CA Spectrum® IP Routing Manager

User Guide

Release 9.3

CA Technologies Product References

This document references the following CA Technologies products:

- CA Spectrum® (CA Spectrum)
- CA Spectrum® Report Manager (Report Manager)
- CA Spectrum® IP Routing Manager
- CA Spectrum® Service Performance Manager (SPM)
- CA Spectrum® Network Configuration Manager (NCM)
- CA Business Intelligence (CABI)

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Introducing IP Routing Manager

This section contains the following topics:

IP Routing Manager and Features

CA Spectrum IP Routing Manager (IPRM) was created as a tool to proactively monitor the state of IP routing protocols. IPRM also assists with troubleshooting failures and performance degradation impacting service delivery. The status of IP routing protocols is critical to the overall health of any environment's network. Additionally, IP Routing Manager helps you monitor and visualize the IP routed path(s) between critical endpoints in the network to ensure data flows over the most desirable and high-performing paths. Understanding the path that data takes is necessary to correlate service assurance alarms to their root cause.

CA Spectrum IP Routing Manager allows you to discover and view a network's topology by integrating with Route Explorer (REX). Route Explorer (REX) is an appliance-based route analytics solution developed and marketed by Packet Design.

CA Spectrum IP Routing Manager features include:

- Discovering and visualization of the Layer 3 network
- Providing visualization of Autonomous System (AS) and OSPF-specific hierarchies
- Discovering real-time Layer 3 paths through the network
- Providing dynamic updates to Layer 3 topology and paths
- Performing dynamic path monitoring:
  - Path hop details
  - Forward and reverse path support
  - ECMP support
  - Path change events/alarms
- Monitoring REX trap events/alarms
- Providing visualization of IP Subnets

- Providing bulk modeling of unmanaged devices
- Performing visualization of Layer 3 link information and custom icons
- Integrating Layer 3 topology view with other CA Spectrum's topology views (for example Universe)

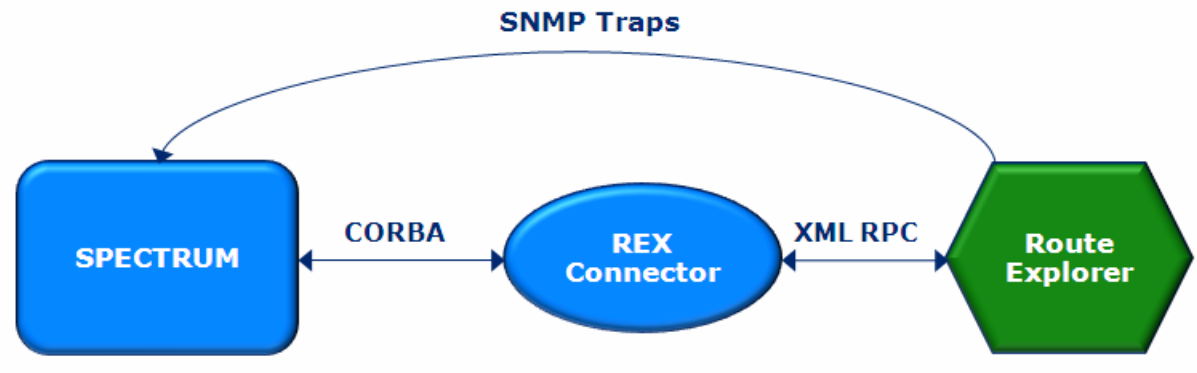
The product supports both fault tolerant and distributed CA Spectrum deployments, with all user configuration and interaction being performed on the main location server (MLS) system.

In addition to REX appliance, IP Routing Manager will also work with IPRM Route Recorder and OEMed versions of REX - RAMS from Hewlett Packard and Route Insight Manager from Juniper. IPRM Route Recorder (IPRM-RR) is a special version of REX that does not expose its GUI, but acts as instrumentation for IPRM delivering real-time routing information via an XML API. Packet Design will make this product available to CA Spectrum customers wishing to take advantage of IPRM.

IP Routing Manager Architecture and Concepts

IP Routing Manager utilizes the following architecture. The REX Connector is a separate process, and is the connection between CA Spectrum and Route Explorer. REX Connector utilizes the REX API to communicate with Route Explorer.

The Route Explorer software can be configured to notify clients of routing events via SNMP traps. Each one indicates some sort of Layer 3 topology change or information. These traps sent from Route Explorer will be translated into CA Spectrum events (and alarms when appropriate) and will be generated on the corresponding device model.

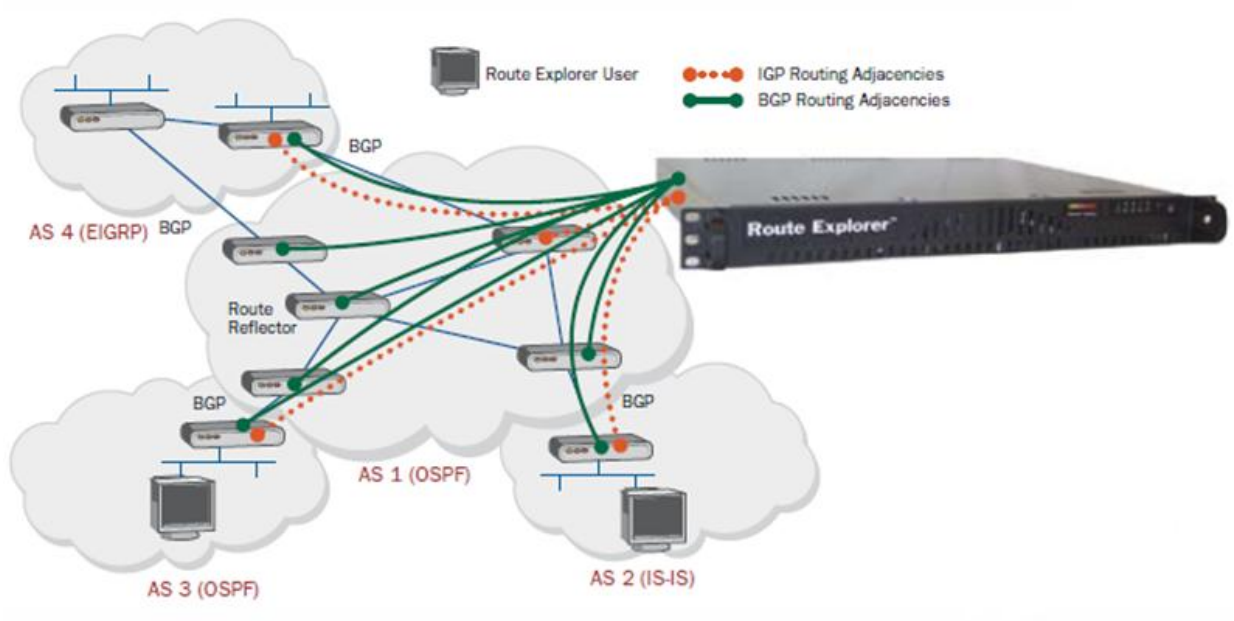


Some important concepts to understand to utilize IPRM fully:

