Cisco OER Master Controller Engine GUI

This chapter provides information about how to use the Cisco OER Master Controller Engine Web-based graphical user interface (GUI).

Access Modes

There are two access modes to the Cisco OER Master Controller Engine:

- Normal
- Secure

Normal mode uses HTTP basic authentication that sends the password in clear text to the server.

Secure mode uses the Secure Sockets Layer (SSL) for login from a Web browser. Once logged in, the Cisco OER Master Controller Engine GUI shows a series of tabs for various system maintenance, configurations, and reporting functions.

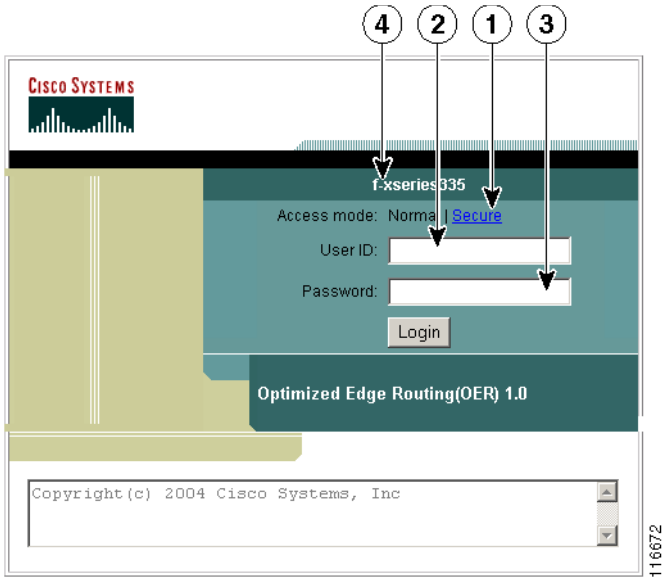
Step 1 To access this user interface, launch your Web browser.

Step 2 Go to:

http://<hostname>:8080/,or **http://<ipaddress>:8080/**

The login page appears (see Figure 2-1).

Figure 2-1 Login Page



1	Secure (https) login option.	**3**	Password dialog block.
2	User ID dialog block.	**4**	Appliance hostname.

If you want to use HTTPS, select **Secure** and continue to login.

Step 3 Enter the default Username:

admin

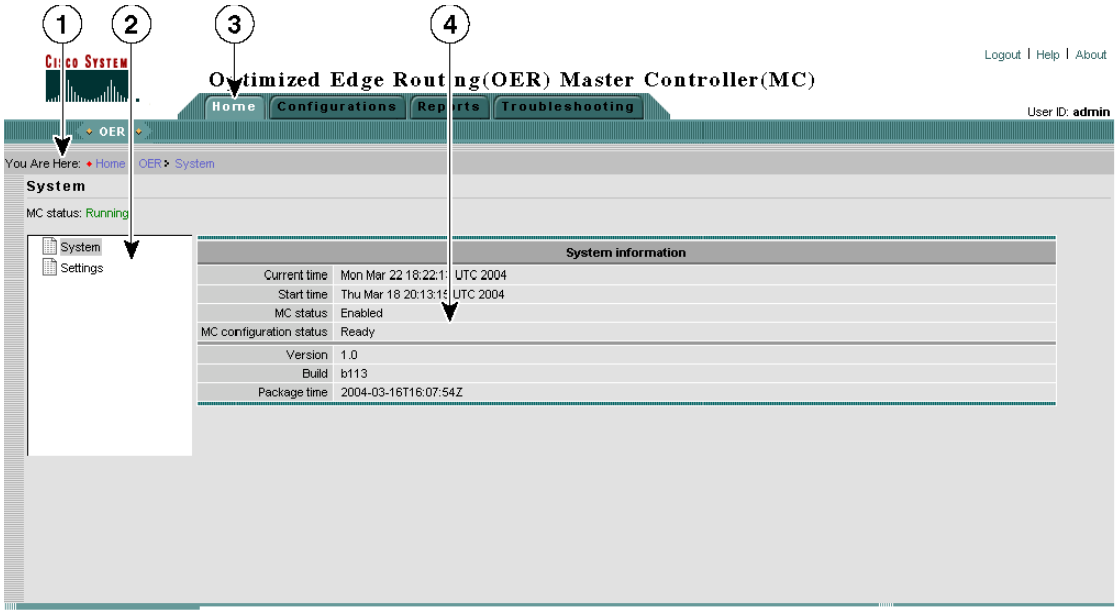
Step 4 Enter the default password:

cisco

The Optimized Edge Routing (OER) Master Controller (MC) Home page appears (see Figure 2-2).

For security reasons, you should change this password. To do this, skip forward to the "Settings - Change Web Password" section on page 2-5.

Figure 2-2 Home Page



1	Context line that shows path to the current function. Click any link in this area to go back to the associated window.	**3**	Tabs for accessing main functions: tabs are displayed in every window in user interface (except in detail pop-up windows).
2	Contents of functions related to the current context.	**4**	Content area where graphs, tables, dialog boxes, charts, and instruction boxes are displayed.

Main Functions

The Cisco OER Master Controller Engine user interface provides four main functions:

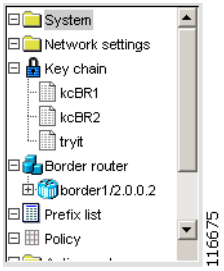
Figure 2-3 Main Function Tabs

- Home
- Configurations
- Reports
- Troubleshooting

Subfunctions

Each main function is further subdivided into subfunctions, which are shown as a tree structure (see Figure 2-4) of the Contents for the Current Context (see callout **1** in Figure 2-2).

Figure 2-4 Contents of Current Context (Subfunctions)



Home

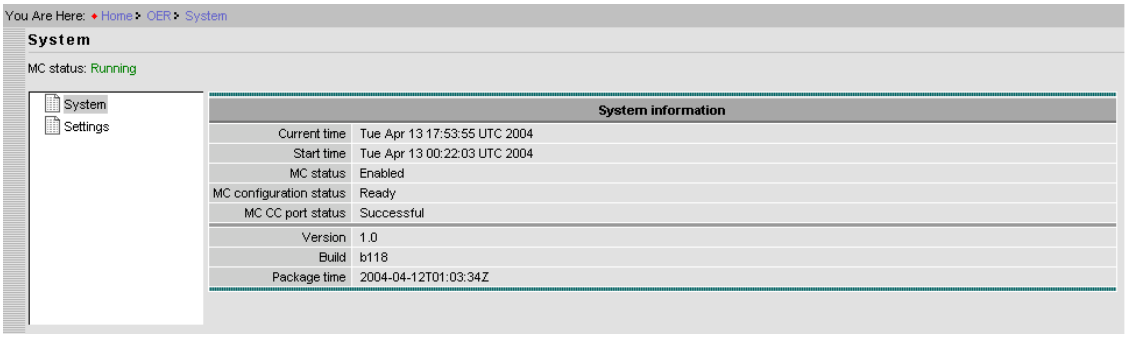
The Home function provides access to system-level information:

- System Status
- Settings

System Status

System status shows the following information:

Figure 2-5 System Status



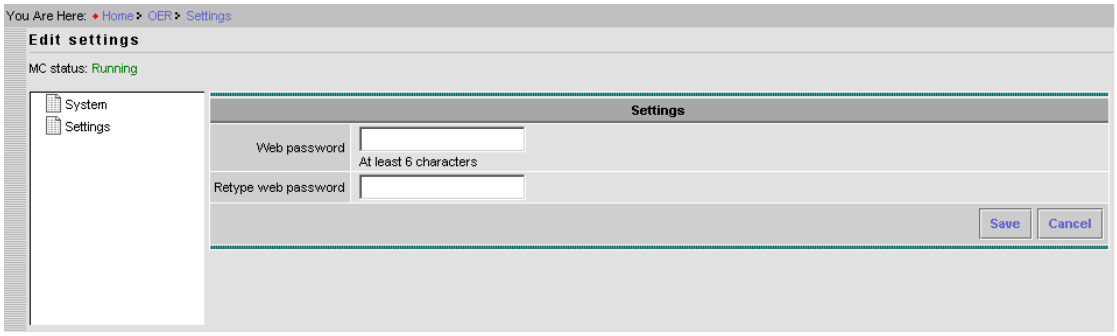
Current time	UTC.
Start time	Time (UTC) when Cisco OER Master Controller Engine was started.
MC status	Whether the Cisco OER Master Controller Engine is enabled or disabled.

MC configuration status	Whether the Cisco OER Master Controller Engine is ready to operate, or not. The minimum configuration requirements for operation (Ready) are: • Each valid border router should have at least one internal interface and one external interface configured and in the UP state. • Total of at least two external interfaces and one internal interface configured and in the UP state on any valid border router. To view the status of border routers go to **Configurations > Border Router** (see Figure 2-14).
MC CC port status	Communication Controller port number currently configured.
Version	Cisco OER Master Controller Engine software version.
Build	Package build type (Release).
Package time	Time (UTC) when build completed.

Settings - Change Web Password

The Settings functions allows you to change the Web password to the user interface:

Figure 2-6 Home > Edit Settings > Change Web Password



Step 1 Enter your new Web password.

Step 2 Enter your new Web password again.

Step 3 To cancel this operation, click **Cancel**.

Step 4 To apply your new Web password, click **Save**.

Configurations

The Configurations main function is divided into two levels:

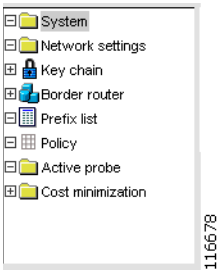
- Basic
- Advanced

At the Basic configuration level, the Cisco OER Master Controller Engine does performance and load balancing functions.

The Advanced configuration level allows you to use the Cisco OER Master Controller Engine to configure custom policies for optimization; including cost optimization for tier links.

The subfunctions (contents list) of the Configurations main function are shown in Figure 2-7.

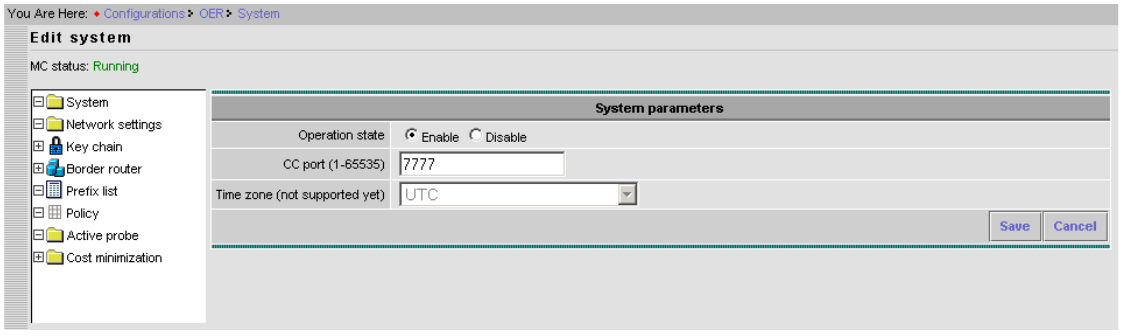
Figure 2-7 Configurations Contents List



System

The System Configurations subfunction allows you to change the system-level settings shown in Figure 2-8.

Figure 2-8 Configurations > System > Edit Settings



Step 1 Accept **Enable** as the default **Operation state**, or click **Disable**.

In **Enable** state, the Cisco OER Master Controller Engine functions per policy and other configuration parameters.

In **Disable** state, the Cisco OER Master Controller Engine stops functioning and allows the configuration to be modified, but does not monitor or control prefixes. The connection between the Cisco OER Master Controller Engine and border routers is disabled.

Step 2 Accept the current value in the **CC port** field, or enter a new value.

CC is the Cisco OER Master Controller Engine Communication Controller that provides messaging with border routers. The **CC port** number must be configured on the Cisco OER Master Controller Engine and all border routers (that are participating in Optimized Edge Routing).

The range of port numbers is **1** to **65535**.

This port cannot be in use by any other application executing on the Cisco OER Master Controller Engine host.

The order of configuration on the Cisco OER Master Controller Engine and border routers in not critical, but all must use the same port number.

Editing the **Time zon**e field is not supported.

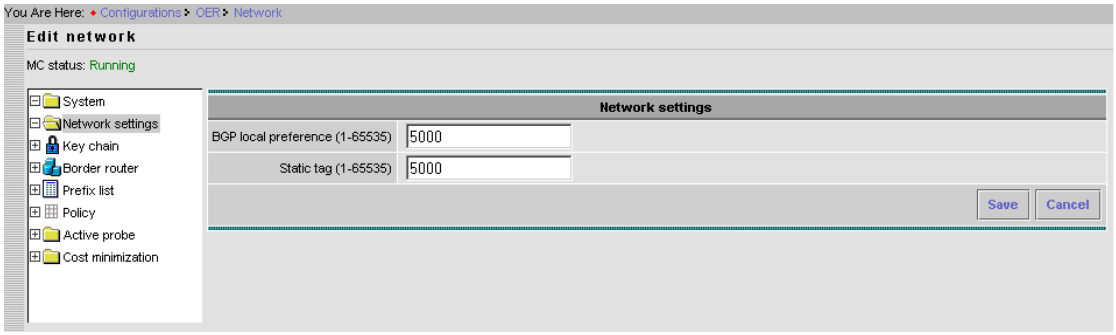
Step 3 To cancel this operation, click **Cancel**.

Step 4 To save settings, click **Save**.

Network Settings

The Network Settings parameters in this subfunction apply globally, not to any individual prefix or exit.

Figure 2-9 Configurations > Network Settings > Edit Network



Step 1 Enter a value for **BGP local preference**.

The Cisco OER Master Controller Engine controls a BGP route by setting high local preference. This setting allows you change the local preference used by the Cisco OER Master Controller Engine.

System default value is **5000**.

Step 2 Enter a value for **Static tag**.

This is similar to BGP local preference, but it is used with static routes.

System default value is **5000**.

Step 3 To cancel this operation, click **Cancel**.

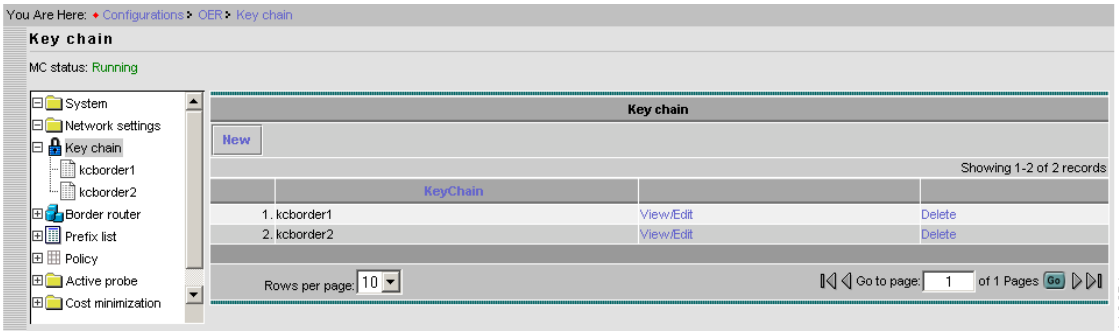
Step 4 To save settings, click **Save**.

Key Chain

Authentication between the Cisco OER Master Controller Engine and associated border routers is mandatory. Key chains are used for this purpose.

More than one key can be configure per key chain. Key chains configured in this subfunction (see Figure 2-10) are used in border router configurations. The same key chain must also be configured on the associated border router. The border router can be configured through a console port, or in-band port, over the internet. You cannot use the Cisco OER Master Controller Engine to configure the border router.

Figure 2-10 Configurations > Key Chain

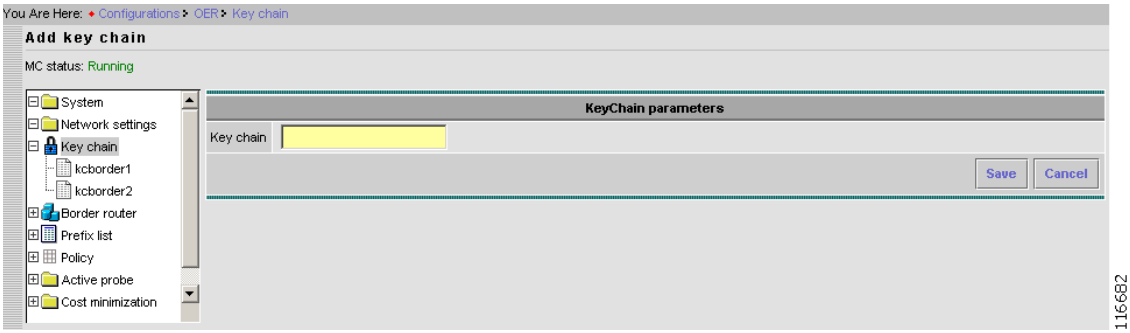


KeyChain	Name of a key chain. A key chain must have at least one key.
Keys	Identification number of a key in the key chain.

New Key Chain

In the Key Chain window, click **New**.

Figure 2-11 Configurations > Key Chain > Add Key Chain



Step 1 Enter name of new **Key chain**.

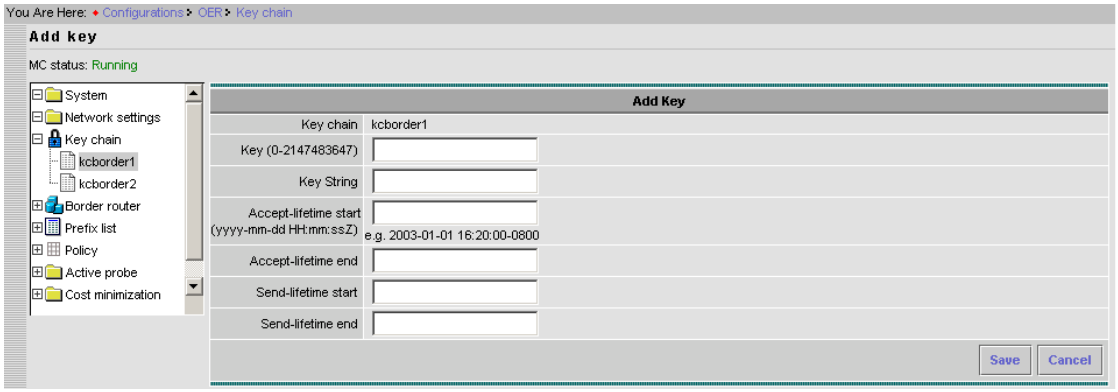
Step 2 To cancel this operation, click **Cancel**.

Step 3 To save settings, click **Save**.

Add Key to Key Chain

Select a key chain, then in that key chain window click, **Add new** (see Figure 2-12).

Figure 2-12 Configurations > Key Chain > Add Key



Step 1 Enter a **Key** identification number.

Step 2 Enter the **Key String**.

Authentication string for the **Key** that must be sent and received in the packets to and from border router.

Same string must be configured on the border router.

Note **Accept-lifetime start/end** and **Send-lifetime start/end** are not supported in this release.

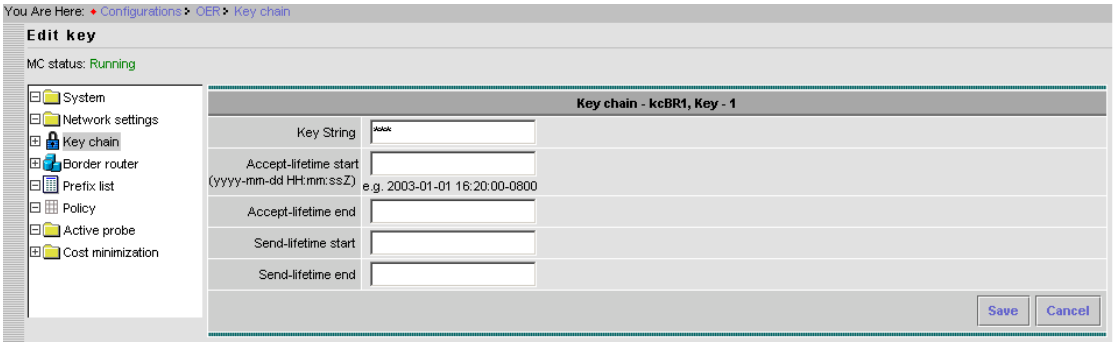
Step 3 To cancel this operation, click **Cancel**.

Step 4 To save settings, click **Save**.

Edit Key Chain

Select a key chain, then in that key chain window click, **View/Edit**.

Figure 2-13 Configurations > Key Chain > Edit Key



Step 1 Enter a new **Key String**.

This is the authentication string for the **Key** that must be sent and received in the packets to and from the border router.

Same string must be configured on the border router.

Note **Accept-lifetime start/end** and **Send-lifetime start/end** are not supported in this release.

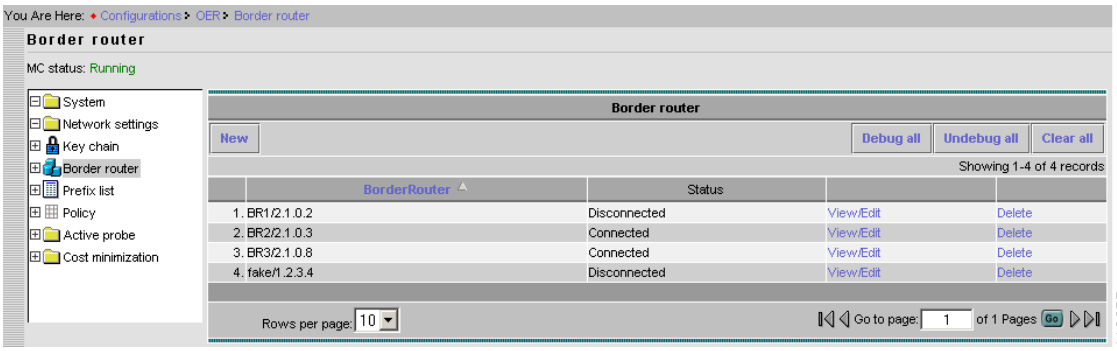
Step 2 To cancel this operation, click **Cancel**.

Step 3 To save settings, click **Save**.

