, or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the "Cisco IOS Optimized Edge Routing Feature Roadmap."

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1   Feature Information for Configuring and Applying OER Policies

Feature Name	Releases	Feature Configuration Information
Optimized Edge Routing	12.3(8)T 12.2(33)SRB	OER was introduced.
OER Support for Policy-Rules Configuration	12.3(11)T 12.2(33)SRB	The OER Support for Policy-Rules Configuration feature introduced the capability to select an OER map and apply the configuration under OER master controller configuration mode, providing an improved method to switch between predefined OER maps. The following sections provide information about this feature: • Policy Rules Configuration to Apply an OER Policy, page 13 • Configuring Policy Rules for OER Maps, page 35 • Configuring Policy Rules for OER Maps: Example, page 66 The following commands were introduced or modified by this feature: **policy-rules**.

Table 1   *Feature Information for Configuring and Applying OER Policies (continued)*

Feature Name	Releases	Feature Configuration Information
OER Support for Cost-Based Optimization	12.3(14)T 12.2(33)SRB	The OER Support for Cost-Based Optimization feature introduced the capability to configure exit link policies based monetary cost and the capability to configure traceroute probes to determine prefix characteristics on a hop-by-hop basis. The following sections provide information about this feature: • OER Link Policies, page 6 • Configuring OER Cost-Based Policies, page 47 • Configuring OER Cost-Based Policies: Example, page 68 The following commands were introduced or modified by this feature: **cost-minimization**, **debug oer master cost-minimization**, **show oer master cost-minimization**.
OER Voice Traffic Optimization	12.4(6)T 12.2(33)SRB	The OER Voice Traffic Optimization feature introduced support for outbound optimization of voice traffic based on the voice metrics, jitter and Mean Opinion Score (MOS). Jitter and MOS are important quantitative quality metrics for voice traffic and these voice metrics are measured using OER active probes. The following sections provide information about this feature: • OER Traffic Class Performance Policies, page 5 • Configuring OER Voice Traffic Optimization Using Active Probes, page 54 • Configuring OER Voice Traffic Optimization Using Active Probes: Examples, page 69 The following commands were introduced or modified by this feature: **active-probe**, **jitter**, **mos**, **resolve**, **set jitter**, **set mos**, **set probe**, **set resolve**, **show oer master active-probes**, **show oer master policy**, **show oer master prefix**.

Table 1　　　**Feature Information for Configuring and Applying OER Policies (continued)**

Feature Name	Releases	Feature Configuration Information
OER BGP Inbound Optimization	12.4(9)T 12.2(33)SRB	OER BGP inbound optimization supports best entrance selection for traffic that originates from prefixes outside an autonomous system destined for prefixes inside the autonomous system. External BGP (eBGP) advertisements from an autonomous system to an Internet service provider (ISP) can influence the entrance path for traffic entering the network. OER uses eBGP advertisements to manipulate the best entrance selection. The following sections provide information about this feature: • Configuring and Applying an OER Policy to Learned Inside Prefixes, page 29 • Configuring and Applying an OER Policy to Configured Inside Prefixes, page 32 • Configuring and Applying an OER Policy to Learned Inside Prefixes: Example, page 65 • Configuring and Applying an OER Policy to Configured Inside Prefixes: Example, page 66 The following commands were introduced or modified by this feature: **clear oer master prefix**, **downgrade bgp**, **inside bgp**, **match ip address (OER)**, **match oer learn**, **max range receive**, **maximum utilization receive**, **show oer master prefix**.

Table 1   Feature Information for Configuring and Applying OER Policies (continued)

Feature Name	Releases	Feature Configuration Information
OER DSCP Monitoring	12.4(9)T 12.2(33)SRB	OER DSCP Monitoring introduced automatic learning of traffic classes based on protocol, port numbers, and DSCP value. Traffic classes can be defined by a combination of keys comprising of protocol, port numbers, and DSCP values, with the ability to filter out traffic that is not required, and the ability to aggregate the traffic in which you are interested. Information such as protocol, port number, and DSCP information is now sent to the master controller database in addition to the prefix information. The new functionality allows OER to both actively and passively monitor application traffic. The following sections provide information about this feature: • OER Traffic Class Performance Policies, page 5 • OER Policy Application, page 12 • Configuring and Applying an OER Policy to Configured Traffic Classes, page 18 • Configuring and Applying an OER Policy to Configured Traffic Classes: Example, page 65 The following commands were introduced or modified by this feature: **show oer border passive applications**, **show oer border passive cache**, **show oer border passive learn**, **show oer master appl**, **traffic-class aggregation**, **traffic-class filter**, and **traffic-class keys**.
Performance Routing - Link Groups	12.4(15)T	The Performance Routing - Link Groups feature introduces the ability to define a group of exit links as a preferred set of links, or a fallback set of links for OER to use when optimizing traffic classes specified in an OER policy. The following sections provide information about this feature: • Performance Routing Link Grouping, page 9 • Implementing Performance Routing Link Groups, page 42 • Implementing Performance Routing Link Groups: Example, page 67 The following commands were introduced or modified by this feature: **link-group**, **set link-group**, and **show oer master link-group**.