- **IP Subnet** – An IP Subnet (REX refers to them as prefixes). IPRM distinguishes between two logical types of subnets:
  - **User Subnet** – IP Subnet attached to at least one router (also known as a gateway) and typically serving a number of hosts and devices. IPRM defaults to hiding these icons from the topology view.
  - **Infrastructure Subnet** – IP Subnet interconnecting two or more routers (REX shows them in its topology GUI as pseudo-nodes). In cases when only two routers are attached to such a subnet, IPRM can be configured to represent these as links in topology view, otherwise these are represented as IP Subnet icons.
- **PointToPoint Link** – IPRM's representation of Layer 3 Point-to-Point Links between two routers.
- **Managed Path** – End-to-end Layer 3 path across managed infrastructure configured for proactive assurance monitoring.
- **Autonomous System (AS)** – Part of the Layer 3 topology (a collection of routers and IP subnets), organized by REX into an Administrative Domain. IPRM also arranges OSPF protocol models within corresponding AS models.

Route Explorer Overview

A single Route Explorer can concurrently monitor and analyze complex IP networks which may have multiple routing protocols (OSPF, IS-IS, EIGRP, BGP) and span multiple autonomous systems. A distributed architecture involving multiple appliances may be employed to enhance management continuity in the event of a network failure while supporting multi-tiered or regionalized management domains.



The routing analytics appliance is developed and marketed by CA's Technology Partner - Packet Design. This appliance operates by passively monitoring the routing protocols exchanges between routers. It 'announces' itself as if it was a router, but doesn't advertise any prefixes, so no traffic flows to/through it. Therefore, it's neither a bottleneck nor a failure point.

IP addresses are assigned and adjacencies are set up with a small number of routers:

- REX requires an adjacency with one router in each OSPF area or IS-IS level. Once adjacencies are up, REX begins monitoring the protocols and is able to present a complete, network-wide map within minutes.
- Each adjacency may be over a physical connection (local) or GRE tunnel/VLAN (remote)

The only messages Route Explorer sends out to its neighbors are periodic 'Hello' messages to maintain adjacencies. Therefore, virtually zero load is placed on the real routers or the network, both during discovery and ongoing monitoring. REX can scale to manage the largest networks in the world (7,000 routers/8 million routes with a single box). In 99%+ of cases a single appliance is adequate.

REX has two interfaces, a web-based user interface for REX administration purposes and a graphical user interface for the end-user. IPRM-RR will have have the REX GUI disabled, to allow for easy CA Spectrum OneClick utilization.

Chapter 2: Integrating Route Explorer

This section contains the following topics:

Installing Route Explorer

See the *Route Explorer Administrator's Guide* for instructions about installing and configuring Route Explorer. You can download this guide from the Support web page on the Route Explorer appliance.

Route Explorer Administration

The following guidelines are helpful to Route Explorer Administration:

- Due to specific API requirements of the IP Routing Manager solution and known incompatibilities with earlier versions of the REX firmware, CA Spectrum r9.2.1 will support REX firmware version 9.3.16-R.

  Note: Additional future versions of REX firmware may be supported by CA Spectrum's r9.2.1 IP Routing Manager based upon API compatibility.
- In a distributed REX installation, for example, a modeling engine and one or more pure route recorder(s); you should configure IP Routing Manager's REX integration settings to connect to the modeling engine.
- Only one REX connection is supported.

REX Connector Process

IP Routing Manager communicates with REX via a process called the REX Connector. This process is managed by process daemon and started up when the SpectroSERVER is started. Because this process can use large amounts of CPU processing when Layer 3 topology discoveries are done, it is ideal to run CA Spectrum on a multi-CPU system.

- Integrates CA Spectrum with Route Explorer
- External Java-based application
- Implements a new CORBA interface allowing CA Spectrum to request Layer 3 topology and path information
- Translates CA Spectrum's CORBA-based requests into Java/XML-Remote Procedure Calls to access REX API

- Performs topology and path polling for change detection, notifies clients of changes via callbacks
- Supports configuration of Route Explorer alerts in the OneClick client
- Utilizes ports 14002 and 14006 to communicate with the SpectroSERVER and Naming Service
- Utilizes port 2000 to communicate with Route Explorer

Note: The REX Connector should run on separate CPU from SpectroSERVER if possible.

Important! IP Routing Manager will be communicating with the REX API via XML-RPC over a TCP connection. This TCP connection is not encrypted. This should be realized for data passing over the tunnel. However, as of Spectrum r9.2.1, the REX API password is encrypted.

Autonomous Systems

Router Explorer organizes protocol instances (for example BGP and OSPF) into groups called 'Administrative Domains'. You can create a hierarchical structure of Administrative Domains to arrange the protocol instances in a way that is coherent with your IT infrastructure. The IP Routing Manager data model provides the Autonomous System model as a logical container for protocol models. To provide continuity, as well as synchronization between the two data models, IP Routing Manager uses the Administrative Domain path as the name of the corresponding Autonomous System model.

For example, the following text is a sample topology name as provided by the REX API:

```
CA.MySubDomain.OSPF/Backbone
```

IP Routing Manager takes the text that precedes the protocol name, in this case OSPF, and uses it as the name of the Autonomous System model: 'CA.MySubDomain'.

You can set the model name on the Autonomous System model according to your needs.

Using the REX Administration Features

Refer to the *Route Explorer Administrator's Guide* for instructions on how to utilize the REX Administration web-based user interface.

Chapter 3: Installing and Configuring IP Routing Manager

This section contains the following topics:

Installing IP Routing Manager

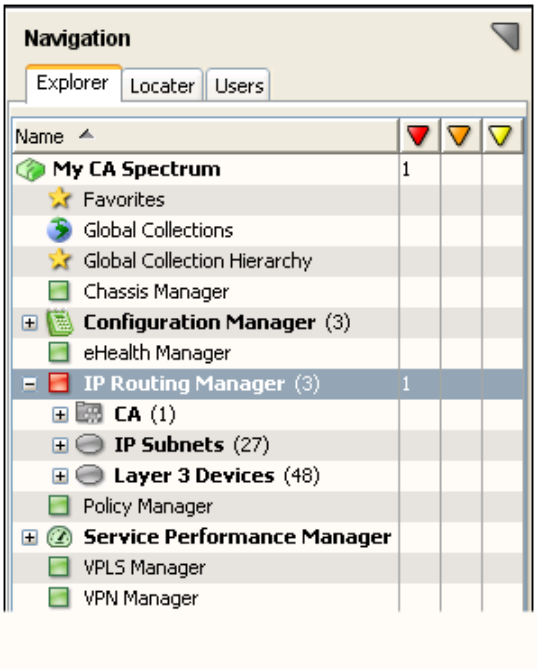
To install IP Routing Manager

1. Run the CA Spectrum installation program to install CA Spectrum and OneClick. See the *Installation Guide* for details.
2. Bring up the CA Spectrum Control Panel, click the Start SpectroSERVER button.