Border Router

The Border Router subfunction allows you to configure parameters pertaining to border routers.

Figure 2-14 Configurations > Border Router

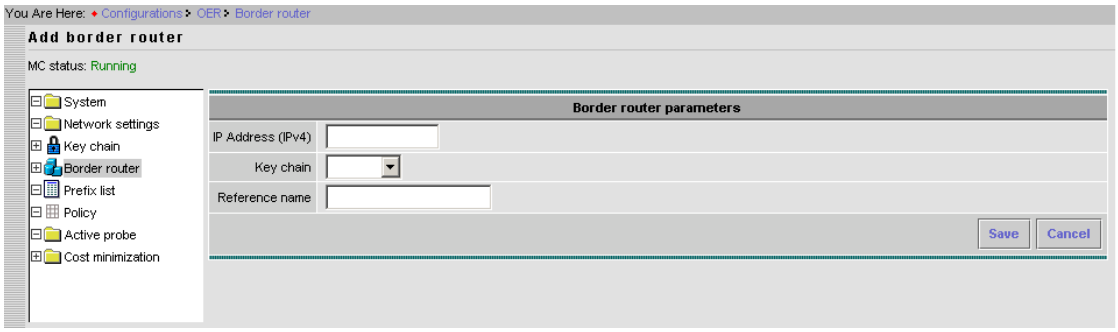


New Border Router

New border router configurations includes configuring the IP address of the border router, key chain used for authentication, and reference name of the border router.

From the **Border router** page, click **New**.

Figure 2-15 Configurations > Border Router > Add Border Router



Step 1 Enter a valid **IP address** for the border router.

IP address of the border router should be the IP address configured on the local interface on the border router. This IP address is used by the border router as a source address to communicate with the Cisco OER Master Controller Engine.

Step 2 Select a **Key chain** from previously configured key chains in the pull-down menu.

Key chain selection is mandatory.

Step 3 Enter a **Reference name**.

The Reference Name is a string used to identify a specific border router. This string is only used to identify a border router in the **Report** main function, and does not have any other meaning.

Unless this also the DNS name, the Reference Name is not pingable.

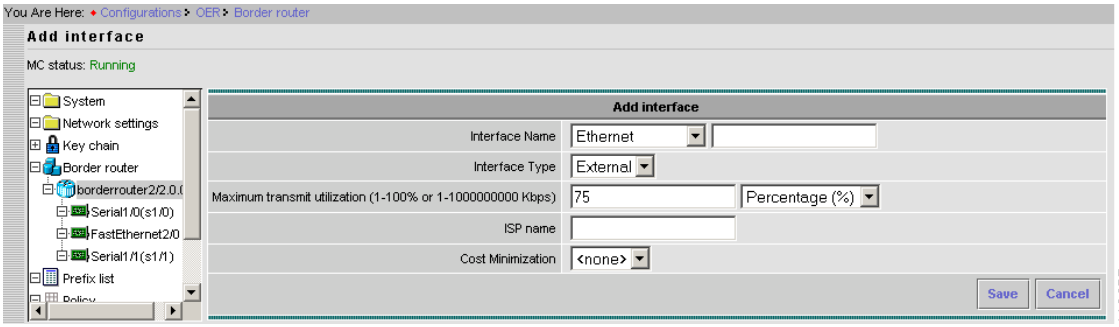
Step 4 To cancel this operation, click **Cancel**.

Step 5 To save settings, click **Save**.

New Interface

To add a new interface, from a selected border router page, click **New interface**.

Figure 2-16 Configurations > Border Router > Add Interface



Step 1 Enter an **Interface Name**.

Interface Name consists of two parts: **name string** and **slot number**.

A pull-down menu for name string is provided along with a field for slot number next to it.

Tip Do not enter interface name and slot identifier for the slot number. For example, **Ethernet** is a valid Interface Name, and **1/1** is a valid slot number, but **s1/1** is not a valid slot number.

Note The slot number is not checked for validity at entry time. However, when the border router connects to the Cisco OER Master Controller Engine, it verifies the configuration interface. If the configured interface is not valid, the status of the interface is set to *Verified invalid*.

Step 2 Select **Interface Type**.

There are two types of Interfaces selected from the pull-down menu:

a. External Interface (faces an ISP) > continue to Step 3.

b. Internal Interface (faces the enterprise) > jump to Step 6.

Step 3 Enter a value for the **Maximum transmit utilization**.

This is a threshold for an Exit policy. If the utilization of Exit is more than the configured threshold, then Exit is considered *Out of policy* and the Cisco OER Master Controller Engine takes an action to reduce it.

The threshold can be specified in terms of absolute bandwidth (kbps) or in terms of percentage of total capacity.

System default value is 75%.

This is only valid for External Interfaces.

Step 4 Enter an **ISP name**.

A string used to identify an ISP, which is only valid for External Interfaces.

This name can be the name of the ISP connected to that interface.

This name is used in the **Report** main function.

Step 5 Select **Cost Minimization** type.

The drop-down menu allows you to select a user-configured Cost Minimization.

Cost Minimization types are the billing criteria that are established with each ISP. For more information about Cost Minimization, see "Cost Minimization" section on page 2-27.

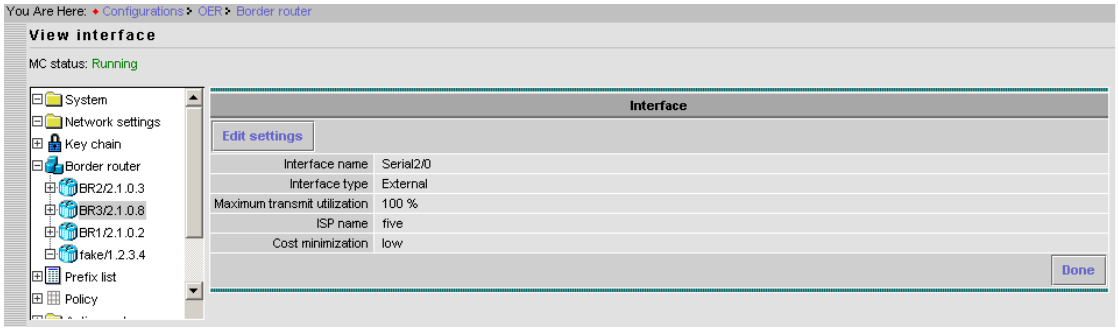
Step 6 To cancel this operation, click **Cancel**.

Step 7 To save settings, click **Save**.

View Border Router Interface

From the selected border router page, select the interface, then click **View/Edit**.

Figure 2-17 Configurations > Border Router > Interface > View Interface

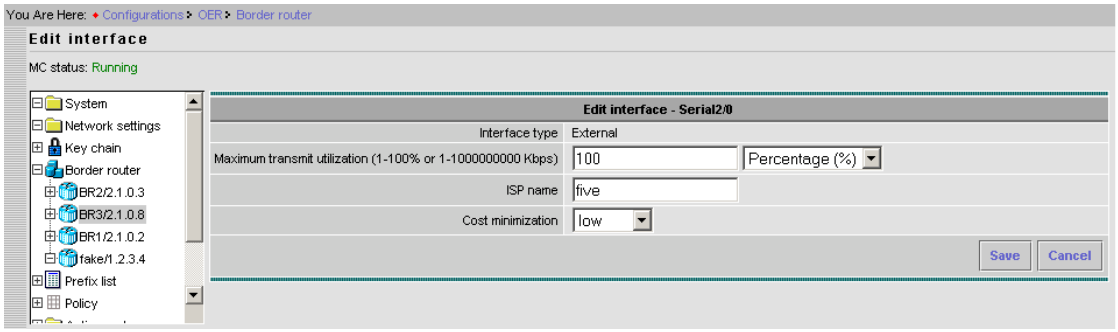


When finished, click **Done**.

Edit Border Router Interface

To edit the selected border router interface parameters, click **Edit Settings**.

Figure 2-18 Configurations > Border Router > Interface > Edit Interface



Step 1 Enter a new value for the **Maximum transmit utilization**.

This is a threshold for an Exit policy. If the utilization of Exit is more than the configured threshold, then Exit is considered *Out of policy* and the Cisco OER Master Controller Engine takes an action to reduce it.

The threshold can be specified in terms of absolute bandwidth (kbps) or in terms of percentage of total capacity.

System default value is 75%.

This is only valid for External Interfaces.

Step 2 Enter an **ISP name**.

A string used to identify an ISP, which is only valid for External Interfaces.

This name can be the name of the ISP connected to that interface.

This name is used in the **Report** main function.

Step 3 Select a **Cost minimization** type.

The drop-down menu allows you to select a user-configured Cost Minimization type.

Cost Minimization types are the billing criteria that are established with each ISP. For more information about Cost Minimization, see "Cost Minimization" section on page 2-27.

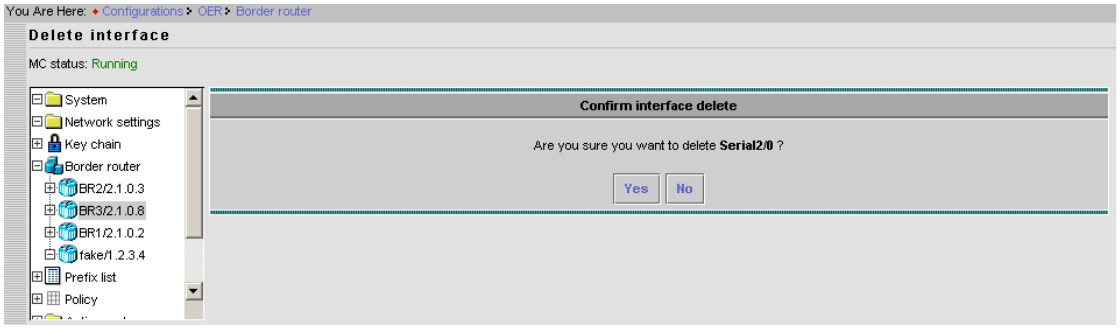
Step 4 To cancel this operation, click **Cancel**.

Step 5 To save settings, click **Save**.

Delete Border Router Interface

From the selected border router page, to delete the selected interface, click **Delete**.

Figure 2-19 Configurations > Border Router > Interface > Delete Interface



Prefix List

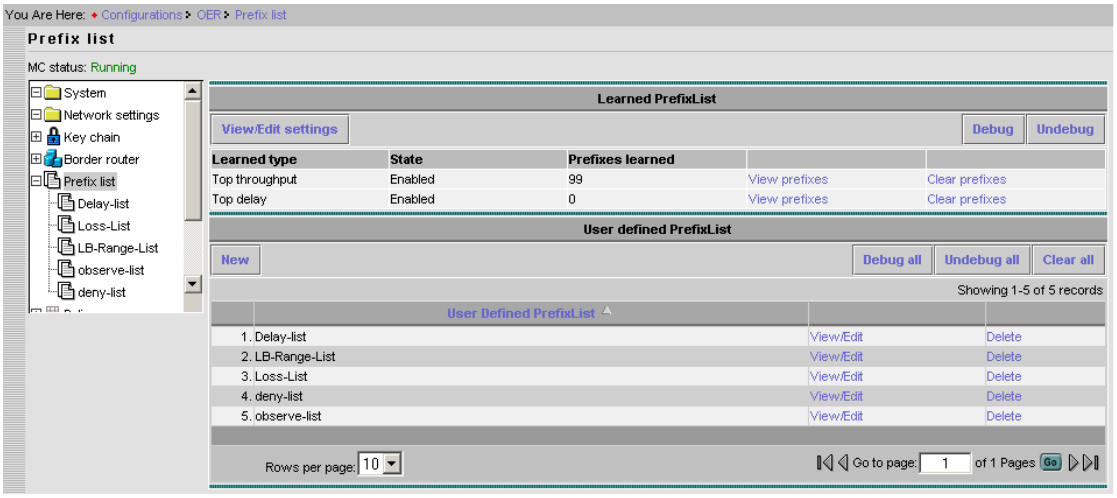
There are two types of prefix lists:

- Learned prefix.
- User-defined prefix.

Prefixes are learned based on the configured settings for learned prefixes and are added or deleted dynamically to the learned prefix lists.

Prefixes in user-defined prefix lists are added or deleted manually.

Figure 2-20 Configurations > Prefix List



Learned Prefix List

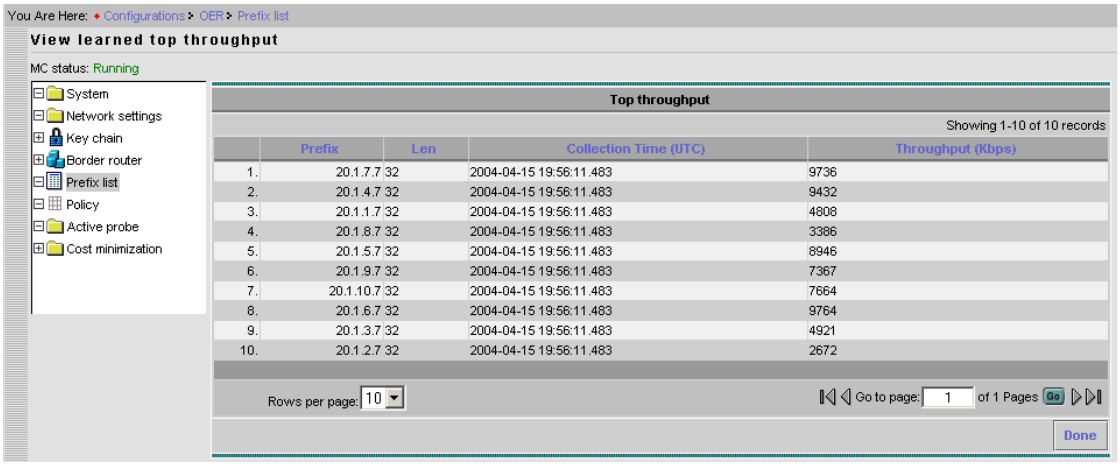
There are two types of learned prefix lists:

- Top throughput
- Top delay

View Top Throughput Prefixes

From the Prefix List page, for Top throughput, click **View prefixes**.

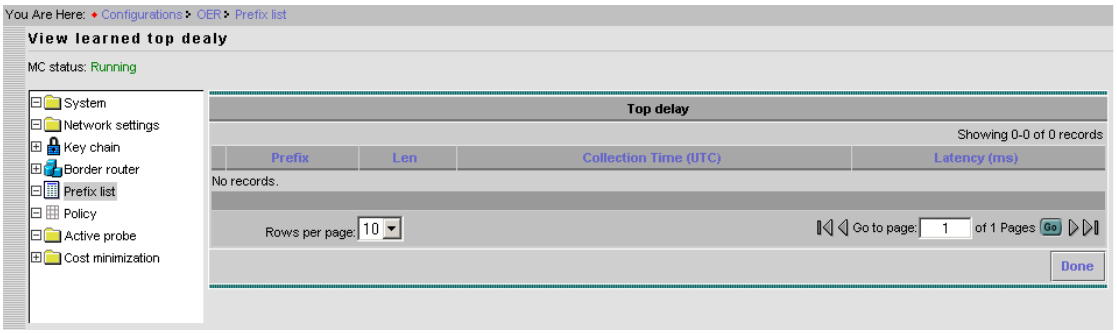
Figure 2-21 Configurations > Prefix List > View Prefixes for Top Throughput



View Top Delay Prefixes

From the Prefix List page, for Top delay, click **View prefixes**.

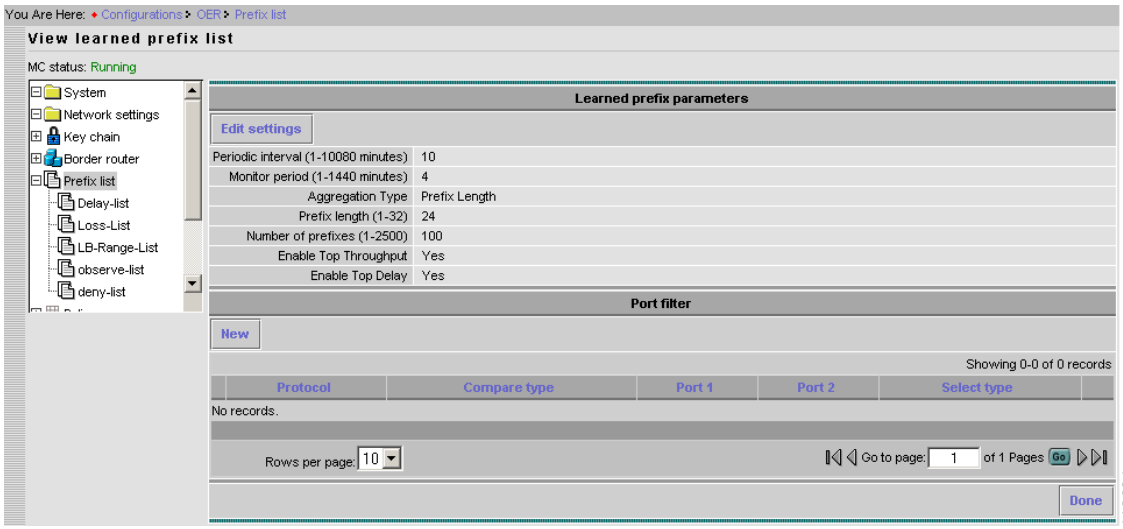
Figure 2-22 Configurations > Prefix List > View Prefixes for Top Delay



View Learned Prefix List Settings

From the Learned Prefix List page, click **View/Edit settings**.

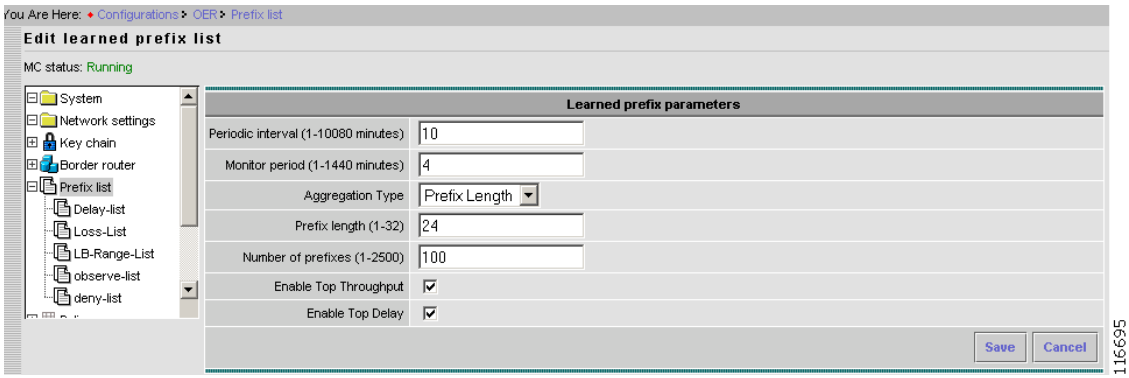
Figure 2-23 Configurations > Prefix List > View Learned Prefix List



Edit Learned Prefix List Settings

From the Learned prefix parameters page, click **Edit settings**.

Figure 2-24 Configurations > Prefix List > Edit Learned Prefix List



Step 1 Enter a value for **Periodic interval**.

The time interval in minutes between two successive learning sessions.

Step 2 Enter a value for **Monitor period**.

The time period in minutes traffic is monitored to determine top-throughput prefixes and top-delay prefixes.

Step 3 Select an **Aggregation Type** from the pull-down menu.

Prefix Length – Prefixes defined by prefix length or prefixes in the RIB with length higher than the prefix length.

Static Routes – Prefixes defined by static routes configured on the border.

BGP – Prefixes defined by prefixes found in BGP routing table on the border.

Step 4 Enter a value for **Prefix length**.

Used only if the **Aggregations Type** is **Prefix Length**.

Step 5 Enter a value for **Number of prefixes**.

The maximum number of top-throughput and top-delay prefixes to be learnt.

Step 6 Click **Enable Top Throughput** check box.

Check box to **Enable** or **Disable** learning prefixes based on Top Throughput.

Step 7 Click **Enable Top Delay** check box.

Check box to **Enable** or **Disable** learning prefixes based on Top Delay.

Step 8 To cancel this operation, click **Cancel**.

Step 9 To save settings, click **Save**.

User-defined Prefix List

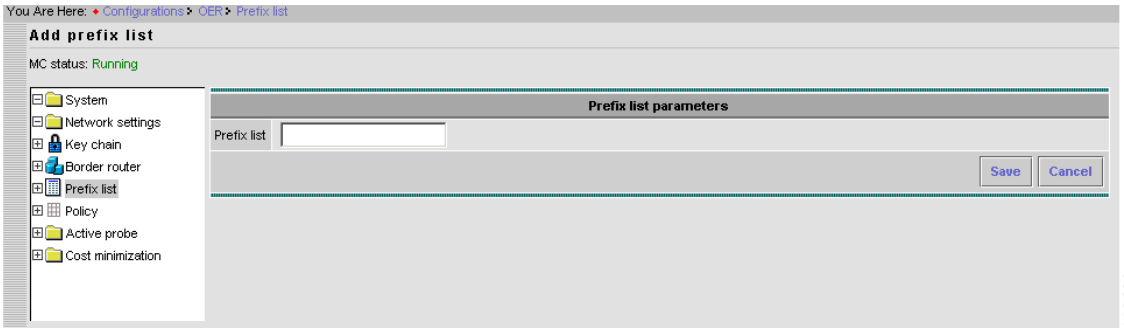
You can create one or more user-defined prefix lists. The use of prefix lists is to assign user policy to a group of user prefixes.

Prefixes are added or deleted by editing prefix list.

Add User-defined Prefix List

From the Prefix List page, in the User-defined Prefix List pane, click **New**.

Figure 2-25 Configurations > Prefix List > User-defined > Add Prefix List



Step 1 Enter the name (type) of the **Prefix list**.

For example, **observe-list**.