After installing this product, you will see an IP Routing Manager entry at the 'global' level in the Navigation Panel of the OneClick Console; the IP Routing Manager model of the Main Location Server (MLS) will be shown. This IP Routing Manager view is the central point for all Layer 3 topology-related activities: viewing Layer 3 topology and paths, configuration tasks, and general information gathering.

When you have discovered the Layer 3 topology, all Layer 3 topology and path data models representing the logical protocol hierarchy will be listed underneath the IP Routing Manager icon in the Navigation Panel. All Layer 3 paths you have created will be listed underneath the IP Routing Manager icon in the corresponding folder icon.

This panel also displays the entire Layer 3 topology across *all* CA Spectrum landscapes. It will also display all critical paths across CA Spectrum landscapes.



Note: IP Routing Manager *can* generate events and alarms even before it is setup or configured. This may happen because you previously configured Route Explorer to send traps to CA Spectrum; when CA Spectrum receives these traps, IP Routing Manager will generate the appropriate events/alarms regardless of whether or not it is setup and connected to Route Explorer.

Upgrading IP Routing Manager from 9.2.0 to 9.2.1

For sites who have configured/used IP Routing Manager in Spectrum 9.2 and are upgrading to a newer release (such as Spectrum 9.2.1), you will need to perform the following steps after the upgrade has finished installing.

To upgrade IP Routing Manager from 9.2.0 to 9.2.1

1. From the OneClick, Explorer option, select 'IP Routing Manager'.
2. Select the Contents, Information tab.
3. Expand the 'Route Explorer Integration' option and select Configuration.

4. For the 'Query Password' field, select the 'set' link and set the appropriate password value; and select Save when finished.

Important! This step needs to be performed even if the 'Query Password' has not changed. This will encrypt the password value and is *required* in order for IP Routing Manager to be able to connect to the Packet Design appliance.

5. If a fault tolerant SpectroSERVER is being used, then an Online Backup should be performed after re-setting the query password so that the attribute change is propagated to the backup SpectroSERVER.

6. After setting the Query Password, you can verify a connection from IP Routing Manager to Route Explorer by selecting Connect.

7. After successfully connecting to Route Explorer, perform a layer 3 topology discovery by selecting the 'Discover' option in the IP Routing Manager configuration subview. You do not need to clear the layer 3 topology first. (This step ensures that certain attributes are updated to support some of the new features introduced in IPRM 9.2.1.)

Connecting to Route Explorer

To connect to Route Explorer

1. Navigate to the Component Details Panel of the IP Routing Manager model.

2. Select the Information Tab, and open the Route Explorer Integration sub-view.

3. Enter the Route Explorer machine's host name, the query password, and the Administrative Domain name you'd like to use.

   You can also choose to enter a new heartbeat value. The heartbeat value determines how often IP Routing Manager pings Route Explorer to make sure it's still up and functioning.

4. Once these values are configured, press the Connect button.

   IP Routing Manager will then attempt to connect to Route Explorer, and you will be notified of the success/failure of the operation.

   Note: You will not be able to connect unless you authorize the SpectroSERVER to be able to connect with the REX machine through the 'Queries' Admin Page in the REX Web UI.

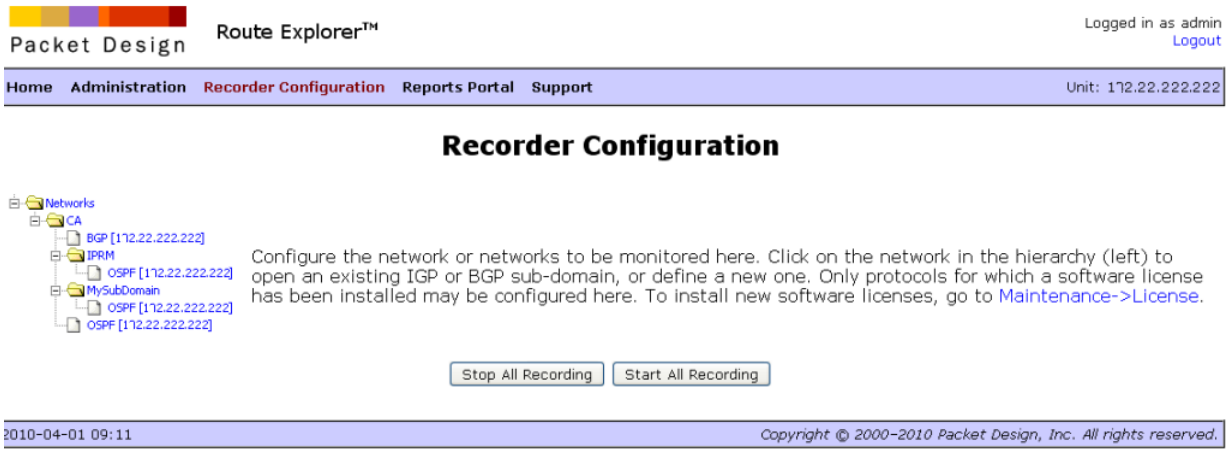
The Connection Status field displays the status of IP Routing Manager's connection to Route Explorer. Once connected, the Connect button will become a Disconnect button, which you can use to disconnect from Route Explorer when desired.

Note: To change any of these REX configuration settings, first disconnect from REX, make the required changes, and then re-connect for the changes to take effect.

Important: If Route Explorer stops recording information on particular protocols, IP Routing Manager will notify you through an event and alarm.

Route Explorer Configuration Considerations

When configuring the 'Administrative Domain' setting in the REX Configuration subview; you should refer to the 'Recorder Configuration' in the Route Explorer web interface. The 'Recorder Configuration' is accessed by logging into the web interface and clicking on the 'Recorder Configuration' in the menu at the top. In the case of a distributed REX deployment (where there are multiple Route Explorer units all replicating their data to a single Modeling Engine unit), refer to the 'Recorder Configuration' on the Modeling Engine's web interface.



The 'Recorder Configuration' page displays a hierarchy containing the Administrative Domains (represented as folders) and the protocol instances (represented as sheets of paper). The 'Networks' folder at the top of the hierarchy is the root folder and cannot be used when configuring IPRM. The next folder down is the top-level administrative domain. Enter the name of the top-level administrative domain into the Route Explorer Configuration sub-view in IPRM.

Chapter 4: Using IP Routing Manager

This section contains the following topics:

Initiating Layer 3 Topology Discovery

A topological model of your Layer 3 topology will be built and maintained inside the SpectroSERVER. The Layer 3 topology, including Autonomous System and OSPF protocol details, will be graphically displayed to you using traditional CA Spectrum device icons, new LAN icons, and pipes. All routers from all landscapes in the DSS will be displayed in this single view.

The entire Layer 3 routing hierarchy will be displayed in the OneClick Navigation Panel under the IP Routing Manager entry. Sub-hierarchies will include an entry for each Autonomous System (AS) that is being managed. Each AS will be further broken down into OSPF protocol details (if applicable). You will be able to expand the hierarchy to drill down and get detailed information about the IP Subnet topology.

Important! IP Routing Manager prevents creating duplicate Layer 3 paths. Duplicates are determined by source IPs, destination IPs, and path names.

To initiate Layer 3 topology discovery

1. Navigate to the Component Details Panel of the IP Routing Manager model.
2. Select the Information Tab, and open the Configuration sub-view.

   The Layer 3 Topology view contains buttons to discover and model the Layer 3 topology.

   Use the Topology and Managed Path Monitoring field to configure how IP Routing Manager should monitor the Layer 3 topology and paths. The various values supported include:

   - Traps and Scheduled Polling – REX Connector polls for changes, and SS responds to REX change traps
   - Initiated by Traps Only – No REX Connector polling, but SS does respond to REX change traps

- Off – No changes are detected. No REX Connector polling and no trap handling. You must manually initiate re-discovery.

If the Traps and Scheduled Polling option is used, you should set the value of Scheduled Polling Interval (s) to the desired value. When changes are detected, IP Routing Manager will dynamically update the Layer 3 topology with new and removed routers and links.

See the '*Without GUI component, how will I be able to configure IPRM-RR traps?*' question within the *Frequently Asked Questions* section for additional information.

3. Click the Discover button to begin the Layer 3 topology discovery and modeling process.

   Depending on the size of the Route Explorer database you've connected to, this process could take many minutes to complete. Once finished, the complete and current Layer 3 topology will be saved in the CA Spectrum database.

   Note: The Last Topology Update field will also contain the date and time of the discovery. The Last Topology Update field is updated every time CA Spectrum models a topology change.

Note: You can click the Discover button at any time to have IP Routing Manager update (or re-discover) the complete Layer 3 topology, and thus stay in sync with Route Explorer. You can also press the Clear button to completely remove all Layer 3 topology modeling (including Layer 3 paths that may have been discovered).

User subnets are discovered and modeled when you invoke a Layer 3 discovery or on dynamic updates. They are differentiated from Infrastructure subnets by a new attribute field in the models' Information Tab. You can choose whether or not User subnets are displayed in the Layer 3 topology view by setting the 'Display User IP Subnets' value in the IP Routing Manager Configuration sub-view.

Additional Discovery Explanation

The following items are important to consider in OneClick Integration:

- IP Routing Manager gathers data from all the distributed landscapes that you have configured and runs at a global level, above any landscape, in the Navigation Panel.
- When you deploy CA Spectrum in a distributed environment, you have multiple landscapes. You must assign one as a main location server. This is where all Layer 3 modeling is stored and then displayed at a global level. All the other landscapes communicate with this main landscape location.

Security Impact

The user privileges can be found in the Component Details panel of the selected user model in the Users tab. IP Routing Manager's privilege group contains the following values:

IPRM hierarchy

Allows a user to see the IPRM hierarchy.

Manage IP Subnet Paths

Enables/disables the path creation menu items and the Layer 3 Path configuration sub-view.

Configure IPRM

Shows/hides the Configuration sub-view on the IPRM model.

Configure Route Explorer Integrations

Shows/hides Route Explorer Integrations sub-view on the IPRM model.

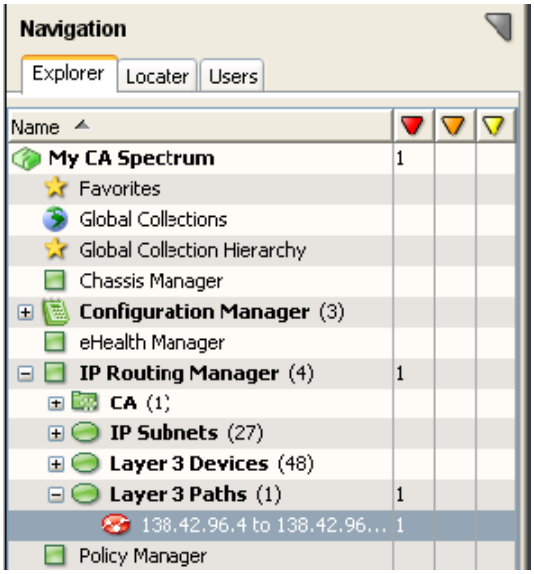
Layer 3 Topology Navigation

The following areas are important when utilizing Layer 3 Topology Navigation.

Navigation Panel

The entire Layer 3 routing hierarchy is displayed in the OneClick Navigation Panel under the IP Routing Manager entry. Sub-hierarchies include an entry for each Autonomous System that is being managed. Each Autonomous System is further broken down into OSPF protocol details (if applicable). You are able to expand the hierarchy to drill down and get detailed information about the Layer 3 topology.

A Layer 3 Devices container and an IP Subnets container exist in the Navigation Panel, allowing you to quickly find and spotlight any IP Subnet device or LAN currently shown in the topology (e.g. user LANs and LANs connected to only two routers are hidden by default, and are not listed in the IP Subnet container).



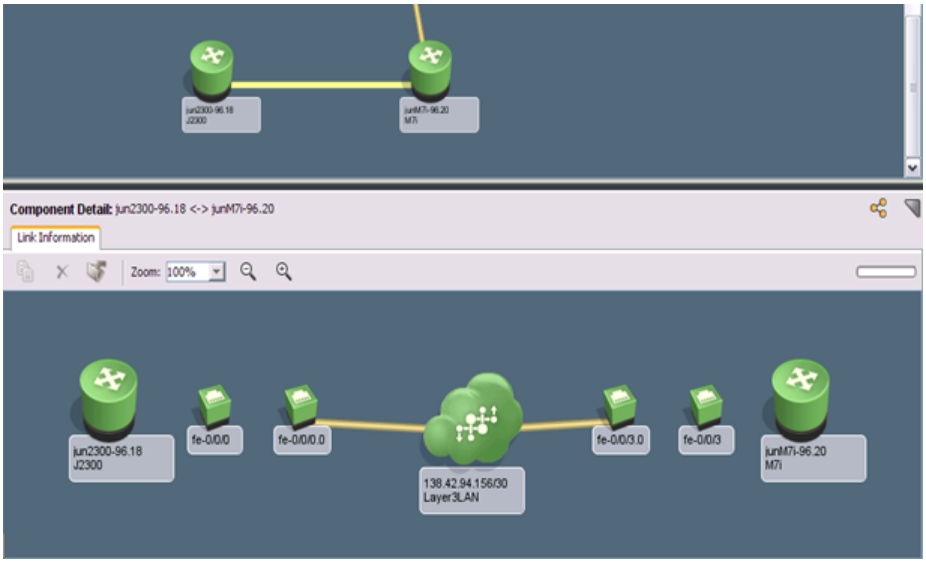
Topology Tab

A topological model of your environment's Layer 3 topology is built and maintained inside the SpectroSERVER. When the Topology Tab is selected, the Layer 3 topology, including Autonomous System and OSPF protocol details, is graphically displayed using traditional CA Spectrum device icons, new IP Subnet icons, and pipes. All routers from all landscapes in the DSS are displayed in a single topology view. A standard information view is provided for IP Subnets.