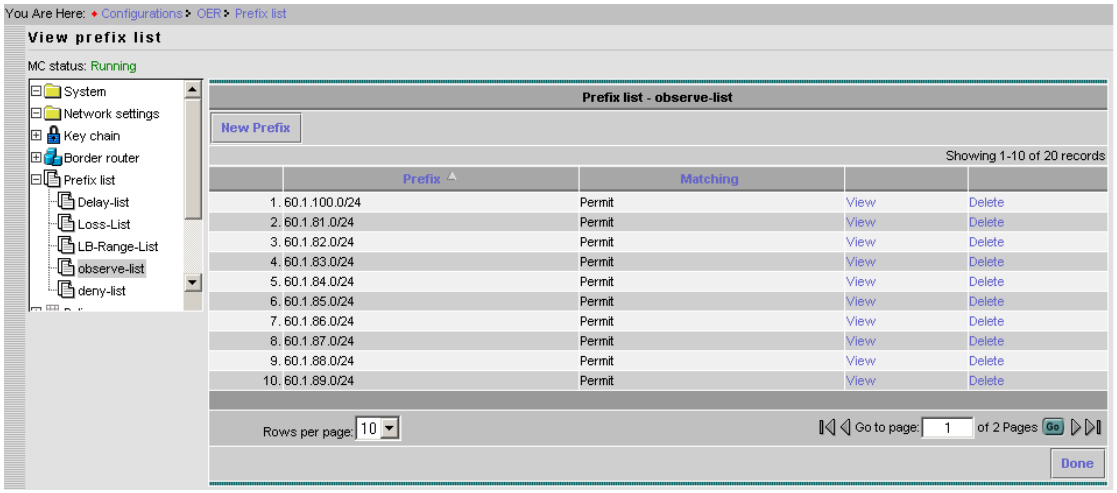
Step 2 To cancel this operation, click **Cancel**.

Step 3 To save settings, click **Save**

User-defined Prefix List

Select a user-defined prefix list.

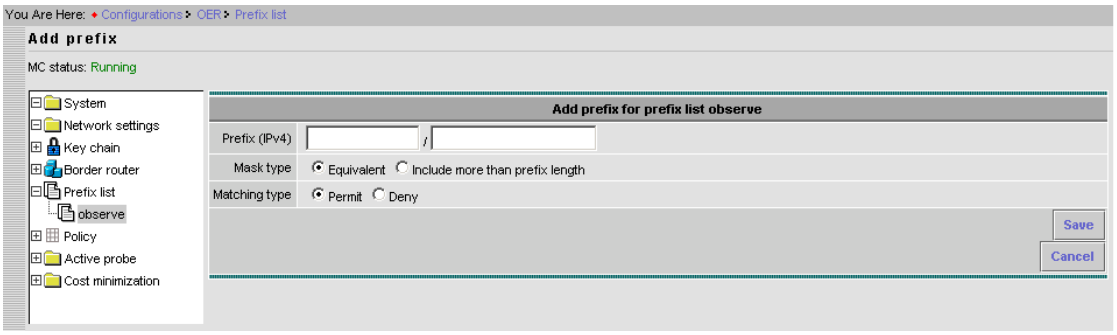
Figure 2-26 Configurations > Prefix List > User-defined



Add New Prefix to a User-defined Prefix List

From the selected User-defined Prefix List page, **New prefix**.

Figure 2-27 Configurations > Prefix List > User-defined Prefix List > Add Prefix



Step 1 Enter a value for the new **Prefix**.

A prefix is comprised of a network address and a mask length.

Only **Ipv4** prefix is supported.

Step 2 Select **Mask type**.

There are two types of mask:

– Equivalent.

– Include more than prefix length (also referred as non-equivalent).

If the mask type is non-equivalent, then all more specific prefixes that match the prefix are controlled as one prefix. For example: 10.1.0.0/16+ is configured, where + means non-equivalent. If there is a prefix 10.1.1.0/24 then it is controlled in the same way as 10.1.0.0/16 is controlled.

10.1.1.0/24 is called a shadow prefix of 10.1.0.0/16+.

The Cisco OER Master Controller Engine does not support configuring shadow prefixes. In other words, if 10.1.0.0/16+ is configured, then 10.1.1.0/24 cannot be configured because it is already part of 10.1.0.0/16+.

If 10.1.1.0/24 is configured first, then 10.1.0.0/16+ is not allowed. If a learned prefix creates the shadow for a user-configured non-equivalent prefix, then the learned prefix is deleted.

Step 3 Select **Matching type**.

There are two matching types:

– Permit

– Deny

If **Deny** is set, then this prefix is not controlled or monitored by the Cisco OER Master Controller Engine. It also prevents automatic learning of the prefix.

Note A prefix is not denied, controlled, or monitored unless the prefix-list in which the prefix is added is assigned a policy.

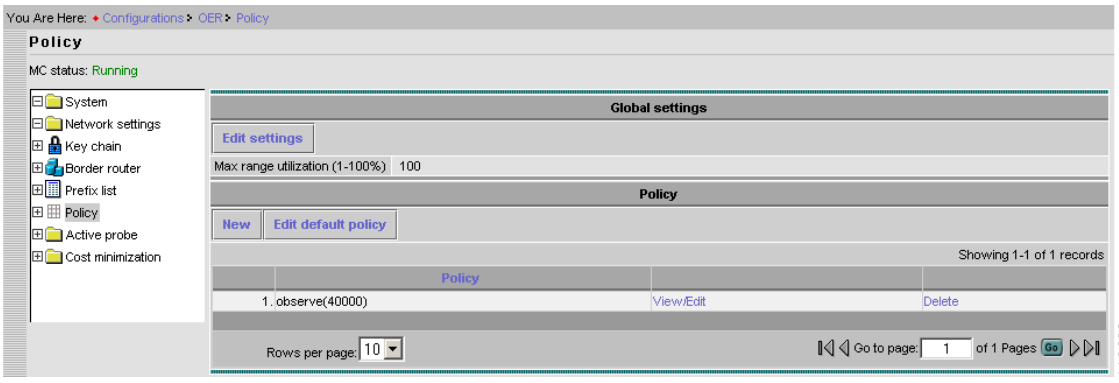
Step 4 To cancel this operation, click **Cancel**.

Step 5 To save settings, click **Save**

Policy

From the Content list under Configurations, select **Policy**.

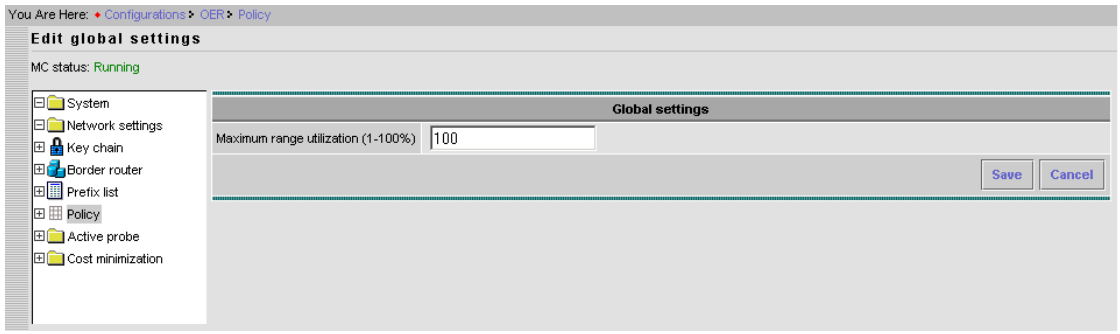
Figure 2-28 Configurations > Policy



Global Settings

From the Policy page, in the Global settings pane, click **Edit settings**.

Figure 2-29 Configurations > Policy > Edit Settings



Step 1 Enter a value for **Maximum range utilization**.

This defines the global policy of link utilization. If the difference between any two links is greater than value, then the Cisco OER Master Controller Engine takes an action to reduce the difference.

System default value is 20%.

Step 2 To cancel this operation, click **Cancel**.

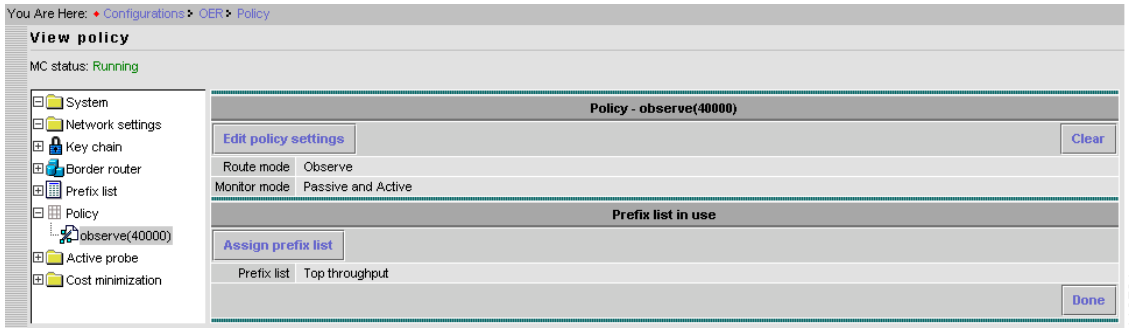
Step 3 To save settings, click **Save**

Default Policy Settings

There is a default policy that applies to all learned prefixes. You can configure a custom policy for finer control.

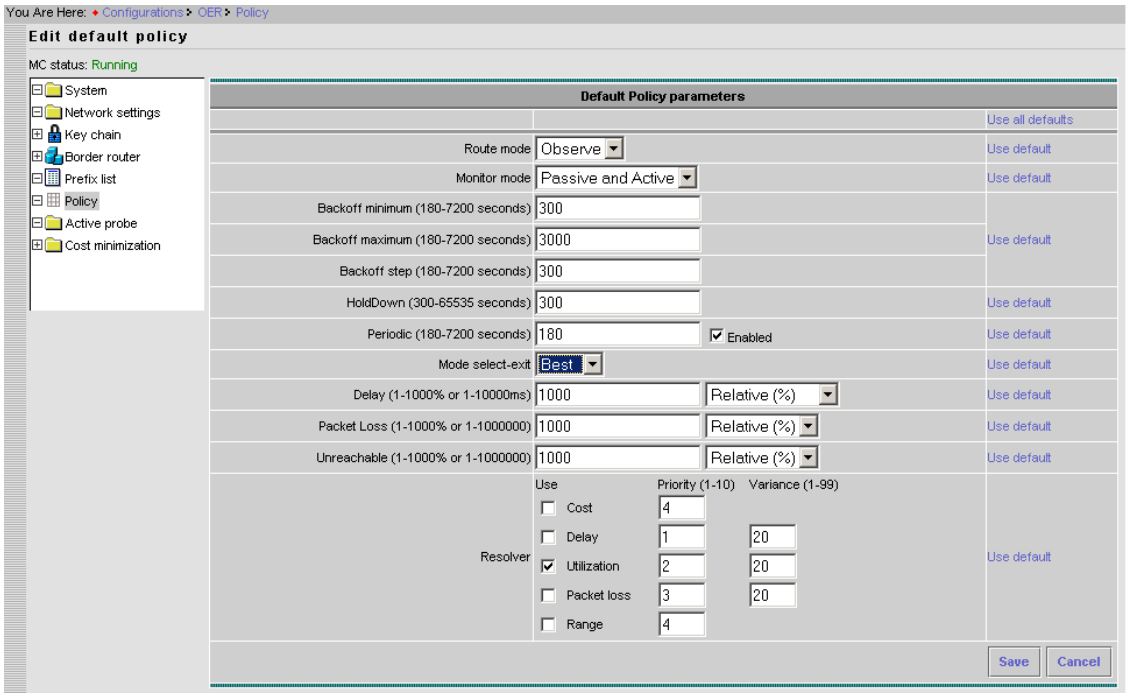
From the Content under Policy, select the default policy.

Figure 2-30 Configurations > Policy > Default



From the Default Policy page, click **Edit policy settings**.

Figure 2-31 Configurations > Policy > Default > Edit



The window shown in Figure 2-31 allows you to edit the default policy as well as add, delete, or edit a custom user-defined policy.

A user-defined policy can be applied to any one Prefix list including learned prefix list (top-throughput-list or top-delay-list). It cannot be applied to more than one prefix list.

A default policy cannot be manually applied to any prefix list. If two different policies are applied to the same prefix list, then the policy with the lower sequence number takes the precedence.

A default policy is applied to top delay and top throughput list automatically. This cannot be changed. However, you can apply a user-defined policy to the top delay and top throughput lists. Since the sequence number of a user-defined policy is always less than the default policy (seq 0x7fffffff), a user-defined policy overrides the default policy.

A user-defined policy can inherit one or more policy parameters from the Default policy. If a parameter is inherited from the Default policy, then any changes to the values of the parameters for the Default policy are reflected in the user-defined policy. Inheritance is useful for parameters that apply globally.

For example, **Holddown time** is most likely to apply to all the prefixes subsequently inherited from the Default policy.

To inherit a parameter from the Default policy, check the box to the right of each parameter.

All the fields for the Default policy have system default values when the Cisco OER Master Controller Engine is run for the first time.

A Policy contains following fields:

Route mode	Two options: • **Control** – prefix is moved to new Exit and traffic for the prefix flows through the new Exit. • **Observe** – prefixes to which this policy applies are only monitored. The Cisco OER Master Controller Engine finds a better Exit for out-of-policy prefixes but it does not modify the route for the prefix, rather it logs the new Exit as a *suggested* route. Suggested routes can be viewed in **Report** section under **Route Change** category. System default value is **Observe**.
Monitor mode	Three options: • **Passive** – netflow data is analyzed and the data of interest is gleaned to calculate such measurements as passive latency. • **Active** – SAA probes are created with learned prefixes as destination address to measure latency. It is not restricted only to learned prefixes. It applies to user-defined prefixes as well. • **Passive and Active** – both passive and active measurements are conducted. This selection is required for **Observe** mode. System default value is **Passive and Active**.
Backoff	Backoff consists of three parameters: • **Backoff minimum** • **Backoff maximum** • **Backoff step** These values are used for the backoff timer. The Backoff timer is started when no In-policy exit is found for a prefix. All the values are in seconds. **Backoff minimum** should be at least equal to the **Holddown** value. System default values are: minimum (**300**), maximum (**3000**), and step (**300**). The backoff_timer is used to schedule transitions from the OOP state. The backoff_count is a counter for the number of times the OOP has been entered without a policy decision being made. The delay is calculated as: **backoff_timer = backoff_min + backoff_count * backoff_step**
Holddown	When a prefix is moved to a new Exit, it is kept on that Exit for at least the **Holddown** time. **Holddown** is specified in seconds. System default value is **300**.

Periodic	This is a timer value. This timer defines how often the Cisco OER Master Controller Engine should look for a better Exit than the current Exit when the prefix is In-policy. If disabled, the Cisco OER Master Controller Engine does not look for a better Exit for In-policy prefixes. System default is **Disabled**.
Mode select-exit	Choice of **Best** or **Good** Mode select-exit. In passive monitor mode, prefixes are moved to passively probe the exit. If the mode select-exit is **Good**, passive probing is stopped as soon as an exit is found which is in-policy. If the mode select-exit is **Best**, all exits are passively probed before deciding the best-exit. The mode select-exit is also used for another purpose. If mode select-exit is **Good** and if all the exits are *Out of policy*, the prefix in uncontrolled. If mode select-exit is **Best** and if all the exits are *Out of policy*, then best exit among all the exits is selected and prefix is controlled by the Cisco OER Master Controller Engine. System default is **Best**.
Delay	Delay parameter is specified in two ways: • Threshold (delay in millisecond). • Percentage (1-1000%). In case of threshold, if the measured delay of the prefix is higher than the configured delay threshold then the prefix is *Out of policy* because of delay. In case of percentage, if the short term delay of the prefix is more than long term delay by the percentage value configured then the prefix is *Out of policy* because of the delay. **Short-term average delay** is the average delay over the last five minutes, or since the most recent exit change, whichever comes first. **Long-term average delay** is the average delay over the last 60 minutes, or since the most recent exit change, whichever comes first. System default is **50%**.
Packet Loss	Packet Loss configuration is the same as Delay except for the units. The loss threshold is specified in terms of packets per million. System default is **10%**.

Unreachable Policy

Unreachable configuration is also similar to Delay except for the units. The unreachable threshold is specified in terms of flows per million.

System default is **50%**.

Resolver

Resolver configuration for setting priorities for policy parameters.

To use a specific parameter for a policy decision, check the **Use** check box corresponding to that parameter.

Parameters are:

- **Cost**.

Note If **Cost** is enabled under resolver priority then make sure that **Cost** is configured and applied to the Exit (External Interface). Exits which do not have cost configure will not be a candidate when the resolver is making a decision based on cost.

- **Delay**.
- **Utilization**.
- **Packet Loss**.
- **Range** (Max Range Utilization).
- **Priority (**determines order in which each prefix state is tested).
  - Possible range of values for priority is 1-10.
  - The lowest value is the highest priority.
  - If a resolver is checked then its priority must be unique in value.
- **Variance**.

  The variance is configured in terms of percentage.

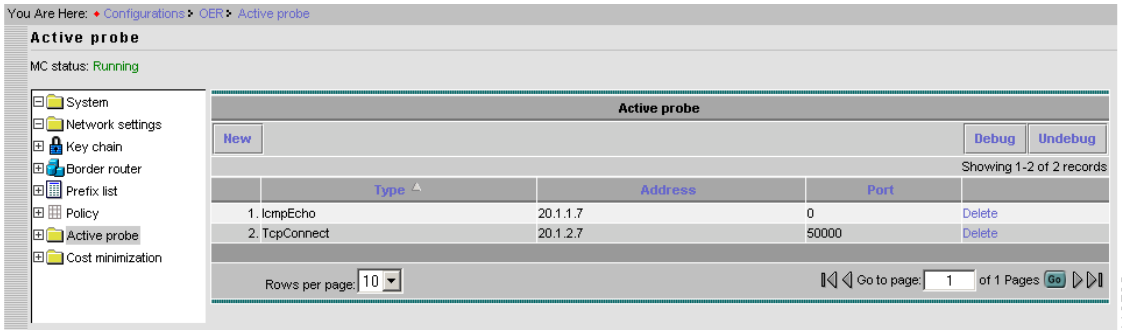
  For example, if the delay variance is 20%, and if the delay for a prefix in Exit A is 100 ms, and Exit B is 115, then the both Exits are considered equal in terms of delay because the difference in delay (15 ms) is less than 20% of the lowest delay (100 ms).

Note Variance is not used for **Cost** and **Range**.

Active Probe

For active measurements, targets are required for user-defined prefixes. This section describes how to configure active probe targets. SAA probes are used to perform active probing from each border router. That is, the border router IP address is the source address and the prefix is the destination address.

Figure 2-32 Configurations > Active Probe



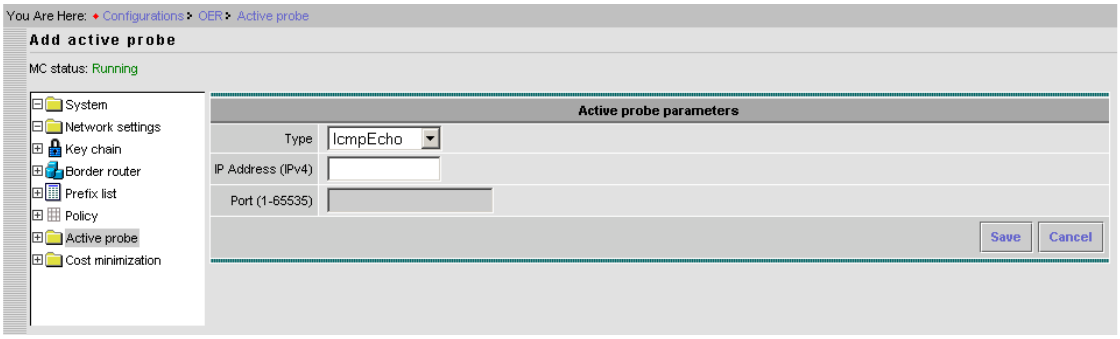
Each target is defined using following parameters:

- Type
- Target IP Address
- Port

Add Active Probe

From the Active Probe window, click New.

Figure 2-33 Configurations > Active Probe > New



Step 1 Select **Type**.

There are three types of probes:

- **IcmpEcho**
- **TcpConnect**
- **UdpEcho**

TcpConnect and **UdpEcho** probes require an SAA responder configured on the target node. SAA is the service assurance agent running on a Cisco device.

Step 2 Enter network **IP address**.

Only **Ipv4** is supported.

Step 3 Enter a value for the **Port**.

Port number to use for **TcpConnect** and **UdpEcho** probes.

Step 4 To cancel this operation, click **Cancel**.

Step 5 To save settings, click **Save**

Cost Minimization

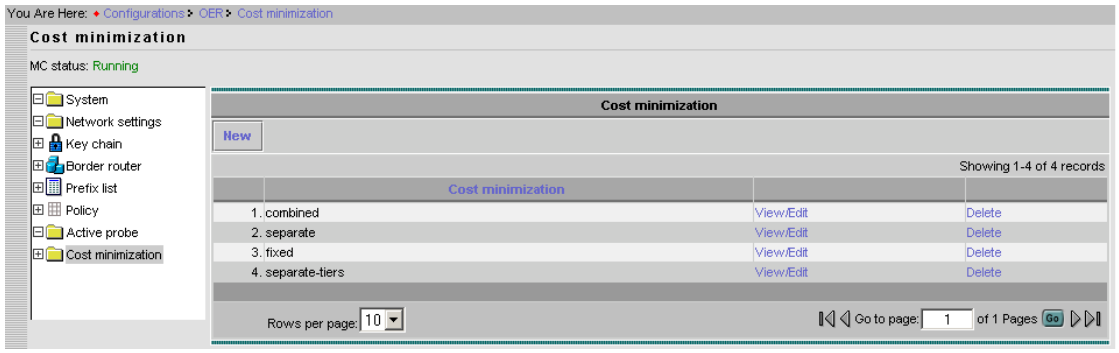
ISPs bill the customer for the use of their services using different methods. The cost minimization configuration supports fixed cost Cost Minimization and *tier based with bursting* Cost Minimization.

Cost Minimization types are the billing criteria that are established with each ISP.