Additionally, a Link Information view is provided to show the port-level connectivity between routers and subnets, as well as show the hidden IPSubnet or PointToPointLink model for a given connection.

The Link Information tab has been enhanced with the concept of a middle model. If you select a link between two routers (a link which represents a IPSubnet or a PointToPointLink) in the Layer 3 topology, the Link Information view will show the port-level connections (if available) between the two routers, as well as the (hidden) IPSubnet or PointToPointLink model between the two routers. If you select a link between a router/UnmanagedDevice and a IPSubnet, the Link Information view will show the port-level connections between the router and that LAN.

Important! Interface connectivity will not be available if the connected router is currently modeled as an 'UnmanagedDevice'.



By default, the Layer 3 topology view will only show an actual icon for the IPSubnet when there are more than two routers connected to it. IP Routing Manager compresses the LAN icons connected to only two routers into a simple pipe. You could optionally turn on display of all IPSubnet icons (via the 'Display IP Subnet Between Two Routers' configuration option on the IP Routing Manager model). The ability to display IPSubnet icons allows you to refine the Layer 3 topology view to best suit your needs. PointToPointLink models are always represented as a simple pipe between two routers.

Mouse-over pop-ups are supported. Any time the mouse hovers over an IP Subnet icon, or any pipe connected to an IP Subnet, simple information about the IP Subnets and connected interfaces will be displayed.

List Tab

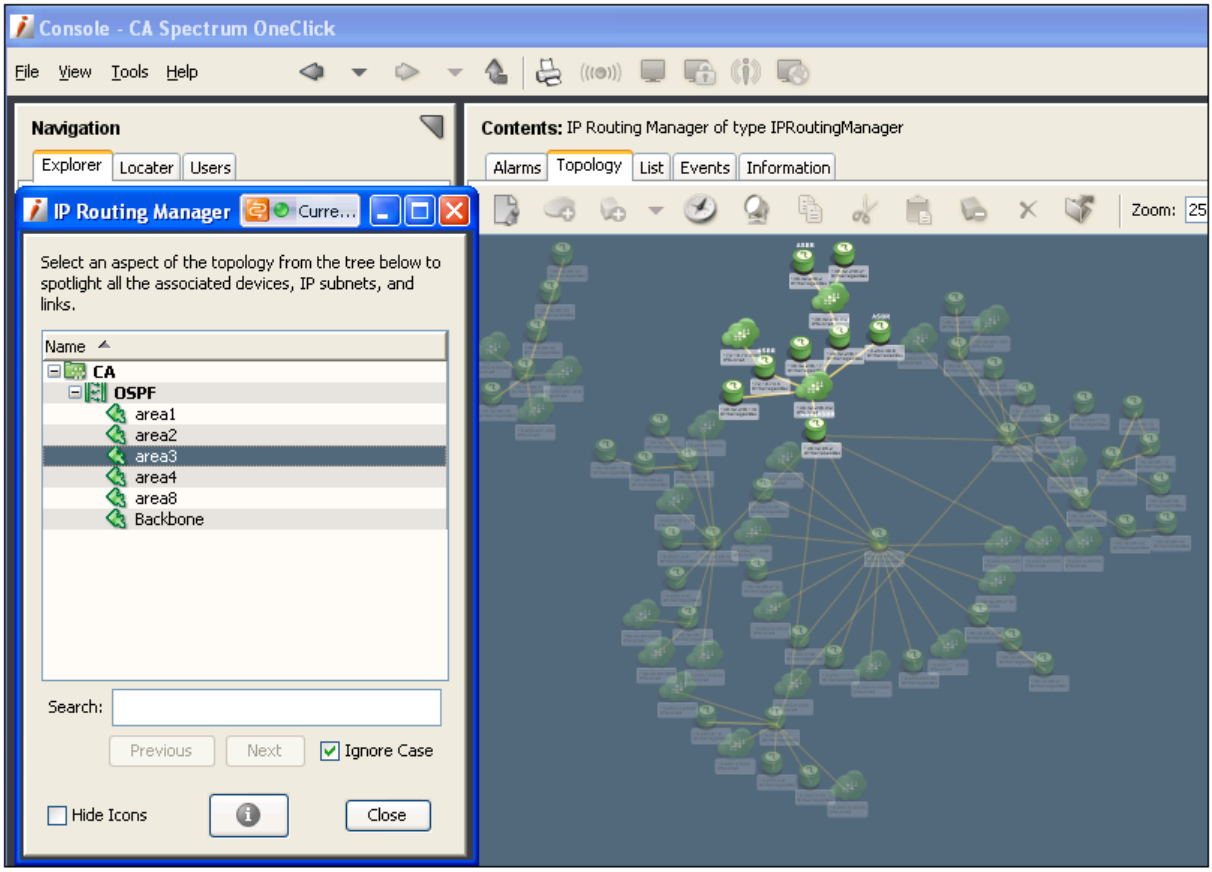
The List Tab of the IP Routing Manager model contains information about all routers and subnets that exist in the IP Subnet topology. The contents of the List Tab will be filtered based on what is selected in the Navigation Panel. Let's say you select an OSPF area. In the Topology Tab, all routers, subnets, and pipes involved in the OSPF area are spotlighted, and the rest are grayed out. The List Tab will then only display the models that are spotlighted. The List Tab contains a new Layer 3 Node Type column which displays the role each router is playing in the Layer 3 topology. Highlighting each model in the List Tab allows you to explore the Component Details of each model. IPSubnet and PointToPointLink models display AS and OSPF-specific data, as well as the designated router IP.

Spotlighting

A new navigation-based spotlighting capability has been introduced. Selecting (highlighting) a Layer 3 path model in the Navigation Panel will cause that particular path to be spotlighted in the IP Routing Manager's topology view. This Navigation Panel feature can be thought of as a built-in spotlighting feature that you can access *without* clicking the spotlight icon in the top menu and opening a separate dialog box. It's built right in.

This product also supports the traditional toolbar-based spotlighting dialog box, similar to VRRP and VLANs, so that you can un-dock the topology view and still use the spotlighting feature. When opened, the dialog box will contain a Layer 3 hierarchy exactly like the one displayed in the Navigation Panel. Toolbar-based spotlighting takes precedence over Navigation-based spotlighting.

For example, when you select an OSPF area in the Navigation Panel, all routers, subnets, and links which are members of the selected OSPF area will be spotlighted. The rest of the topology view will be grayed out. Spotlighted router icons will display protocol-specific annotations such as ABR and ASBR and the like.



Unmanaged Devices

All routers that Route Explorer knows about may not be modeled in the CA Spectrum DSS environment. When this happens, an UnmanagedDevice model is created, and its NetworkAddress attribute is filled in with the IP address of the router. UnmanagedDevice models are displayed in the Layer 3 topology just like 'full' CA Spectrum router models.

To model an UnmanagedDevice as a 'full' CA Spectrum router model, you have two options:

1. Right-click the icon and select 'Manage selected device…'. The Create by IP dialog opens, which lets you discover the device and replace the new model in all CA Spectrum views where the current UnmanagedDevice model exists.
2. Select multiple UnmanagedDevice models in the IP Routing Manager List Tab. Right-click and select 'Manage selected devices ...' to launch an AutoDiscovery. Auto discovery automatically populates the IP range list with the IP addresses of all selected models.

Both methods of discovery allow you to select which landscape (if in a DSS) to place the newly discovered device models.

In addition to the Model Unmanaged Device menu option, you can use the Discovery application to model your unmanaged devices. Every time AutoDiscovery is run, it will always attempt to replace any UnmanagedDevice models with a newly discovered device in its results set.

The existing context-launch functionality of Discovery is leveraged to allow users to select one or more UnmanagedDevice models in the topology tab and the list tab, and then launch Discovery from the toolbar or right-click menu. Discovery uses the IP information from the selected UnmanagedDevice models to create a new Discovery configuration. The Discovery configuration can then be used to discover the unmanaged devices and create device-specific models to replace the UnmanagedDevice models.

During the final stages of a modeling process (within the Discovery app), the CA Spectrum searches all landscapes for UnmanagedDevice models. It then compares the IP addresses of the newly modeled devices with the IP addresses of the UnmangedDevice models. If an address from a new model matches the address from the UnmanagedDevice model, the UnmanagedDevice model is replaced with the new device-specific model (even if the new model is a Pingable). In the IPRM topology view, the UnmanagedDevice icon is replaced with the icon of the new model.

Jump to Feature

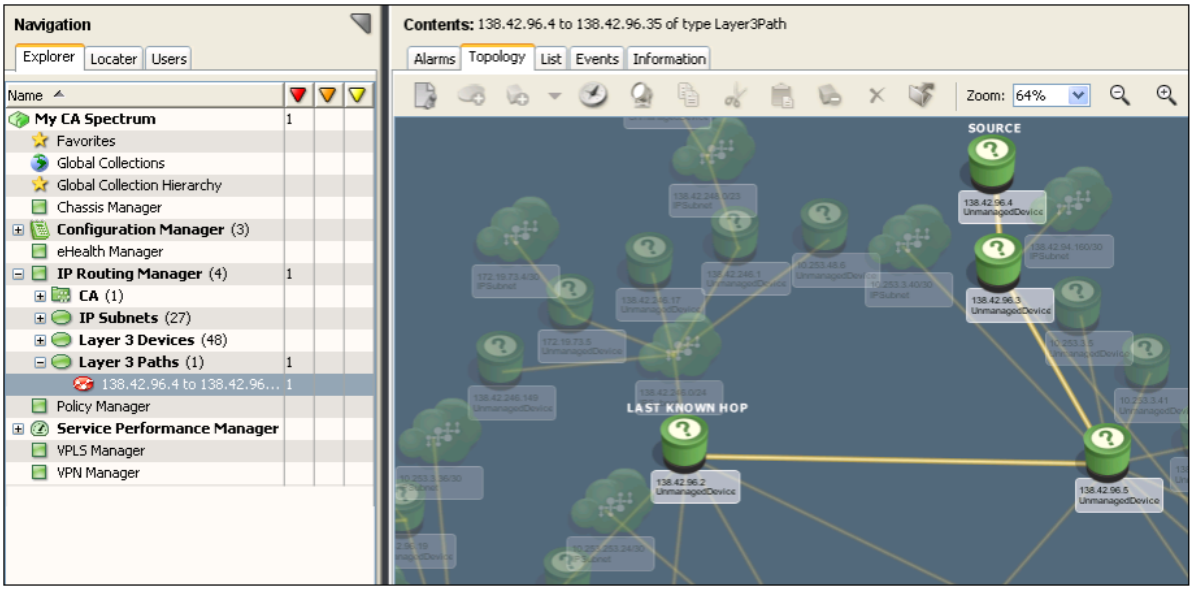
You are able to right-click on any router in the Layer 3 topology and select Location, Universe. This enables you to view the traditional CA Spectrum topology/universe view of the container model in which the router model exists. If the router model exists in a remote landscape in a DSS environment, it supports this as well. The router model is highlighted in the view. This feature is the key to integrating the new Layer 3 topology with the traditional CA Spectrum modeling and viewing hierarchy (Layer 2).

You are also able to right-click on any router in a traditional CA Spectrum topology or any other OneClick view and select Location, IP Routing Manager. This enables you to jump to the new Layer 3 topology view of the MLS and highlights the router in the view.

Important! The most efficient way to search when you have a long list of models in the Explorer is to find the model using a Locater search, select the found model, right click and select Location, IP Routing Manager.

Providing End to End Layer 3 Path Visualization

IP Routing Manager provides end-to-end Layer 3 path visualization. This provides you with hop-by-hop paths and alerting on critical paths.



Using the Layer 3 Path Discovery Feature

You have the ability to view and monitor the current Layer 3 path(s) between any two IP-based endpoints within REX's visibility on demand using OneClick.

Using the Layer 3 Path Discovery Feature

1. Select the start point in the IP Routing Manager Topology View; right-click on the node and select 'Utilities, Select As Layer 3 Path Source'.
2. Select the end point in the IP Routing Manager Topology View; right-click on the node and select 'Utilities, Create Layer 3 Path'.

   This will bring up up a new dialog for you to enter additional information.

   A name for the Layer 3 path is automatically created by CA Spectrum, but you can assign any name in the dialog box. When manually entering path destination IP address information, you may choose a single device/port IP address, or a subnet IP/mask pair. The path source must be a single IP address of a router. When entering an IP subnet for the path destination, dotted-decimal or CIDR suffix notation may be used for the mask.

   Note: Duplicate Layer 3 paths cannot be created. Duplicates are determined by source/destination IPs, as well as path names.