The Cost minimization page provides a way for you to model the service level agreement with an ISP. If the Resolver Cost minimization is enabled, prefixes are moved based on the cost criteria for each ISP. That is, less costlier ISP will be preferred over a higher cost ISP.

More than one Cost Minimization type can be configured. The Cost Minimization type is then applied to an Exit by editing **Configurations > Border router > Interface > Edit settings** (see "Edit Border Router Interface" section on page 2-13).

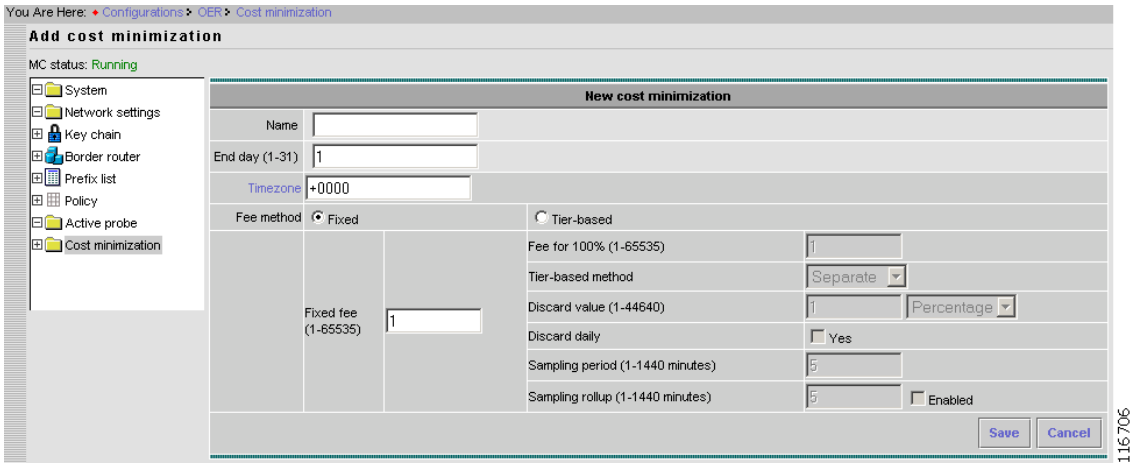
Figure 2-34 Configurations > Cost Minimization



New Cost Minimization Contract

From the Cost Minimization page, click **New**.

Figure 2-35 Configurations > Cost Minimization > Add Cost Minimization



Step 1 Enter a **Name**.

Step 2 Enter an **End day**.

The last day of the billing cycle.

Step 3 Enter a **Timezone**.

By default a billing cycle ends at 23:59:59 UTC on the **End day**. This value allows a billing cycle to expire before or after 23:59:59 UTC.

The format is **[+|-]HHmm**.

For example, if billing cycle expires four hours early, then **Timezone** should be set to +0400.

Step 4 Select **Fee method**.

Fixed

a. Enter a value for **Fixed fee**.

Monthly cost of Fixed cost link. This value is not used for any cost minimization. It is merely used for reporting.

Tier-based

a. Enter **Fee for 100%**

Fee for the top tier (100%).

b. Select **Tier-based method**.

There are three methods within the tier-based-with-bursting structure. These methods define the manner in which bursty usage is discarded.

Separate: Egress and Ingress utilization samples are separately stacked to discard the bursty usage from each stack. Each stack is sorted in descending order, highest usage sample being on the top. Top ***n*** samples are discarded, where ***n*** is the discard value in terms of absolute or percentage. The remaining highest utilization on each stack is called *sustained utilization*. For **Separate**, the larger of the two sustained utilization is the *monthly sustained utilization* billed by the ISP.

Combined: Egress and Ingress utilization samples are put on one stack.

Summed: Egress and Ingress utilization values are added before putting them onto a single stack.

c. Enter **Discard value**.

The number of samples discarded from the stack of link utilization samples to remove the bursty link usage. It is specified in absolute terms or a percentage. The value applies to each stack. If **Sampling rollup** is enabled, the discard value applies to the stack of rollup utilization.

d. Choose to Enable **Discard daily**, or not.

If daily discard is enabled, then process of discarding is done daily and *sustained utilization* is calculated on each day. At the end of the billing cycle *monthly sustained utilization* is calculated by averaging *daily sustained utilization*.

e. Enter a value for **Sampling period**.

Rate at which link utilization is sampled.

Default is every **5** minutes.

f. Enter a value for **Sampling rollup**.

To reduce the number of samples, samples are aggregated (rolled up) by hours or minutes. If **Sampling rollup** is enabled, all the samples collected during the rollup period are averaged to calculate the rollup utilization.

Rollup utilization is used for all the calculations.

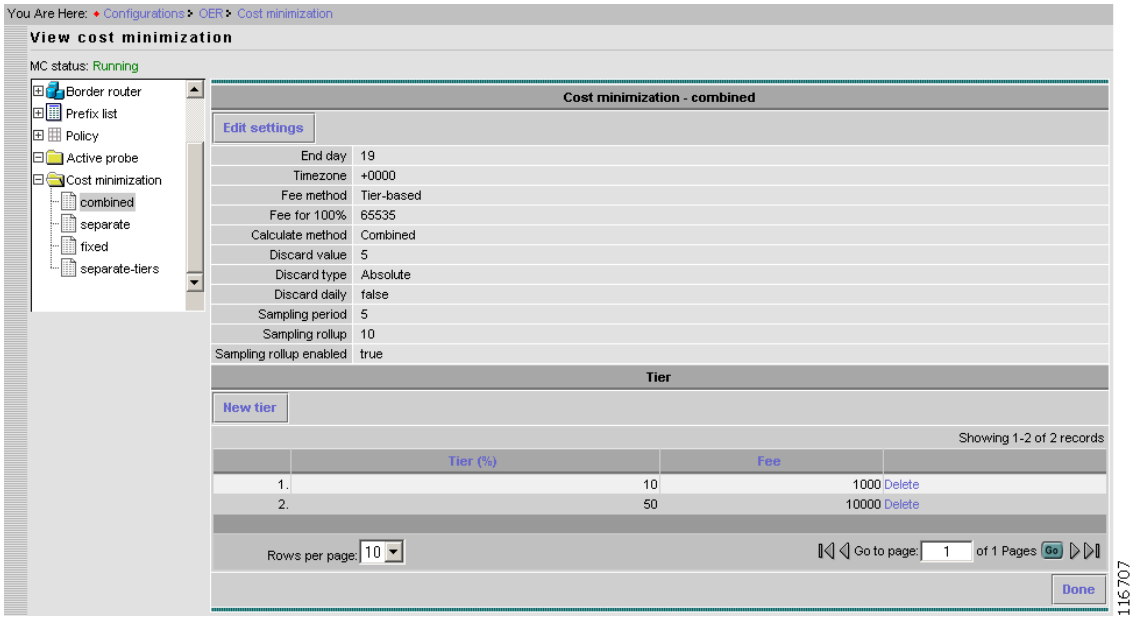
Step 5 To cancel this operation, click **Cancel**.

Step 6 To save settings, click **Save**

View Cost Minimization

From the Content list under Cost Minimization, click on the desired Cost Minimization type.

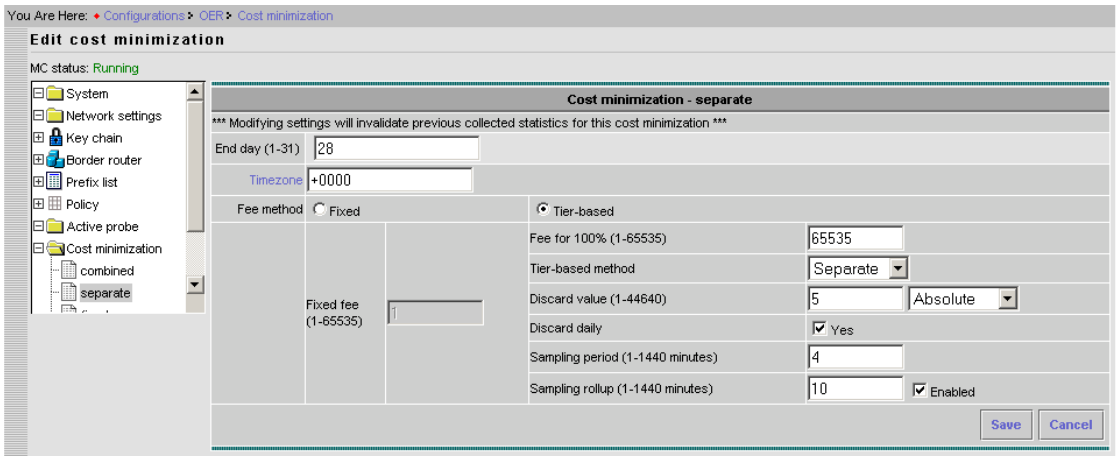
Figure 2-36 Configurations > Cost Minimization > View Cost Minimization



Edit Cost Minimization

From the View Cost Minimization page, click **Edit Settings**.

Figure 2-37 Configurations > Cost Minimization > Edit Cost Minimization



Warning **Modifying settings will invalidate previous collected statistics for this cost minimization**

Step 1 Enter a value for **End day**.

The end day of the billing cycle.

Step 2 Enter a **Timezone**.

By default a billing cycle ends at 23:59:59 UTC on the **End day**. This value allows a billing cycle to expire before or after 23:59:59 UTC.

The format is **[+|-]HHmm**.

For example, if billing cycle expires four hours early, then **Timezone** should be set to +0400.

Step 3 Select **Fee method**.

Fixed

a. Enter a value for **Fixed fee**.

Monthly cost of Fixed cost link. This value is not used for any cost minimization. It is merely used for reporting.

Tier-based

a. Enter **Fee for 100%**

Fee for the top tier (100%).

b. Select **Tier-based method**.

There are three methods within the tier-based-with-bursting structure. These methods define the manner in which bursty usage is discarded.

Separate: Egress and Ingress utilization samples are separately stacked to discard the bursty usage from each stack. Each stack is sorted in descending order, highest usage sample being on the top. Top ***n*** samples are discarded, where ***n*** is the discard value in terms of absolute or percentage. The remaining highest utilization on each stack is called *sustained utilization*. For **Separate**, the larger of the two sustained utilization is the *monthly sustained utilization* billed by the ISP.

Combined: Egress and Ingress utilization samples are put on one stack.

Summed: Egress and Ingress utilization values are added before putting them onto a single stack.

c. Enter **Discard value**.

The number of samples discarded from the stack of link utilization samples to remove the bursty link usage. It is specified in absolute terms or a percentage. The value applies to each stack. If **Sampling rollup** is enabled, the discard value applies to the stack of rollup utilization.

d. Choose to Enable **Discard daily**, or not.

If daily discard is enabled, then process of discarding is done daily and *sustained utilization* is calculated on each day. At the end of the billing cycle *monthly sustained utilization* is calculated by averaging *daily sustained utilization*.

e. Enter a value for **Sampling period**.

Rate at which link utilization is sampled.

Default is every **5** minutes.

f. Enter a value for **Sampling rollup**.

To reduce the number of samples, samples are aggregated—rolled up—by hours or minutes. If **Sampling rollup** is enabled, all the samples collected during the rollup period are averaged to calculate the rollup utilization.

Rollup utilization is used for all the calculations.

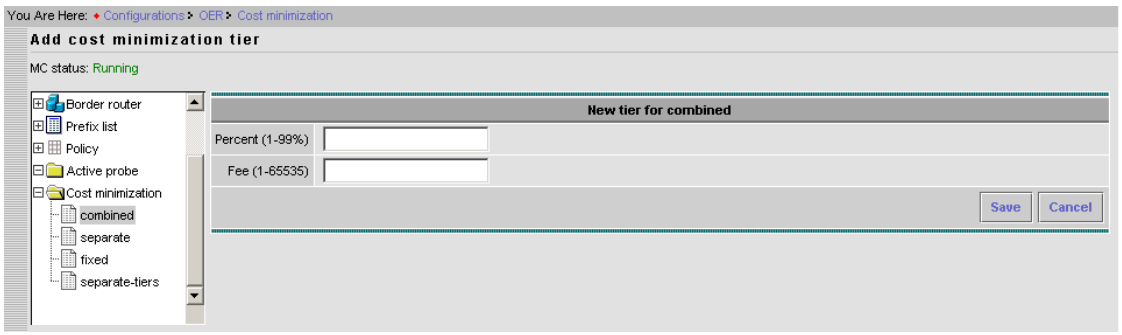
Step 4 To cancel this operation, click **Cancel**.

Step 5 To save settings, click **Save**

New Tier

From the View Cost Minimization page, click **New tier**.

Figure 2-38 Configurations > Cost Minimization > Add Cost Minimization Tier



Step 1 Enter a value for **Percentage**.

Step 2 Enter a value for **Fee**.

Step 3 To cancel this operation, click **Cancel**.

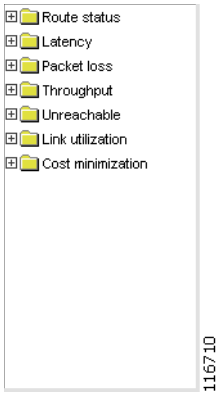
Step 4 To save settings, click **Save**

Reports

Using the Reports main function, you can see the last ***n*** minutes/hours/days worth of data either in summarized form or as is. The Contents list shows the various subfunctions available under Reports.

- Router status
- Latency
- Packet loss
- Throughput
- Unreachable
- Link utilization
- Cost minimization

Figure 2-39 Reports Contents List



Router Status

Under Router Status, you can find the following type reports:

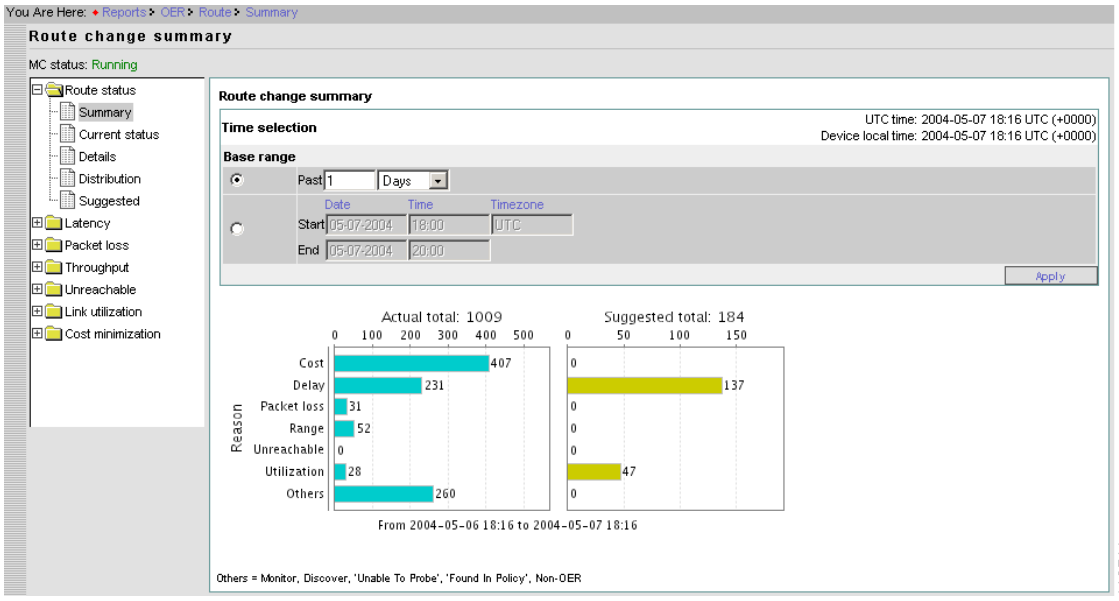
- Summary
- Current status
- Details
- Distribution
- Suggested

Summary

Summary router status shows overall summary with respect to Route Change.

From the Contents list, open the menu under **Router status**, then click **Summary**.

Figure 2-40 Reports > Router Status > Summary



Instead of selecting the last ***n*** minutes/hours/days, a time range can be selected by specifying start time and end time.

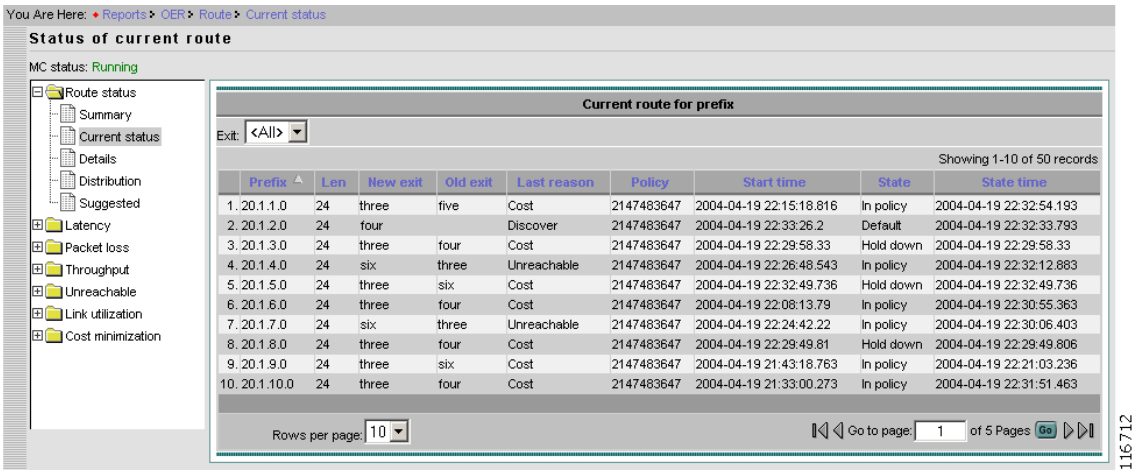
The format is: **yyyy-mm-dd**.

The **Timezone** is specified only with start time and the same is used for end time. For reference, the current UTC time and device local time are displayed on upper right corner of the page. If **Timezone** is not specified, the local time zone is used.

Current Status

From the Content List, select **Current status**. This reports contains the current status of each prefix.

Figure 2-41 Reports > Router Status > Current Status

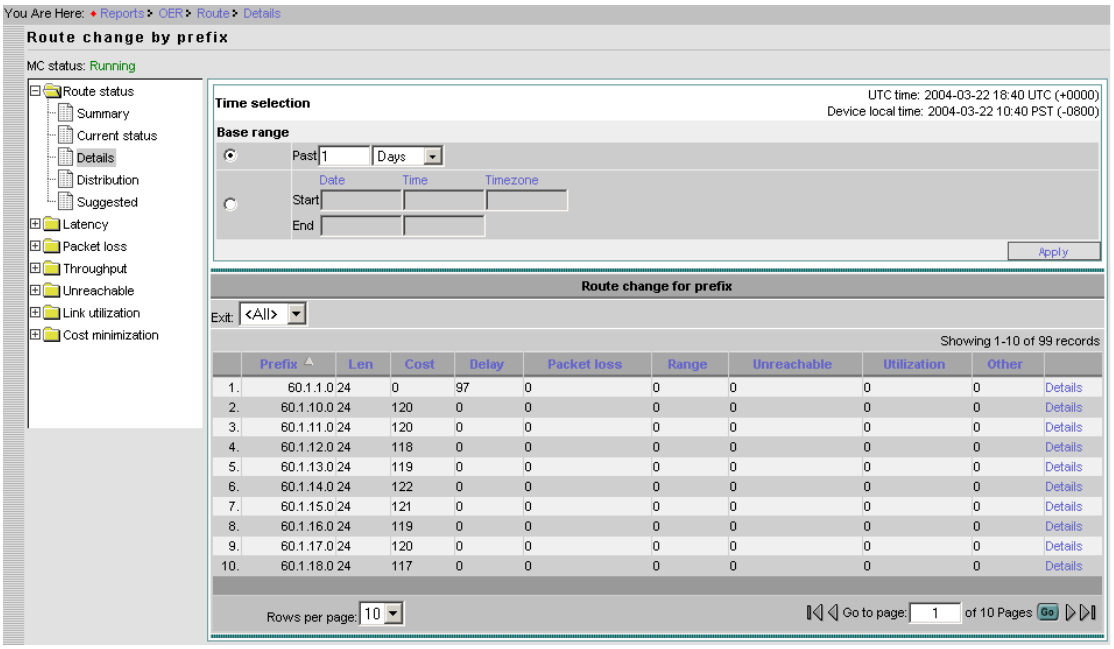


Prefix	Prefix.
Length	Prefix length.
New exit	Current Exit of the Prefix.
Old exit	Previous Exit.
Last reason	Last reason for changing to New Exit for the prefix.
Policy	Sequence number/Name of the current policy that applies to the prefix.
Start time	Time at which the New Exit was selected for the prefix.
State	Current state of the prefix. There are five states for a prefix: HOLDDOWN, INPOLICY, OOPOLICY, CHOSE_EXIT, DEFAULT.
State time	Time at which the prefix was assigned the State.

Details

From the Content List, select **Details**. This reports contains the Router Status Details of each prefix.