   You also have the option to discover only forward paths between the source and destination, or both forward and return paths. Discovering return paths will help you discover asymmetric paths, as well as add to IP Routing Manager's ability to detect when a path is down.
3. Click the OK button in the Create Layer 3 Path dialog to initiate path discovery and modeling.

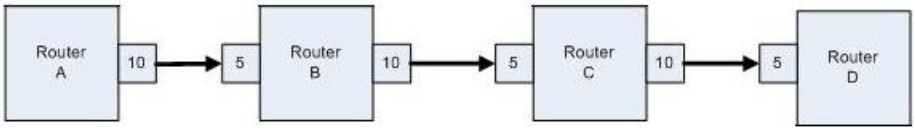
   When finished, the new Layer 3 path model is displayed in the Navigation Panel under a new Layer 3 Paths container in the IP Routing Manager hierarchy.

Important Considerations

There is no separate monitoring mode for paths. All paths will be monitored for changes according to the global Topology and Managed Path Monitoring value.

When you trace a path to a loopback IP on a router, there's a good chance that REX will include the last internal hop in its cost calculation and hops returned. Since IP Routing Manager has no way to graphically display this internal hop in the topology view, the REX Connector prunes it from the data returned, and IP Routing Manager doesn't show it in the topology view or the path hop details table. The cost of the internal hop is included in the overall path cost, however.

The cost of a path is determined by adding the routing metrics assigned to each of the egress interfaces of each hop in the path. See the attached picture for an example. The path is from the loopback IP address of router A to the loopback IP address of router D. The path data REX sends will contain a path cost of 31. This is the sum of all egress interface metrics, plus the internal hop of router D. Since IPRM cannot visualize the internal hop in router D, it doesn't include that hop in the Path Hop Details table.



Important! IP Routing Manager currently only supports creation of Layer 3 paths whose endpoints are within REX's visibility. If you enter an IP/subnet that is outside this visibility, then the path may not be complete, and a path lost alarm could be generated.

Layer 3 Path Viewing

Selecting a Layer 3 path model in the Navigation Panel allows you to view data about the path. The Component Detail panel contains source and destination IP information, the cost of the path, the number of hops, and the date/time it was discovered or last updated.

If the path has more than one equal-cost multi-path (ECMP), then CA Spectrum creates separate Layer 3 ECMP models, and displays them as children of the Layer3Path model in the Navigation Panel. When you highlight a Layer 3 Path in the Navigation panel, the Layer 3 topology will spotlight all of the routers, subnets and connections which are included by all of the associated ECMP's. When you highlight a specific Layer 3 ECMP in the hierarchy, the topology will spotlight only the routers, subnets and connections which represent that particular ECMP.

Note: Alarms are never generated on ECMP models, only the Layer 3 Path model. Thus, an ECMP model will always be green.

Select a Layer 3 Path or ECMP to view the Path Hop Details table, which contains dynamic, comprehensive information for each hop in the path. Details include source/destination routers, ingress/egress interfaces, link type and prefix, hop cost, and protocol.

Note: Path Hop Details are dynamic only when 'Topology and Managed Path Monitoring' is set to 'Traps and Scheduled Polling' or 'Initiated by Traps Only'. For more information, see Initiating Layer 3 Topology Discovery (see page 19).

You can destroy Layer 3 Path models by simply right-clicking on them in the OneClick Navigation Panel and selecting Delete.

In REX, pseudonodes represent IP Subnet IP subnets/LANs. The REX GUI displays them as nodes in the topology with routers connected to them. REX considers pseudonodes as distinct hops in a Layer 3 path. For example, for a path between 3 routers (A, B, and C), there will be two IP subnets (X and Y) with one between each router. REX would consider this path to have 4 hops: A -> X, X -> B, B -> Y, Y -> C.

IPRM uses pseudonodes to create IPSubnet models, and displays them similarly to how REX displays them. But in Layer 3 Paths, IPRM treats pseudonodes (IPSubnets) as something that a hop transitions through. So, for the path above, IPRM says the path has 2 hops: A -> X -> B, B -> Y -> C. A subnet is not really a hop endpoint, but a portion of the network that the data travels through to get to the next hop.

Note: In Route Explorer version 9.3.16, pseudonodes are no longer recognized as distinct hops in a path. Instead, pseudonodes are now treated similarly to how IP Routing Manager recognizes them.

Layer 3 Path History

The Layer 3 Path history feature allows the user to view changes in the Layer 3 path between two end points over a specified period of time.

Using the Layer 3 Path History Feature

1. Select the start point in the IP Routing Manager Topology View; right-click on the node and select 'Utilities, Select As Layer 3 Path Source'.
2. Select the end point in the IP Routing Manager Topology View; right-click on the node and select 'Utilities, View Layer 3 Path Change History'.

   This will bring up a new dialog.
3. In the dialog, enter the time range for historical data you want to view.
4. Click the View History button.

   The Path Change History table appears.

   Note: The content of the Path Change History table is static. For dynamically updated information on the path, use the Path Hop Details table as described in Layer 3 Path Viewing (see page 29).

Viewing the Path History of a Monitored Path

For any Layer 3 Path model you have created you have the ability to see the path change history for that monitored path.

- Right click on an existing Layer 3 Path model in the explorer view and select 'Utilities, View Layer 3 Path History' top launch the path history view.

  This automatically fills in the Source and Destination IPs for the dialog.

Viewing the Path History from an Alarm

If you receive a Layer 3 Path Lost or a Layer 3 Path Change alarm you can view the path change history.

- Right click on the alarm in the Contents Panel and selecting 'Utilities, View Layer 3 Path History'.

Important Considerations

Note: For Spectrum r9.2.1, If IP Routing Manager is connected to a Packet Design appliance that is running version 9.2 or greater of the Packet Design/Route Explorer software, the Path Change History's 'Link Prefix' column may contain missing values.

The path change history functionality works by taking samples of the Layer 3 topology at specified times. By default IPRM take 100 samples over the time range. This is the maximum allowed; the minimum is 5. If you experience performance problems or the path history takes a long time to render you can reduce this value by setting a parameter in the $SPECROOT/IPRM/REX/config.xml file:

```
<path_history_sample_count>10</path_history_sample_count>
```

Note: CA Spectrum recommends setting this value to 30 for 2x series Packet Design appliances running REX software below version 8.0. For 3x series appliances running REX software 8.0 or higher, you can experiment setting the value as high as 100 (which is the default) depending on the size of your Layer 3 topology.