Figure 2-42 Reports > Router Status > Details > Route Change by Prefix

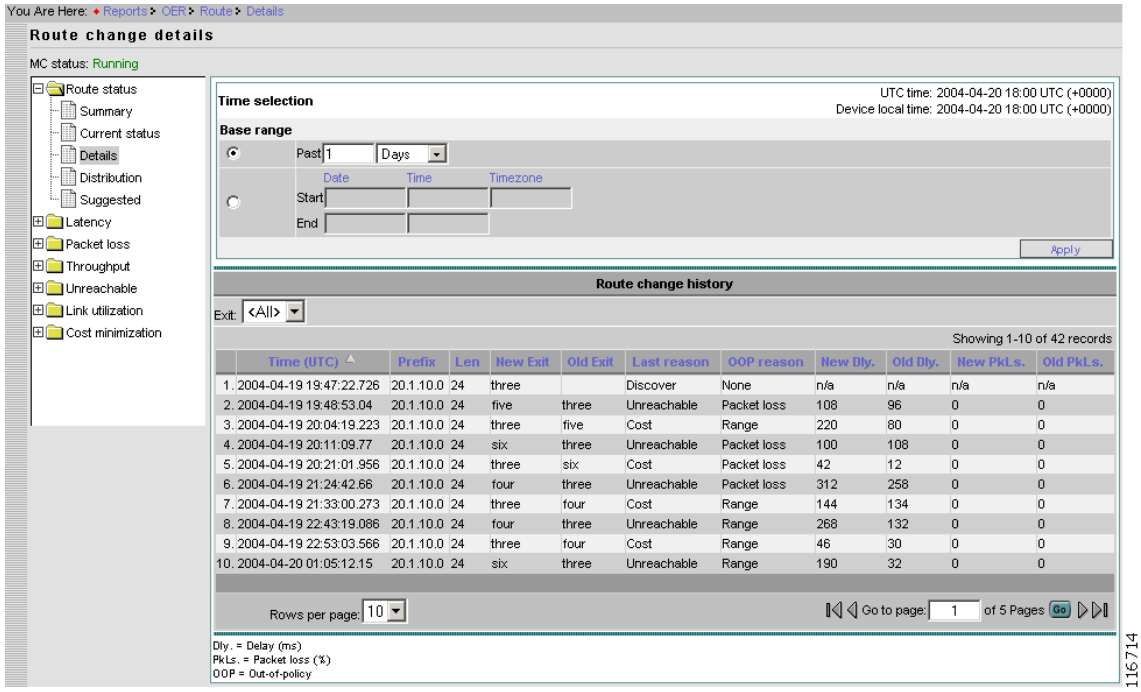


Prefix	Prefix
Length	Prefix Length
Cost	Route change because cost on old link is higher than on the new Exit.
Delay	Route is changed because delay is lower on new Exit than on the old Exit.
Packet loss	Route is changed because packet loss is lower on new Exit than on the old Exit.
Range	Route is changed because difference between link utilization on old Exit and at least one other Exit was higher than the maximum range unitization configured.
Unreachable	Route is changed because prefix was unreachable on old Exit.
Utilization	Route is changed because old Exit had link utilization higher the maximum threshold configured.
Other	Route is changed for other reasons.

Route Change Details

From the **Route change by prefix** page, Select the prefix of interest, then click **View details**.

Figure 2-43 Reports > Router Status > Details > Route Change Details



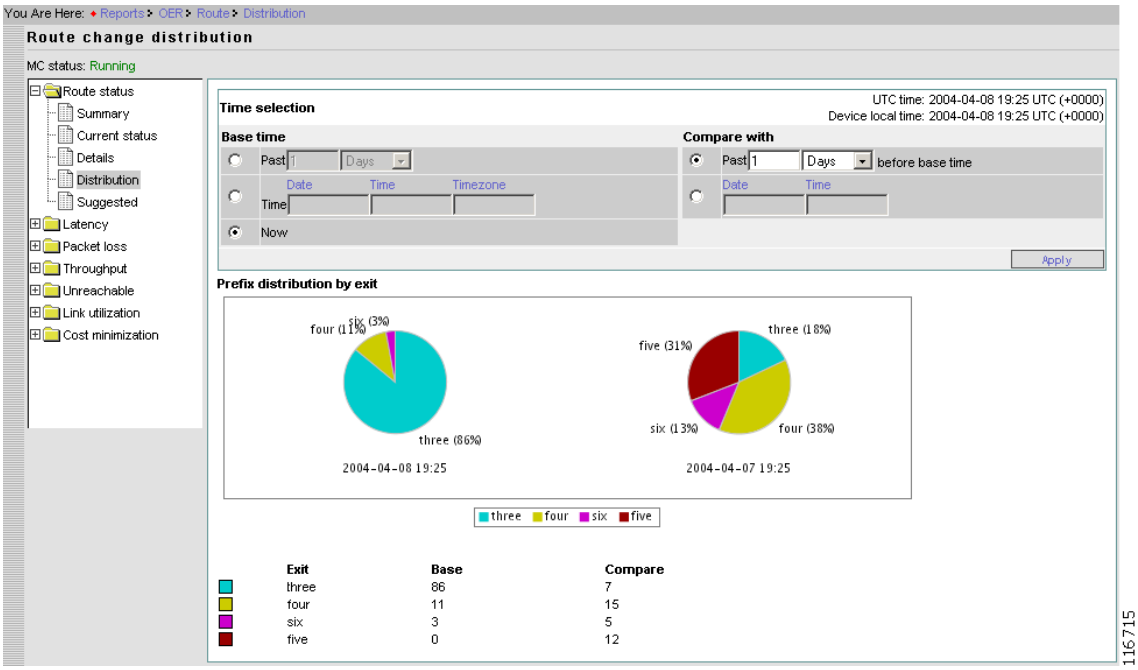
Time (UTC)	Time of report.
Prefix	Prefix.
Length	Prefix length.
New exit	Current Exit of the Prefix.
Old exit	Previous Exit.
Last reason	Last reason for changing to New Exit for the prefix.
OOP reason	OOP (Out-of-policy) reason is a trigger to find a new Exit. It can trigger due to delay, packet loss, unreachable, utilization, range, cost, or Timer Expired. Timer Expired reason is selected when a new Exit is selected because one of the timer (periodic, backoff) expired. It is not necessary that last reason is same as OOP Reason. For example, delay OOP may trigger the Cisco OER Master Controller Engine to find a new Exit. But it may decide, based on resolver priority, to move a prefix from the current Exit for reason other than delay.
New delay	Delay using the new Exit.

Old delay	Delay using the old Exit.
New packet loss	Packet loss using the new Exit.
Old packet loss	Packet loss using the old Exit.

Distribution

From the Content List, select **Distribution**. The Distribution pie chart shows the number of prefixes being forwarded on all the Exits at two different time. You can select any two different times.

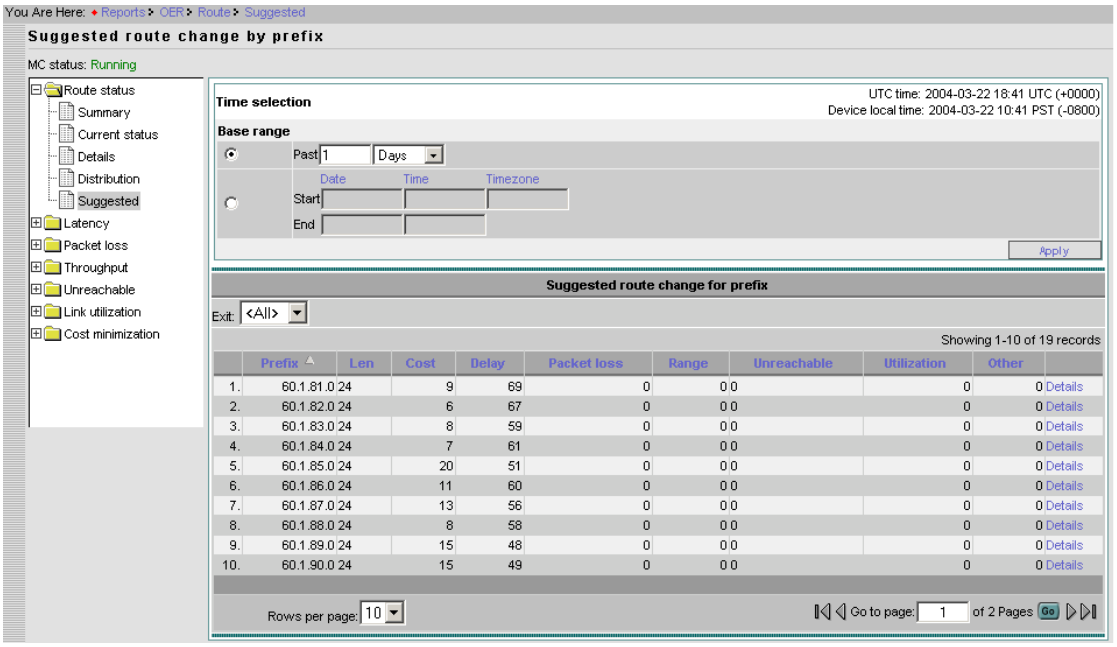
Figure 2-44 Reports > Router Status > Route Change Distribution



Suggested

From the Content List, select **Suggested**.

Figure 2-45 Reports > Router Status > Suggested Route Change by Prefix



This page shows the same information as the Detail page (Figure 2-42), but the route changes are not actual. All the data pertains to suggested route changes.

If a prefix is in observe mode (see "Default Policy Settings" section on page 2-21) then Route is not changed for the prefix, but it is just logged for reporting.

Latency

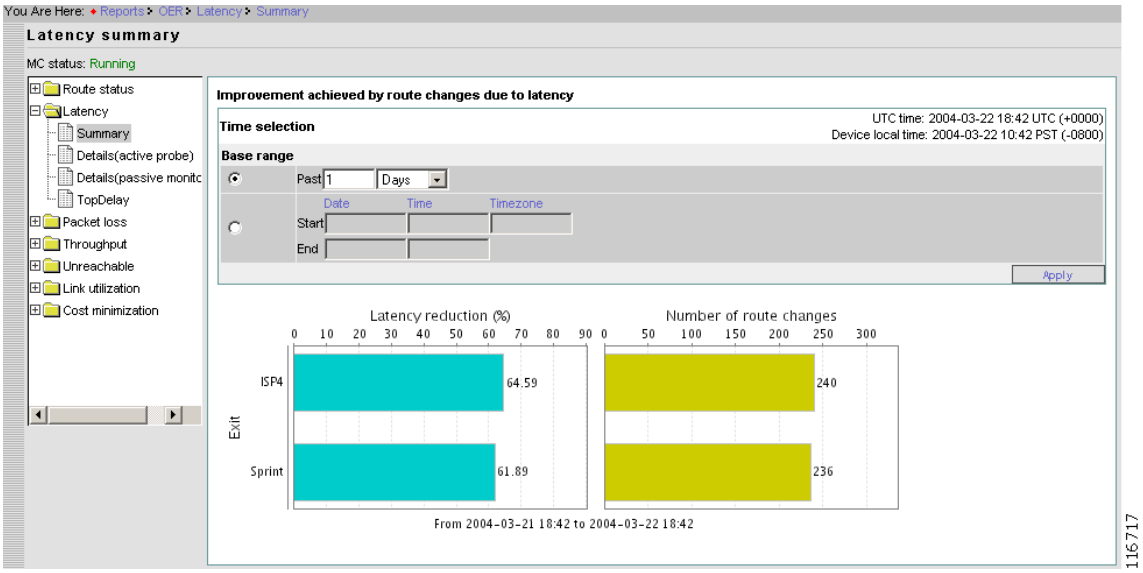
Under Latency, you can find the following type reports:

- Summary
- Details (active probe)
- Details (passive monitoring)
- Top Delay

Summary

From the Contents list, open the menu under **Latency**, then click **Summary**.

Figure 2-46 Reports > Latency > Summary

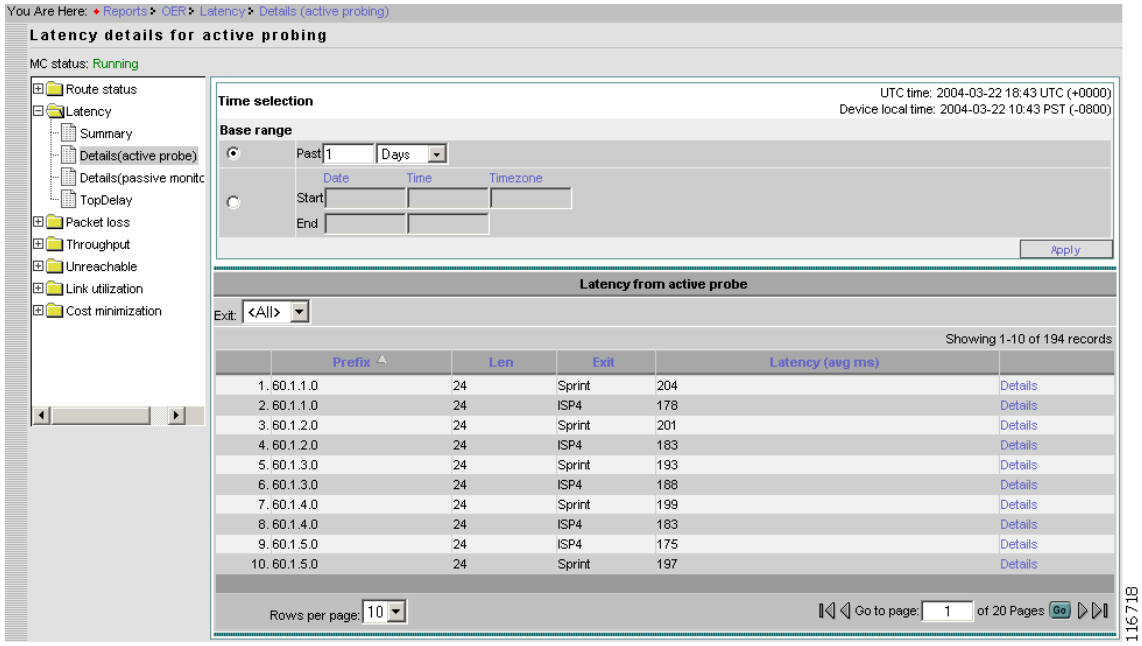


The Latency Summary report displays the graph of average delay reduction per exit for selected duration. Delay reduction is calculated as (delay on old Exit – delay on new Exit) / (delay on old Exit). There is another graph (bar chart) displaying number of prefixes that were moved to the Exit due to delay reason for each Exit.

Details - Active Probe

From the Contents list, open the menu under **Latency**, then click **Details (active probe)**. Figure 2-47 displays average active delay per Prefix per Exit for selected duration.

Figure 2-47 Reports > Latency > Details for Active Probe

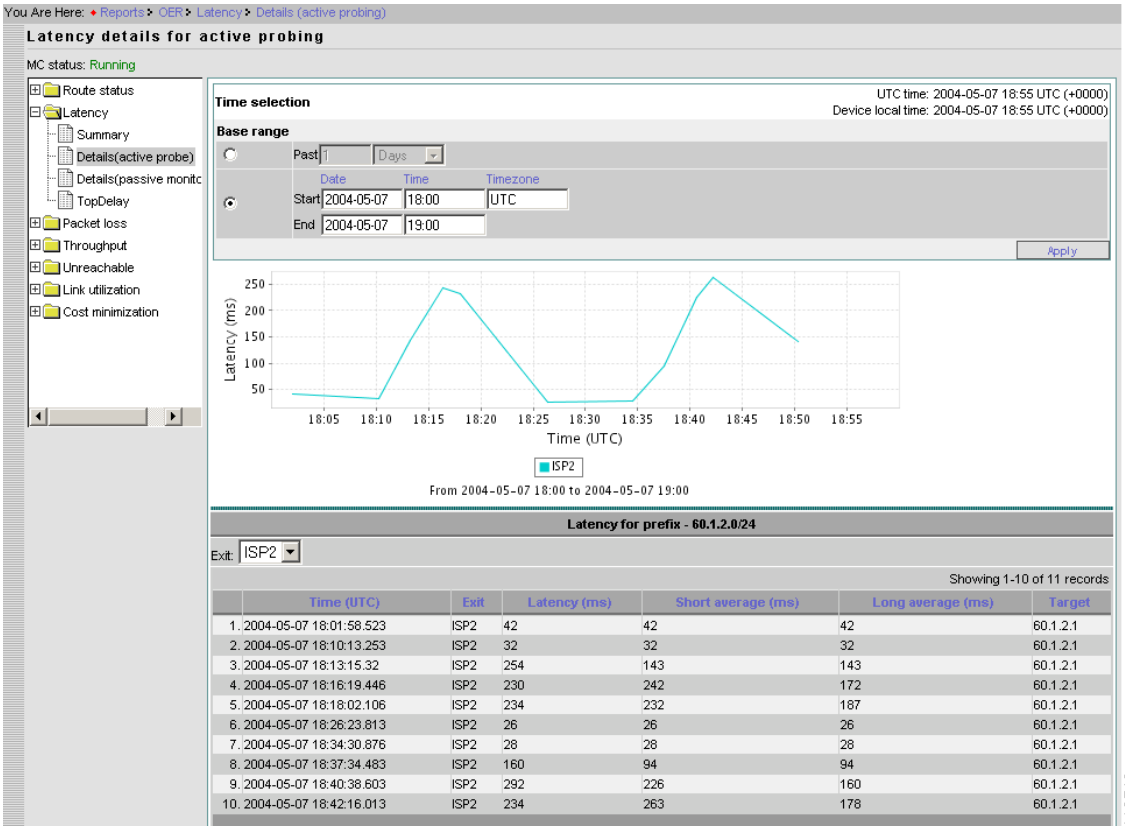


Prefix	Prefix.
Length	Prefix length.
Exit	Current Exit of the Prefix.
Latency	Latency time in milliseconds.

Active Probe Details for Selected Prefix

From the **Latency details for active probing** page, select the probe of interest, then click **Details**.

Figure 2-48 Reports > Latency > Details (Active Probe) > Probe Details



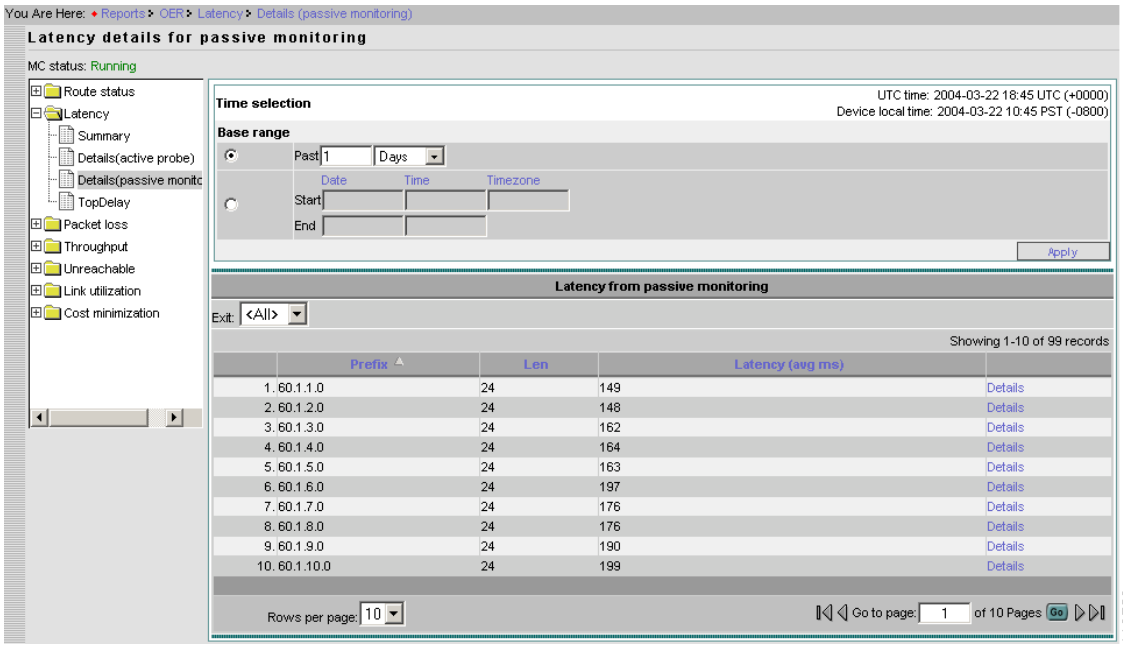
Time (UTC)	Time of report.
Exit	Exit for which the data is displayed. Or, you can select **<All>**.
Latency	Latency time in milliseconds.
Short average	Short term average delay for Prefix.
Long average	Long term average delay for Prefix.
Target	IP address of the host that is actively being probed.

Multiple lines (one for each Exit) can be displayed. This is because active probing is performed simultaneously on all Exits.

Details - Passive Monitoring

From the Contents list, open the menu under **Latency**, then click **Details (passive monitoring)**.

Figure 2-49 Reports > Latency > Details (Passive Monitor)



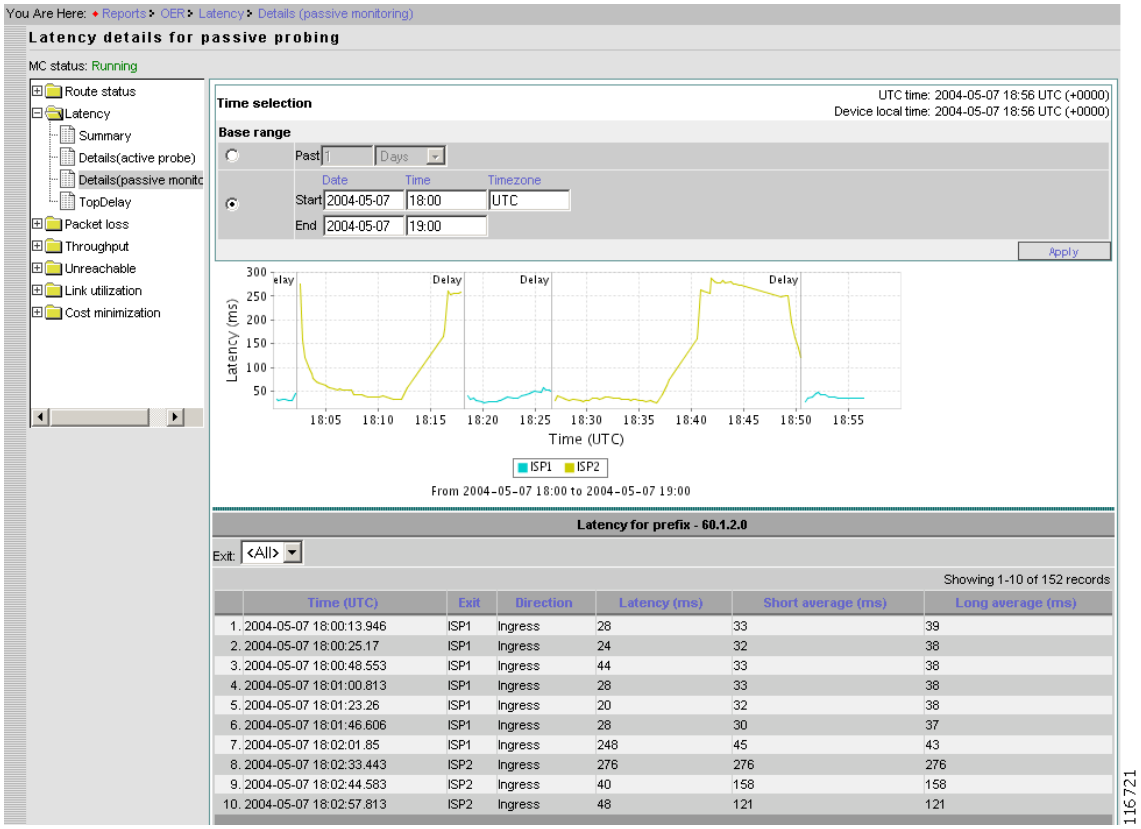
Passive Monitoring Details for Selected Prefix

From the **Latency details for passive monitoring** page, select the probe of interest, then click **Details**.

The time series chart displays the running short term average delay for a Prefix. If the Prefix was moved to a different Exit in selected duration then the color of the line is changed to indicate the change in Exit.

Apart from time series chart for delay, there are vertical bars that corresponds to route change. Each bar has a text associated with it which describes the reason why a Prefix was moved to a different Exit.

Figure 2-50 Reports > Latency > Details (Passive Monitoring) > Details

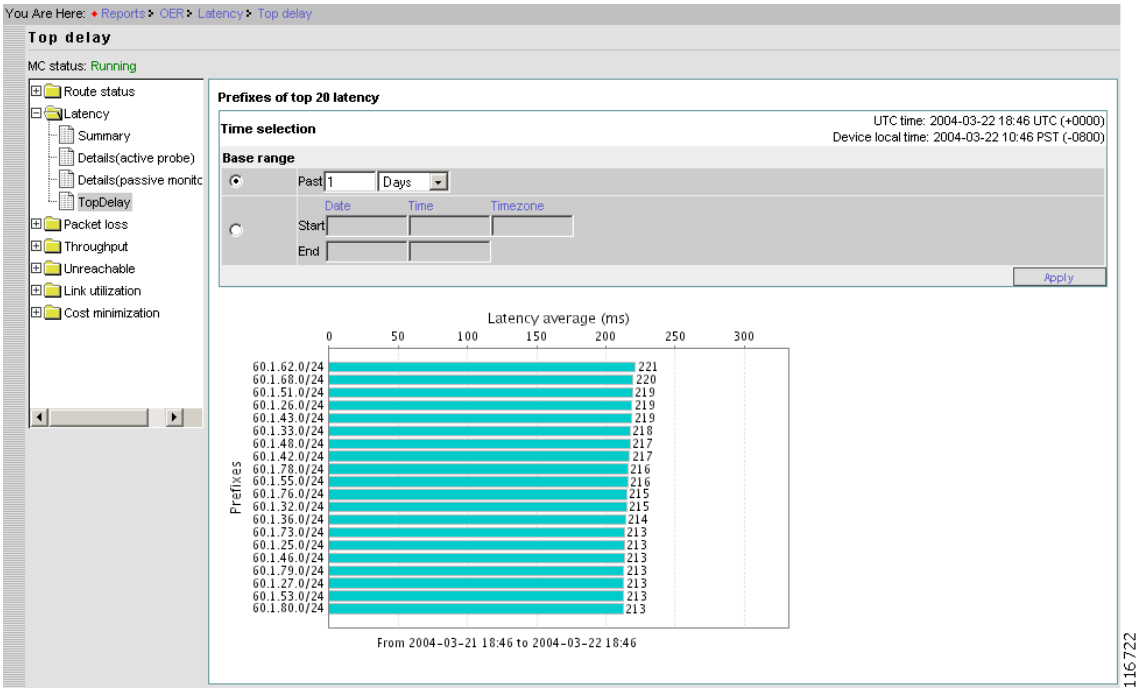


Time (UTC)	Time of report.
Exit	Exit for which the data is displayed. Or, you can select **<All>**.
Direction	Direction of traffic.
Latency	Latency time in milliseconds.
Short average	Short term average delay for Prefix.
Long average	Long term average delay for Prefix.

Top Delay

From the Contents list, open the menu under **Latency**, then click **TopDelay**.

Figure 2-51 Reports > Latency > Top Delay



Packet Loss

Under Packet Loss, you can find the following type reports:

- Summary
- Details (active probe)
- Details (passive monitoring)

Summary

From the Contents list, open the menu under **Packet loss**, then click **Summary**.

Figure 2-52 Reports > Packet Loss > Summary

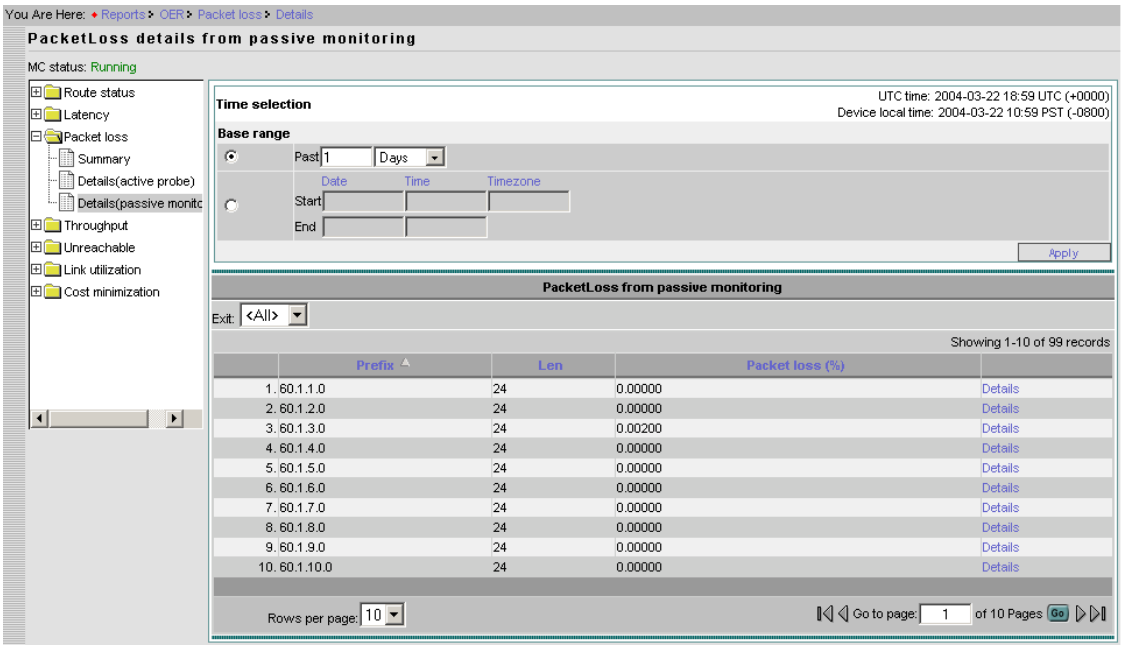
Details - Active Probe

Note This particular feature is not supported in this release.

Details - Passive Monitoring

From the Contents list, open the menu under **Packet loss**, then click **Details (passive monitoring)**.

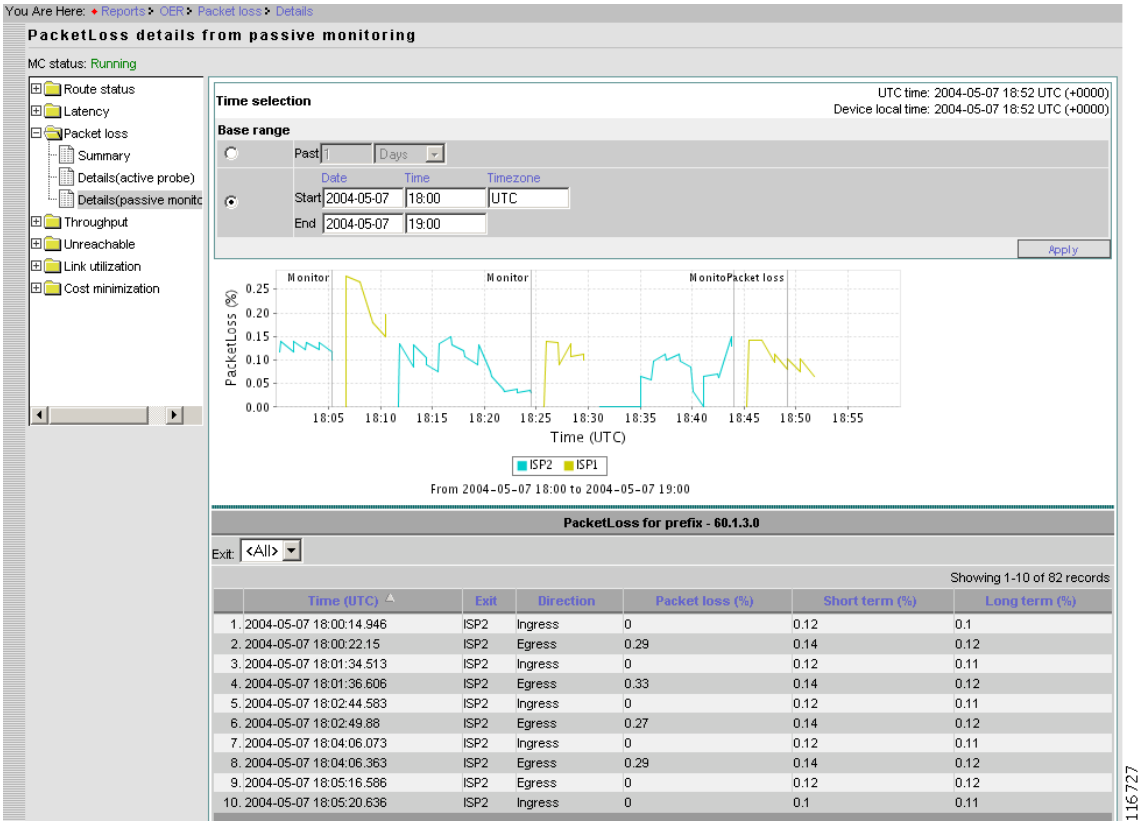
Figure 2-53 Reports > Packet Loss > Details From Passive Monitoring



Passive Monitoring Details for Selected Prefix

From the **PacketLoss details from passive monitoring** page, select the probe of interest, then click **Details**.

Figure 2-54 Reports > Packet Loss > Details From Passive Monitoring > Prefix Details



Throughput

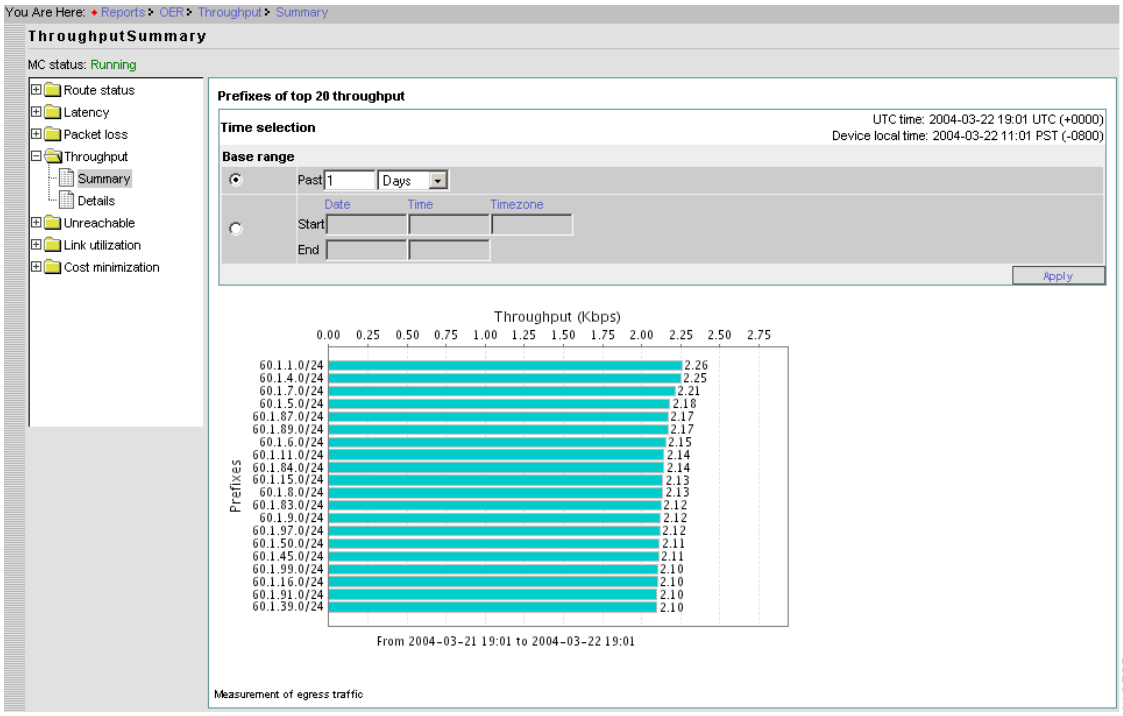
Under Throughput, you can find the following type reports:

- Summary
- Details

Summary

From the Contents list, open the menu under **Throughput**, then click **Summary**.

Figure 2-55 Reports > Throughput > Summary

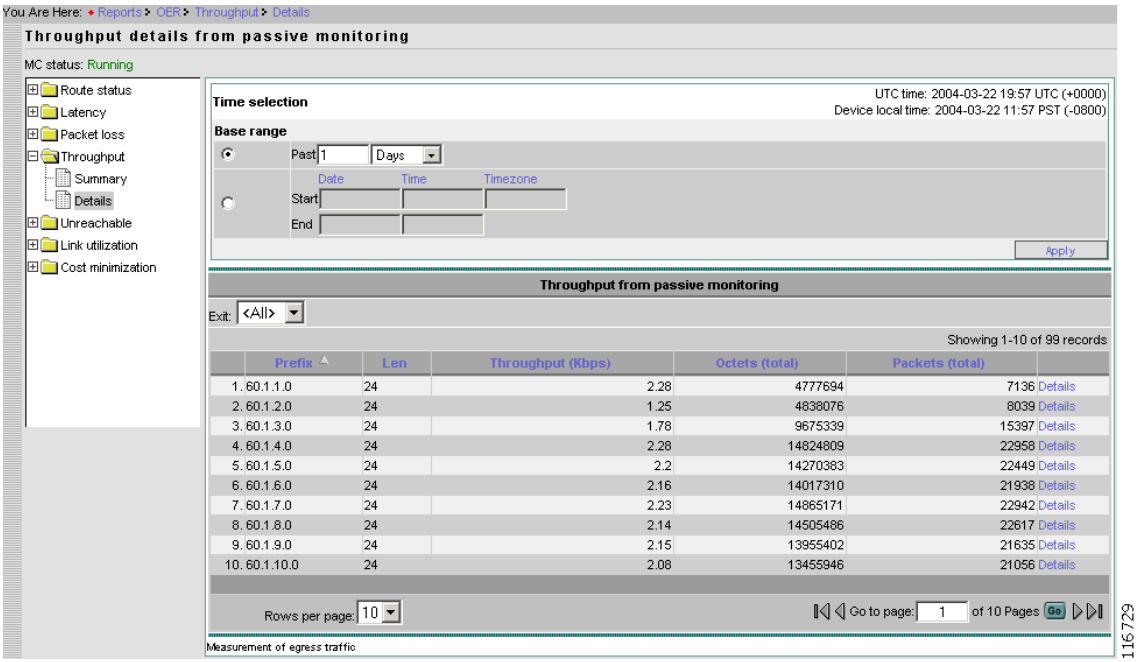


This report provides the top 20 prefixes by average throughput observed during the selected duration.

Details

From the Contents list, open the menu under **Throughput**, then click **Details**.

Figure 2-56 Reports > Throughput > Details

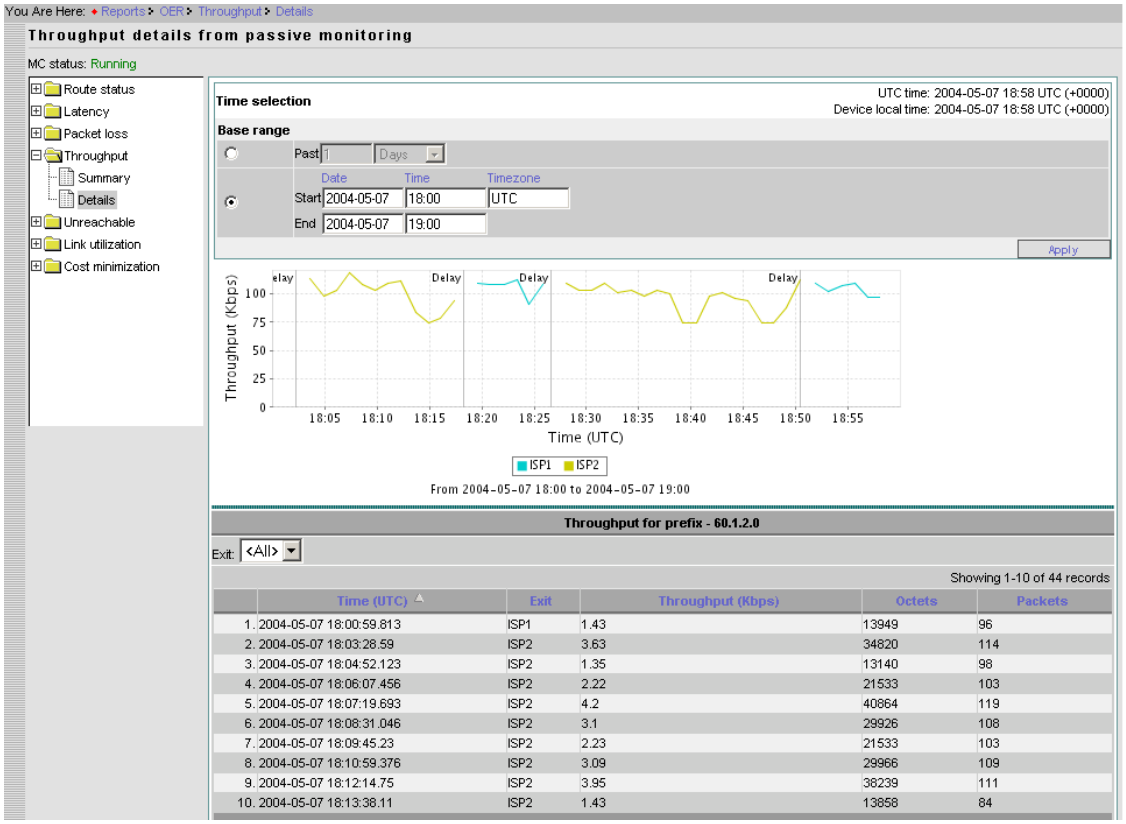


Prefix	Prefix.
Length	Prefix length.
Throughput	Throughput shown as rate of traffic.
Octets	Total egress octets.
Packets	Total number of packets.

Details for Selected Prefix

From the **Throughput details from passive monitoring** page, select the probe of interest, then click **Details**.

Figure 2-57 Reports > Throughput > Details From Passive Monitoring> Prefix Details



Unreachable

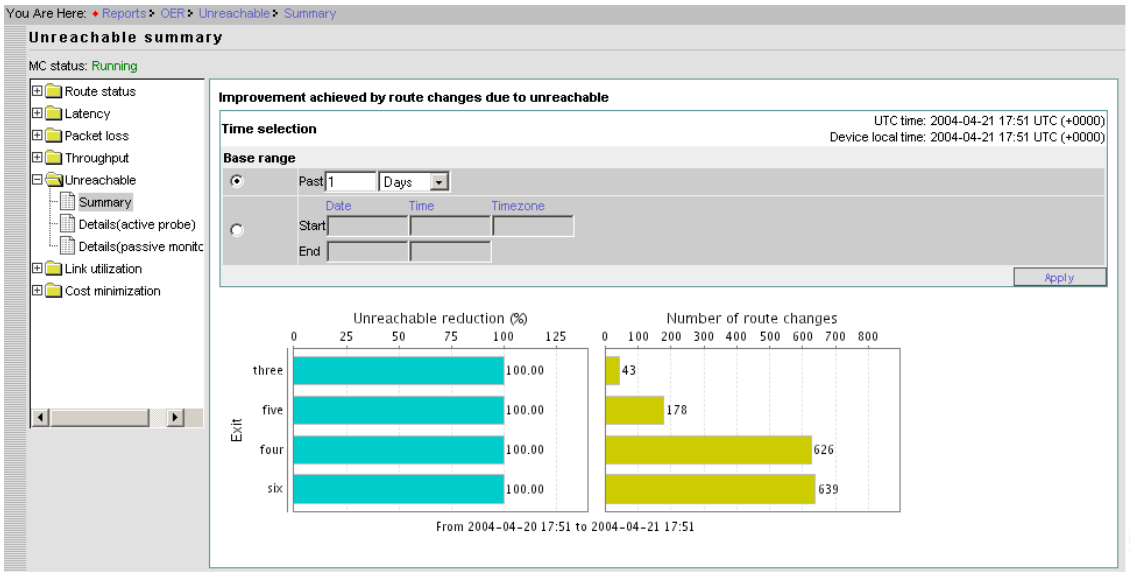
Under Unreachable, you can find the following type reports:

- Summary
- Details (active probe)
- Details (passive monitoring)

Summary

From the Contents list, open the menu under **Unreachable**, then click **Summary**.

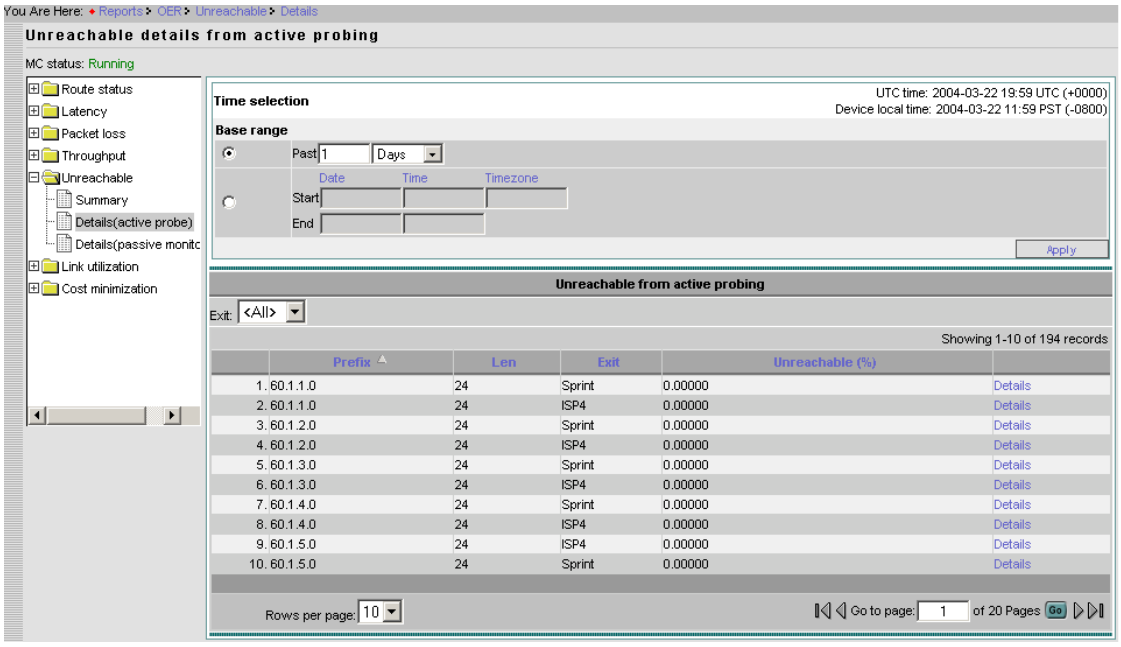
Figure 2-58 Reports > Unreachable > Summary



Detail - Active Probe

From the Contents list, open the menu under **Unreachable**, then click **Details (active probe)**.

Figure 2-59 Reports > Unreachable > Details From Active Probe

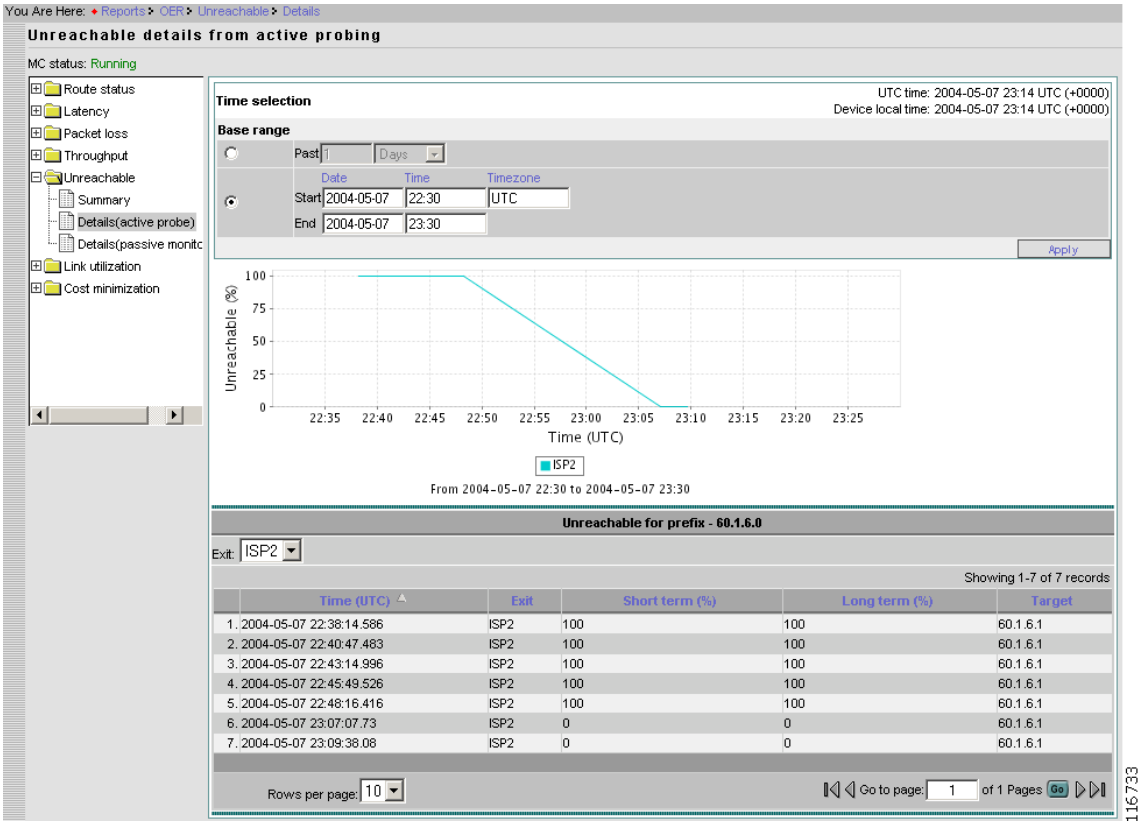


Prefix	Prefix.
Length	Prefix length.
Exit	Exit for which the data is displayed. Or, you can select **<All>**.
Unreachable	Percentage unreachable.

Active Probe Details for Selected Prefix

From the **Unreachable details from active probing** page, select the probe of interest, then click **Details**.

Figure 2-60 Reports > Unreachable > Details From Active Probe > Prefix Details



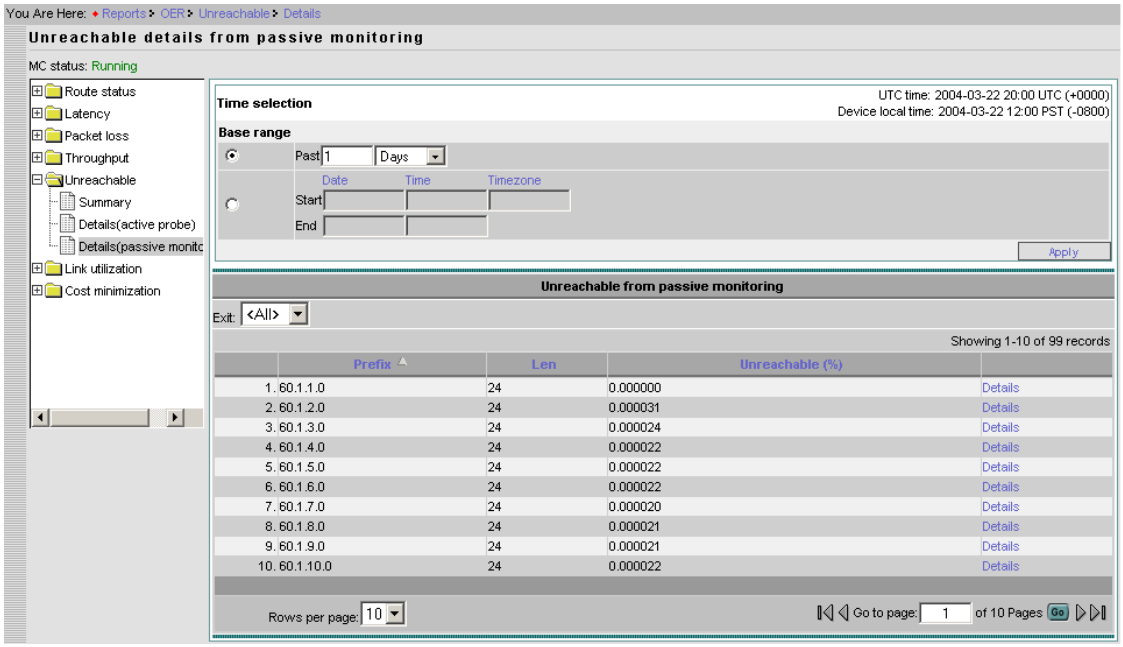
Time (UTC)	Time of report.
Exit	Exit for which the data is displayed. Or, you can select **<All>**.
Short term	Short term percentage Unreachable for Prefix.

Long term	Long term percentage Unreachable for Prefix.
Target	Target Prefix

Details - Passive Monitoring

From the Contents list, open the menu under **Unreachable**, then click **Details (passive monitoring)**.

Figure 2-61 Reports > Unreachable > Details From Passive Monitoring

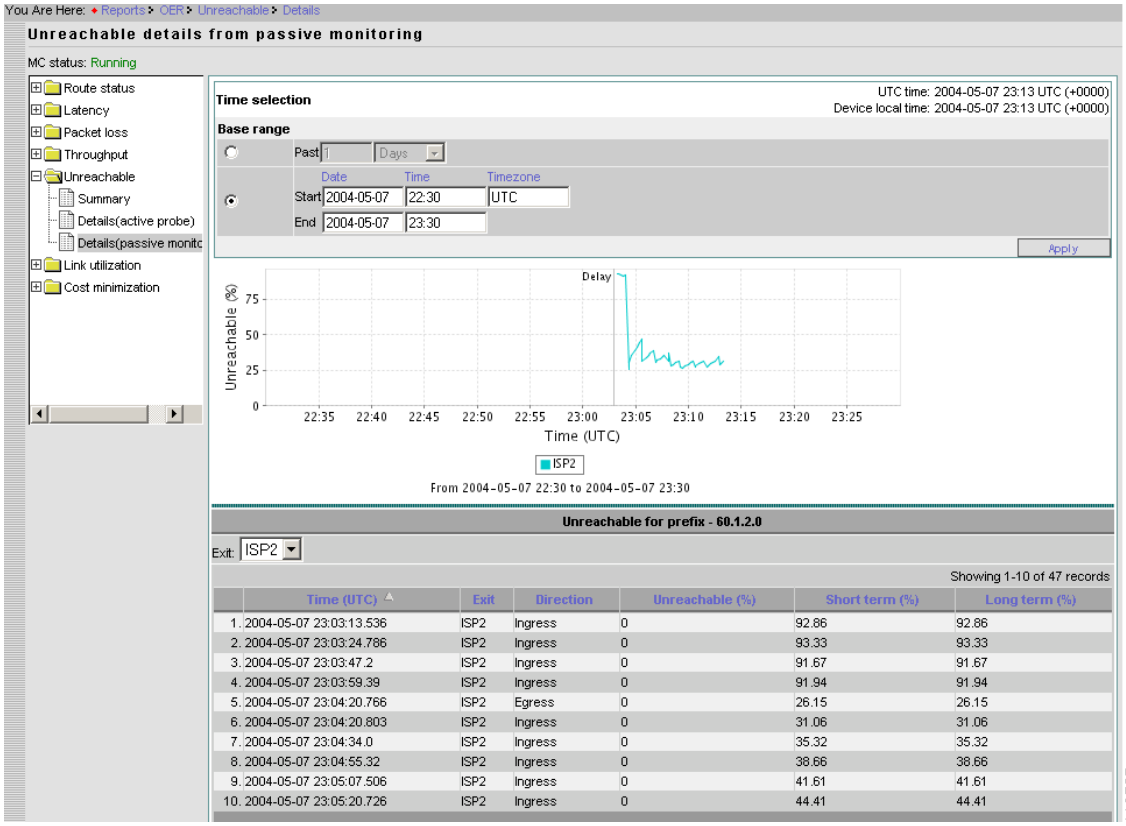


Prefix	Prefix.
Length	Prefix length.
Exit	Exit for which the data is displayed. Or, you can select **<All>**.
Unreachable	Percentage Unreachable.

Passive Monitoring Details for Selected Prefix

From the **Unreachable details from passive monitoring** page, select the probe of interest, then click **Details**.

Figure 2-62 Reports > Unreachable > Details From Passive Monitoring > Prefix Detail



Time (UTC)	Time of report.
Exit	Exit for which the data is displayed. Or, you can select **<All>**.
Direction	Direction of traffic.
Unreachable	Percentage Unreachable.
Short term	Short term percentage Unreachable for Prefix.
Long term	Long term percentage Unreachable for Prefix.

Link Unitization

Under Link Utilization, you can find the following type reports:

- Summary
- Details
- Distribution

Summary

From the Contents list, open the menu under **Link utilization**, then click **Summary**.

Figure 2-63 Reports > Link Utilization > Summary

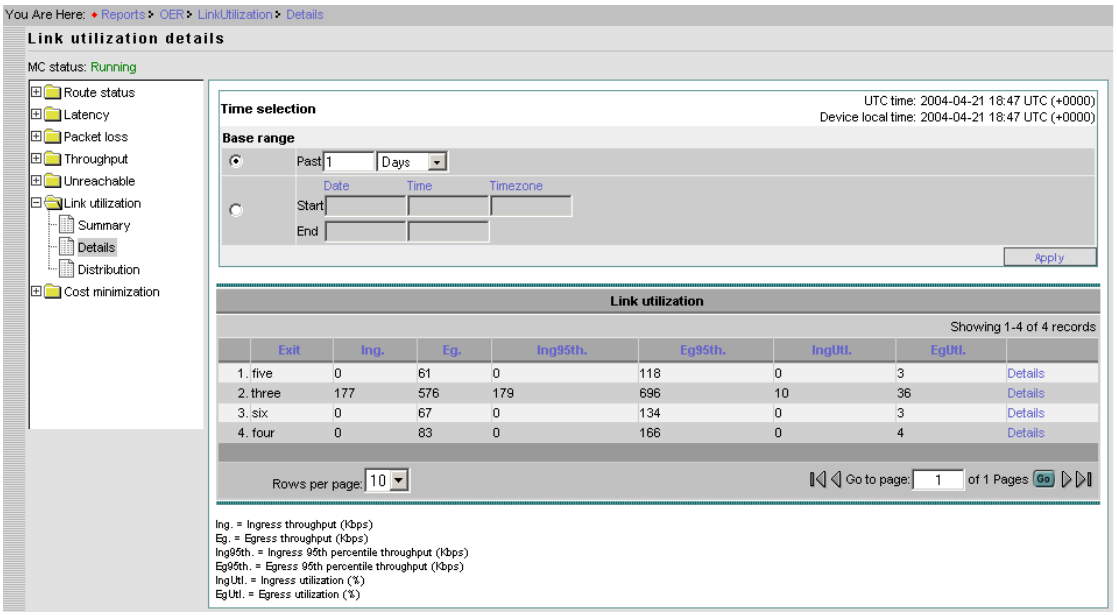
This graph shows throughput, 95th percentile throughput and utilization for ingress and egress direction of all the links for the selected time range.

Throughput and utilization are average values over the selected time range.

Details

From the Contents list, open the menu under **Link utilization**, then click **Details**.

Figure 2-64 Reports > Link Utilization > Details

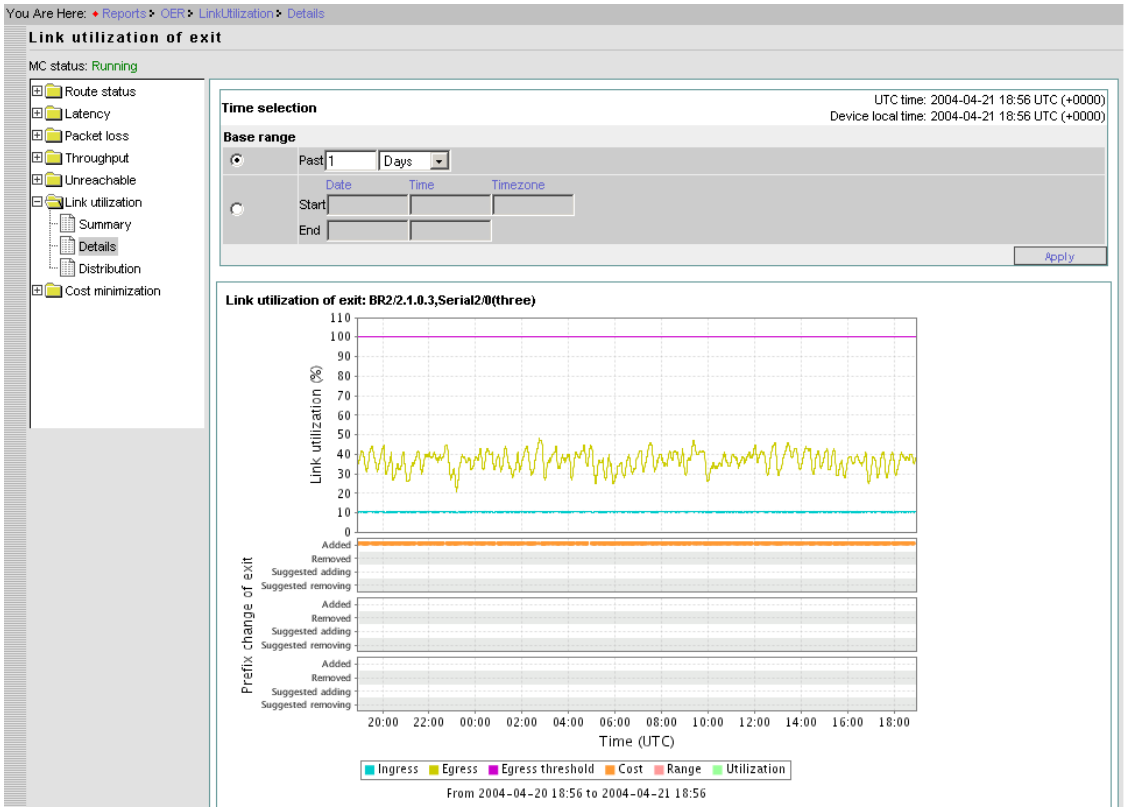


Exit	Exit where prefix is being forwarded.
Ingress	Ingress throughput.
Egress	Egress throughput.
Ingress 95th	Ingress 95th percentile throughput in Kbps.
Egress 95th	Egress 95th percentile throughput in Kbps.
Ingress utilization	Ingress utilization.
Egress utilization	Egress utilization.

Link Utilization Details by Exit

From the **Link utilization details** page, select an Exit, then click **Details**.

Figure 2-65 Reports > Link Utilization > Details > Exit Details



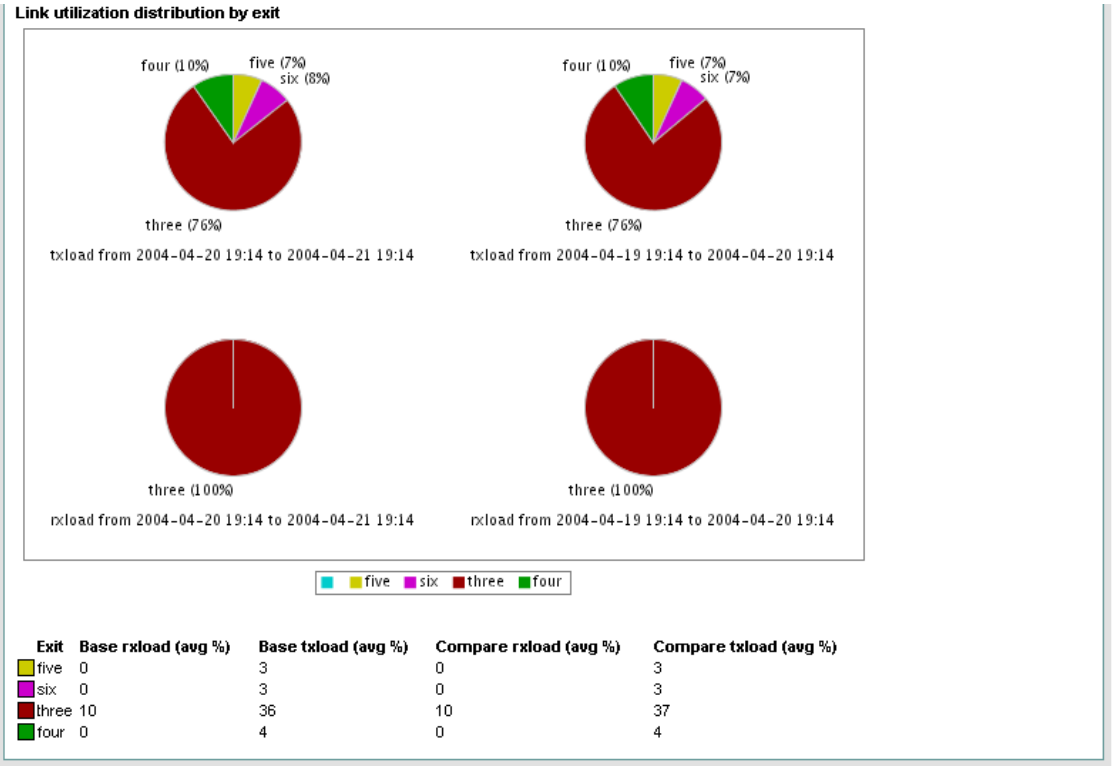
The graph shows egress utilization, ingress utilization, and max-egress-utilization (configured) in a time series chart. It also shows the prefix added and removed, to and from the link at the bottom of the chart.

One dot is displayed for each prefix added and removed. Further more, if Prefix is in Observe mode, the dot is displayed on *suggested adding* or *suggested removing*. The dots are color coded based the reason it was added and removed, to and from the link.

Distribution

From the Contents list, open the menu under **Link utilization**, then click **Distribution**.

Figure 2-66 Reports > Link Utilization > Distribution



This graph allows the you to compare distribution of traffic over two different periods.

The first period is called *base range* and the second period is called *compare range*.

The base range can be specified in two ways:

- Last x minutes/hour/days.
- Range of time: select start time and end time.

The compare range can also be specified in two ways:

- Minutes/hour/days before the start-time of the base range. If the base range is *Last one hour* and current time is11:00 pm, then the start-time is 10:00 pm.
- Select start time. In this case the time range is the same duration as the base range; if base range is one hour and the start-time (compare) is 3:00 pm, then the time range is from 3:00 pm to 4:00 pm.

Cost Minimization

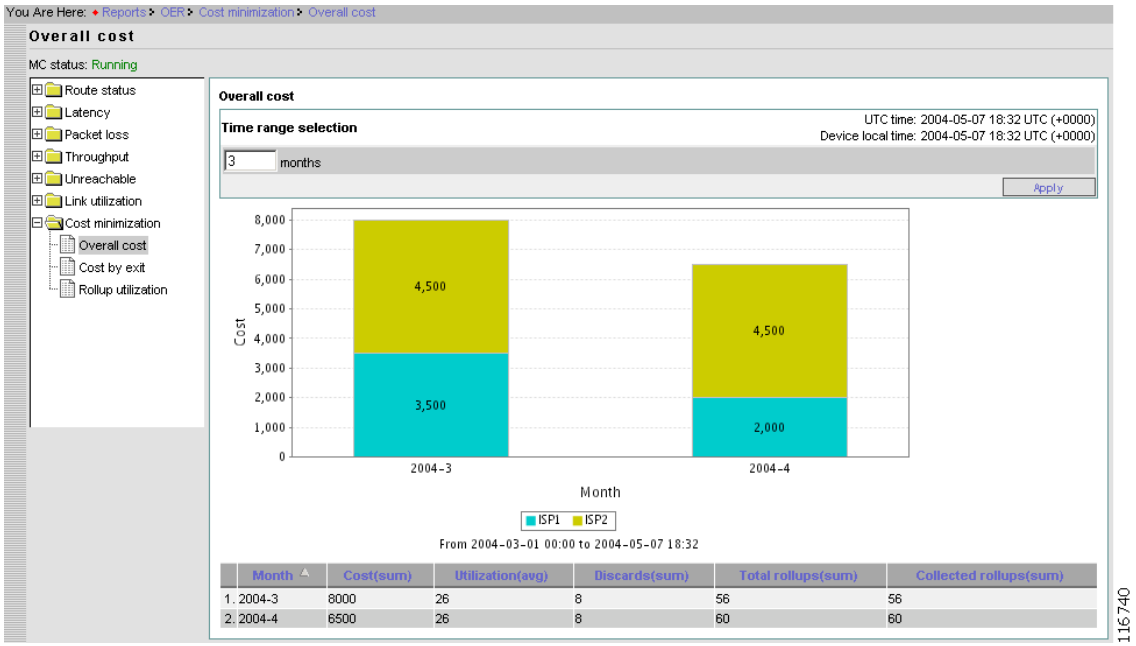
Under Cost Minimization, you can find the following types of reports:

- Overall
- Cost by exit
- Rollup utilization

Overall

From the Contents list, open the menu under **Cost minimization**, then click **Overall**.

Figure 2-67 Reports > Cost Minimization > Overall



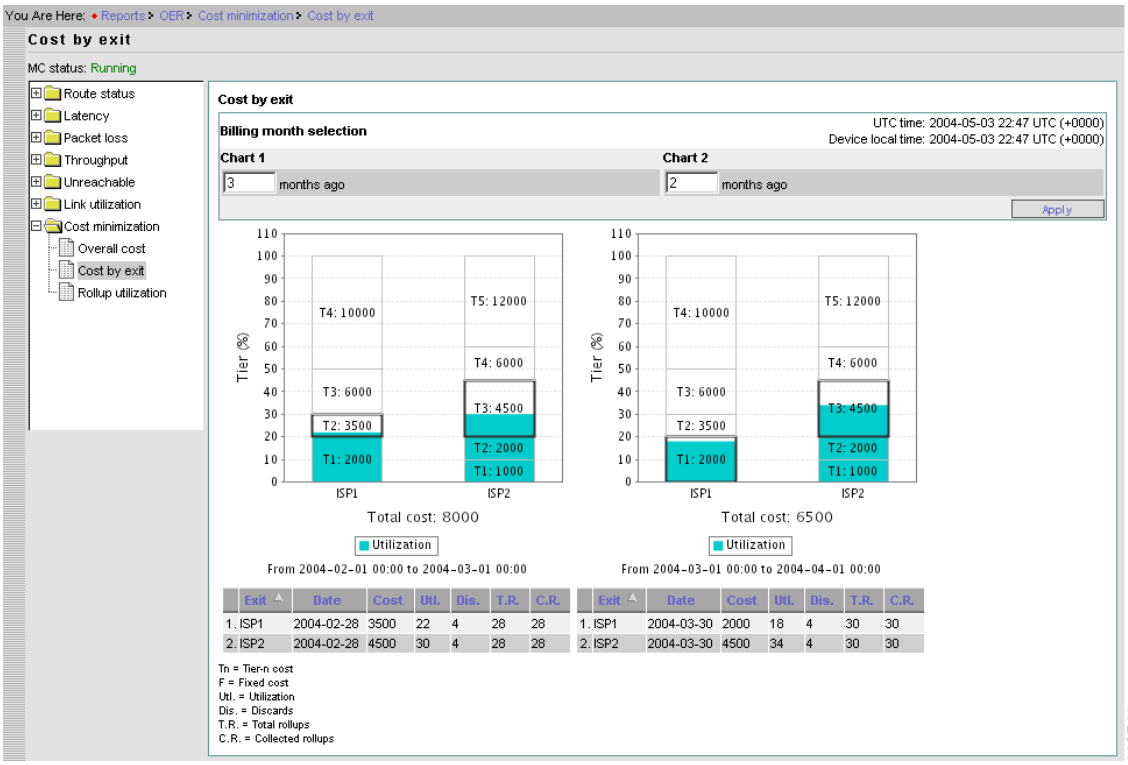
This page shows the overall cost for the number of billing periods selected.

For each billing period there is one stacked bar. The stack consists of the cost of each exit during that billing cycle.

Cost by Exit

From the Contents list, open the menu under **Cost minimization**, then click **Cost by exit**.

Figure 2-68 Reports > Cost Minimization > Cost by Exit



The graph displays the cost of each Exit for two different billing periods. Zero months ago is the latest billing period. One month ago is the billing period before the latest one.

The graph shows stacked tiers on top of the sustained utilization. This gives an indication in which tier the sustained utilization falls.

The table at the bottom of the page shows more details about Cost Minimization configuration and data used for the billing period. Brief description of each item is shown below.

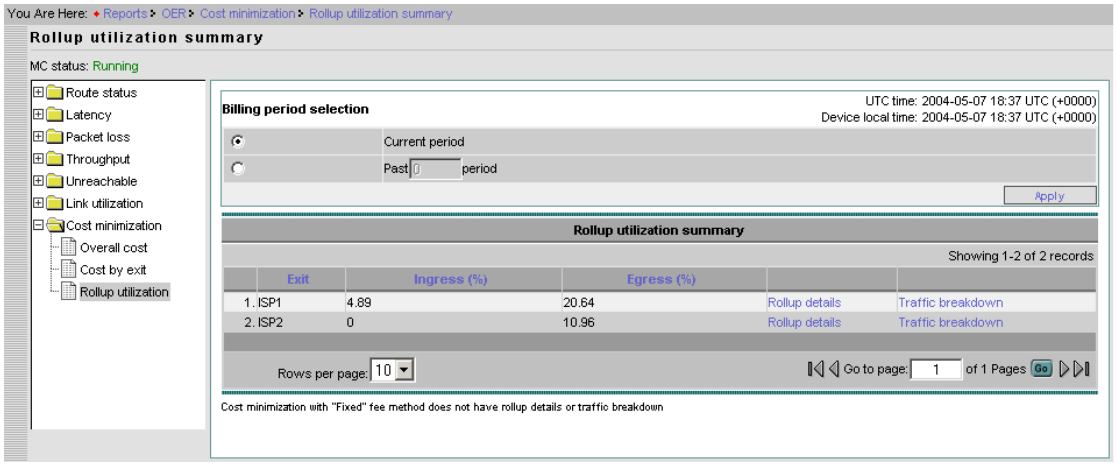
Cost	Cost per Exit.
Utilization	Sustained utilization (as calculated by the method configured) for the given period (months). This value is actually used to bill the customer.
Discards	Number of rollups that are discarded from the collected rollups at the end of the billing period. The discard rollup is configured in terms of percentage of total Rollups or in absolute terms.

Total rollups	Total rollups is the number of rollups in a billing period. For example, if the billing period has 31 days and rollup period is 15 minutes, then there will be 2976 rollups in the billing period.
Collected rollups	Number of rollup period for which the Cisco OER Master Controller Engine was able to collect the data. If it was started in the middle of the billing period or cost-minimization was configured half-way through the billing period, then the number of collected rollups would be less than the total rollups. If this value is not same as the total rollups then the billing estimate is calculated on partial data.

Rollup Utilization

From the Contents list, open the menu under **Cost minimization**, then click **Rollup utilization**.

Figure 2-69 Reports > Cost Utilization > Rollup Utilization Summary



Exit	Exit where prefix is being forwarded.
Ingress (%)	Link utilization due to incoming traffic. It is shown in Separate, Combined, and Summed methods.
Egress (%)	Link utilization due to outgoing traffic. It is shown in Separate and Combined, and Summed methods.

Rollup Details

From the **Rollup utilization summary** page, select an Exit, then click **Rollup details**.

Figure 2-70 Reports > Cost Utilization > Rollup Utilization > Rollup Details

Traffic Breakdown

From the **Rollup utilization summary** page, select an Exit, then click **Traffic breakdown**.

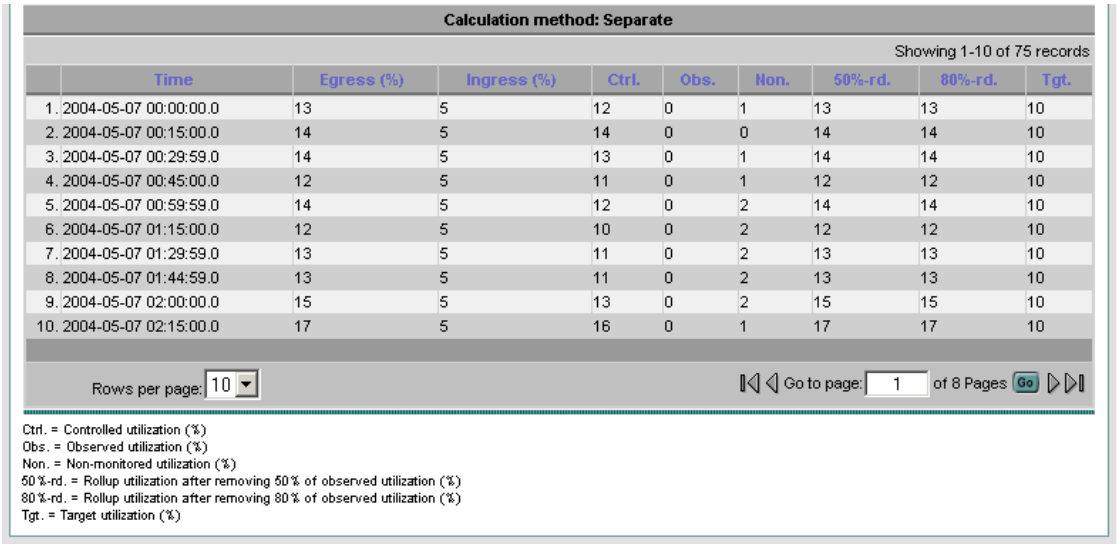
Figure 2-71 Reports > Cost Utilization > Rollup Utilization > Traffic Breakdown (Top Half)

This page shows the target utilization and actual utilization. The Cisco OER Master Controller Engine tries to keep actual utilization below the target utilization.

This page also shows egress utilization (summed utilization in case of Summed method) broken down into controlled, observed and non-monitored utilization.

In addition the graph also shows what would be the actual utilization if the Cisco OER Master Controller Engine was able to move 50%/80% of the observed traffic off of the link.

Figure 2-72 Reports > Cost Utilization > Rollup Utilization > Traffic Breakdown (Bottom Half)



Calculation method: Separate

Showing 1-10 of 75 records

	Time	Egress (%)	Ingress (%)	Ctrl.	Obs.	Non.	50%-rd.	80%-rd.	Tgt.
1.	2004-05-07 00:00:00.0	13	5	12	0	1	13	13	10
2.	2004-05-07 00:15:00.0	14	5	14	0	0	14	14	10
3.	2004-05-07 00:29:59.0	14	5	13	0	1	14	14	10
4.	2004-05-07 00:45:00.0	12	5	11	0	1	12	12	10
5.	2004-05-07 00:59:59.0	14	5	12	0	2	14	14	10
6.	2004-05-07 01:15:00.0	12	5	10	0	2	12	12	10
7.	2004-05-07 01:29:59.0	13	5	11	0	2	13	13	10
8.	2004-05-07 01:44:59.0	13	5	11	0	2	13	13	10
9.	2004-05-07 02:00:00.0	15	5	13	0	2	15	15	10
10.	2004-05-07 02:15:00.0	17	5	16	0	1	17	17	10

Rows per page: 10 Go to page: 1 of 8 Pages Go

Ctrl. = Controlled utilization (%)
Obs. = Observed utilization (%)
Non. = Non-monitored utilization (%)
50%-rd. = Rollup utilization after removing 50% of observed utilization (%)
80%-rd. = Rollup utilization after removing 80% of observed utilization (%)
Tgt. = Target utilization (%)

116745

Summed utilization	In case of Summed method egress and ingress utilization is added and showed as summed utilization.
Controlled utilization	Controlled Utilization. The part of the egress utilization which is contributed by the prefixes that are controlled by the Cisco OER Master Controller Engine. The value is approximate based on Netflow data.
Observed Utilization	The part of the egress utilization which is contributed by the prefixes that are in observe mode. The value is approximate based on Netflow data.
Non-monitored Utilization	The part of the egress utilization (or summed utilization in case of Summed method) remaining after deducting controlled utilization and observed utilization. This is mainly attributed by the prefixes that are not configured in the Cisco OER Master Controller Engine. The Cisco OER Master Controller Engine is neither controlling these prefixes nor observing these prefixes. It also includes the ingress utilization for summed method.
50%-reduction utilization	This value represents the total link utilization if the Cisco OER Master Controller Engine was able to remove 50% of the observed utilization had those prefixes been changed to control mode. This value is used to determine if these prefixes were changed to control mode would the rollup utilization be below the target utilization.
80%-reduction utilization	Same as 50%-reduction except that it uses 80% instead of 50%.
Target utilization	This the target utilization set at the beginning of the rollup period. The Cisco OER Master Controller Engine tries to achieve the average utilization of the link for the entire rollup period to be less than the target utilization. The target is calculated based on cost configured and the historical rollup utilization for the current billing cycle.

Troubleshooting

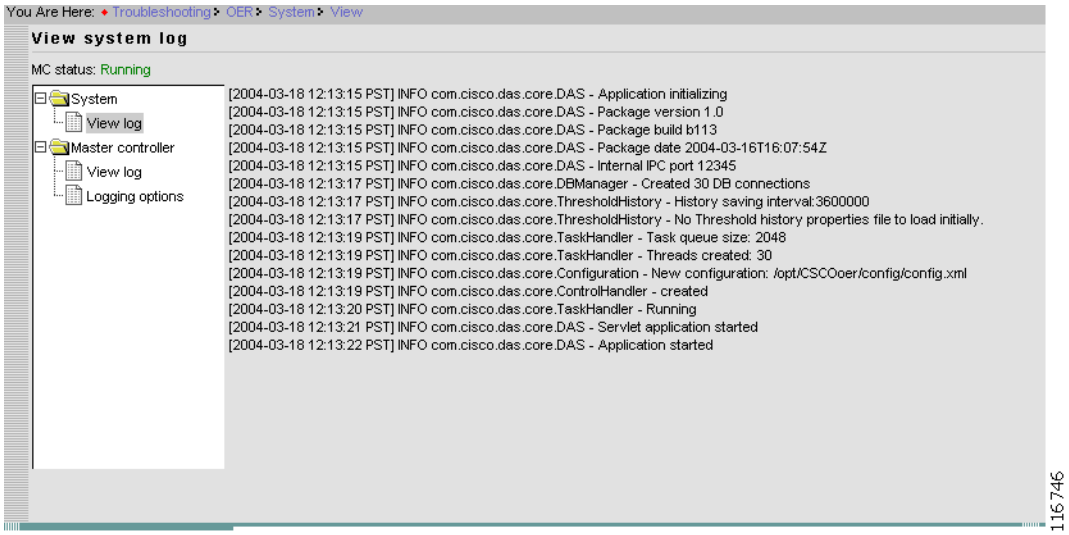
Troubleshooting main function displays the error and debug messages logged. There are two categories of logs:

- System log
- Master controller log

System Log

System log contains the messages pertaining to overall system. This yields logging of the Cisco OER Master Controller Engine startup, start, and stop activity.

Figure 2-73 Troubleshooting > System > View Log



Note An error message usually indicates that the Cisco OER Master Controller Engine has failed to start or stopped working.

Master Controller Log

The Master Controller log contains the error and debugging messages for Cisco OER Master Controller Engine operations.

This yields logging of events after the Cisco OER Master Controller Engine is up and running.

Figure 2-74 Troubleshooting > Master Controller > View Log

Usually, communication between the Cisco OER Master Controller Engine and border routers are logged. Each message is prefixed with local timestamp. Messages also contains the severity.

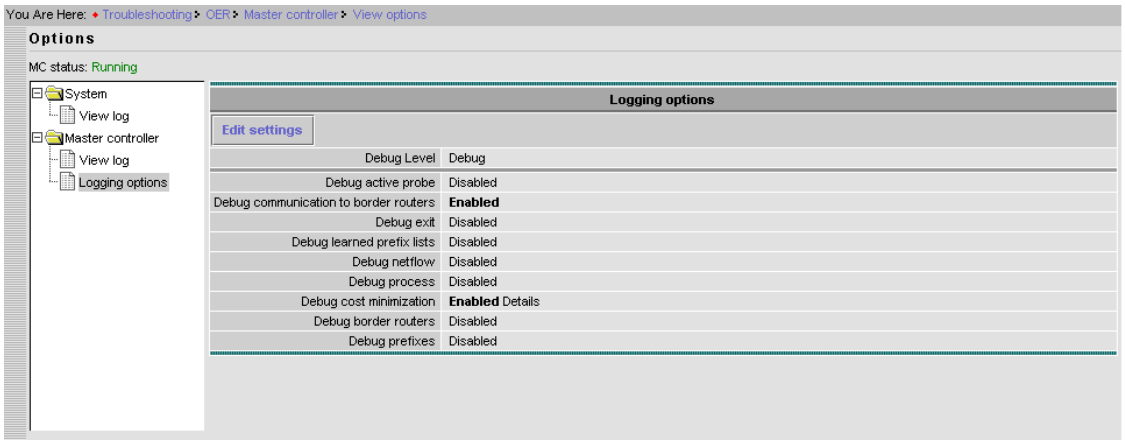
All the message with DEBUG severity also contains a component name. For example, following DEBUG message is from Communication Control (CC):

Mon Aug 11 11:20:27 2003: OER MC-6-DEBUG CC: BR TT status received: 10

Logging Options

From the Contents list, under **Troubleshooting** select **Master controller**, then **Logging options**.

Figure 2-75 Troubleshooting > Master Controller > Logging Options



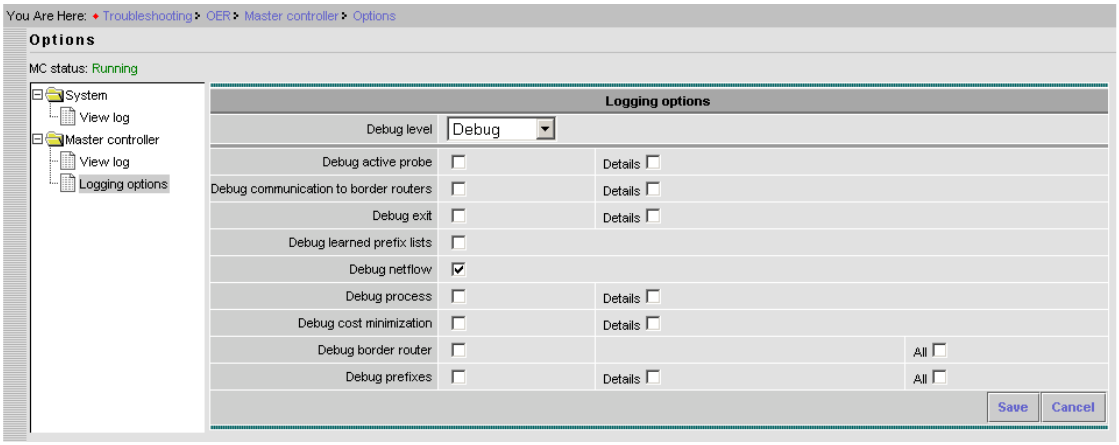
Debug Level	There are seven levels of debug information. Debug (most informative) Info Notice Warning Alert Error Emergency (least informative) If the level selected is Error, Emergency, Alert, and Error messages are logged. If level selected is Debug, all messages are logged.
Active probe	Logs debug message related to active probes; which includes creating, deleting, retrieving stats, and so forth.
Communication to border routers	Logs debug messages about communication between border routers and the Cisco OER Master Controller Engine.
Exit	Logs the debug message related Exit OOP, Exit statistics, and so forth.
Learned prefix-list	Logs the debug message pertaining to the process of learning prefix. It does not turn on debug on the prefixes that are learned.
Netflow	Logs the debug message related to netflow updates from the border router.
Process	Logs the debug message related to decision making process.

Cost minimization	Logs the debug message pertaining to cost OOP, cost algorithm.
Border routers:	Logs messages pertaining to Border specific events.
Prefixes:	Logs the message to specific prefix, or list of prefixes, or all prefixes. Once debug prefix is enabled, it provides an option to edit the debug prefix list.

Edit Settings

From the **Options** page, click **Edit Settings**.

Figure 2-76 Troubleshooting > Master Controller > Logging Options > Edit Settings



How to Set up Logging Messages Specific to a Prefix

Step 1 From Troubleshooting go to **Logging options**.

Step 2 Click **Edit settings**.

Step 3 Click **Debug prefixes**, then Click **Details**.

Step 4 Click **Save**.

The Logging options page appears showing Debug prefixes as **Enabled**.

Step 5 Click **View/Edit** for Debug prefixes

Step 6 Enter prefix of interest for **Prefix(IPv4)** and prefix length.

Step 7 Click **Add**.

Step 8 Repeat Steps 6 and 7 for more prefixes as required.

Step 9 When done, click **Done**.