Useful Tips

The following presents useful tips for CA Spectrum's IP Routing Manager for the CA Spectrum r9.2.1 release:

- REX Connector should run on separate CPU from SpectroSERVER if possible to reduce impact on SpectroSERVER. This is because when Layer 3 discovery is performed, the REX Connector causes additional CPU usage. This is primarily applicable to Windows, which can be adjusted by using Task Manager's 'Set Affinity' option. UNIX/Linux applications handle the load balancing better.
- You must disconnect from REX to change REX configuration settings (for example, REX administrative domain), and then re-connect for the changes to take effect.
- When using Monitoring Mode = 'Off', you must manually configure topology and path-related change notifications (traps) within REX GUI beforehand.
- Disconnected routers age-out of REX database slowly. The time for the disconnected routers to age out of the REX database is based on the routing protocol being used. In the case of OSPF, it is approximately one hour.
- Use 'Clear Layer 3 Topology' button to start over. This deletes all IPRM modeling in MLS, including subnets, paths, and UnmanagedDevice models.

- An AutonomousSystem in IPRM is equivalent to an 'Administrative Domain' in REX.
- Source and destination of Layer 3 paths must be within REX's visibility.
- When tracing a path to a router loopback IP, the last internal hop is used in cost calculation and number of hops, but not included in path hop details nor topology view. This last internal hop is not represented visually in topology view.
- In OneClick, the 'View Layer 3 Path Change History', 'Create Layer 3 Path' and 'Select as Layer 3 Path Source' menu items may be disabled in the Tools, Utilities menu. These items are enabled/disabled based on what is currently selected in the Explorer tab.

  For example, if you select a router model under the 'Layer 3 Devices' container in the Explorer tab, all three of these menu items will be enabled under Tools, Utilities.

Chapter 5: Alarms and Events

This section contains the following topics:

Alarm and Event Configuration

CA Spectrum 9.2.1 adds the ability to manage the alert configurations on the Packet Design appliance via a subview in OneClick. Expanding the Route Explorer Integration, Alerts subview reveals the alert configuration settings. Modifying the alert configuration settings in this view will automatically create the appropriate corresponding alert configurations on the Packet Design appliance to which IP Routing Manager is connected.

Note: In order to configure alerts, IP Routing Manager must be connected to an appliance and 'Topology and Managed Path Monitoring' must be set to either 'Initiated by Traps Only' or 'Traps and Scheduled Polling'.

Traps Sent to MLS

Since the IP Routing Manager product will span all SpectroSERVERs in a DSS environment, and Route Explorer will only be communicating with the MLS landscape, the MLS will forward traps sent from Route Explorer to the correct SS in a DSS environment so events and alarms are generated on the correct device models.

In CA Spectrum 9.2, you must use the Route Explorer GUI in order to configure alerts. In CA Spectrum 9.2.1, IPRM has been enhanced such that you can now configure four types of alerts (adjacency state, router state, peering state and prefix state) through OneClick.

Note: See the *Route Explorer Administrator's Guide* for assistance in configuring the traps.

Topology Change Trap Details

IP Routing Manager supports the following *Router State Change Traps*:

Router Connected

This trap is sent when a router begins participating in the routing protocol. The router may have just come up. This is a notification that a full adjacency has been established between the router and one of its neighbors.

Router Isolated

This trap is sent when a router becomes isolated from the network. The router may not actually be down, but isolated because of another outage.

Router State Flap

This trap is sent when the router's connected/isolated flap count exceeds a threshold over a given duration. CA Spectrum will include the threshold values in the event generated.

IP Routing Manager supports the following *Adjacency State Change Traps*:

Adjacency State Up

This trap is sent when a IP Subnet protocol adjacency comes up. This adjacency can be between two routers (and each one's interfaces), or between a router and a pseudo-node (this is how REX refers to a IP Subnet LAN).

Adjacency State Down

Same information as above, but the adjacency goes down.

Adjacency State Flap

This trap is sent to indicate adjacency flapping. CA Spectrum will include the threshold values in the event generated.

IP Routing Manager supports the following *Path Change Traps*:

Path Change

This trap is sent when REX detects any change in the IP Subnet path(s) between the given end points, including number of hops, path cost (metric), intermediate hops, etc. This trap does not directly result in an event or alarm being generated. CA Spectrum uses this trap as a way to detect topology/path changes, and the needed event or alarm will be generated when the topology/path changes are modeled.

IP Routing Manager supports the following *Prefix State Change Traps*:

Prefix State Up

This trap is sent when a router interface is turned on (enabled). This trap announces that the interface's prefix has come online. This trap is also sent for routes that are redistributed from another routing protocol via a router.

Prefix State Down

This trap is sent when a router goes away, and all of its prefixes are removed. A router may also remove a prefix that it is advertising (premature withdrawal).

Prefix State Flap

Same handling as for other 'flap' traps.

Path Change

You can configure each monitored path to generate an event or an alarm of a specified severity when the path changes. Changes detected include: path cost, number of ECMPs, and actual path hops traversed.

To accomplish this, select a specific Layer 3 Path model's Information Tab, and configure the relevant settings.

Important: Once a path change alarm is created for a given managed path, any subsequent changes will not result in new alarms but will instead be appended as events to the existing outstanding alarm.

Note: You can utilize the Layer 3 Path History (see page 30) feature to help debug why the path may have changed or been lost.

Path Loss

You can configure each monitored path to generate an event or an alarm of a specified severity when the path is lost. A path is determined to be 'lost' if there does not exist at least one complete forward and return path, if applicable, where both the source and destination nodes are matched with the requested source and destinations.

To accomplish this, select a specific Layer 3 Task model's Information Tab, and configure the relevant settings.

Self Monitoring

If IP Routing Manager loses the connection to REX, or there is a configuration problem with the integration, a red alarm is asserted on the IP Routing Manager model notifying the user of the situation.

Fault Tolerance Support

IP Routing Manager fully supports fault-tolerant SpectroSERVER setup. The REX Connector runs on primary and secondary landscapes, both connected to REX. Secondary landscapes periodically poll Route Explorer to verify that it is still available, but they do not detect any topology or path changes. On failover, secondary SpectroSERVER resumes normal REX communication and polling.

In order for REX traps to be handled correctly, you need to configure REX to send traps to both the primary and secondary SpectroSERVERs. Optionally, a tool like TrapExploder could be used which allows you to configure REX to send traps to a single IP address, and the TrapExploder can be configured to replicate the traps it receives to multiple recipients.

As of Spectrum 9.2.1, when a secondary SpectroSERVER becomes active it will automatically configure alerts on the Route Explorer appliance so that the desired traps are sent to the secondary SpectroSERVER. In order for this to function properly, you must perform an OnlineBackup after you have configured the alerts on the primary SpectroSERVER.

Note: If the secondary SpectroSERVER is in 'warm' or 'cold' standby mode it will not process any traps; if it is in 'hot' standby mode it will process traps.

Chapter 6: Frequently Asked Questions and Useful Tips

This section contains the following topics:

Frequently Asked Questions

Integration Overview

Question: Does the REX appliance perform the layer 3 topology discovery and CA Spectrum IPRM imports that information from REX? Or does CA Spectrum perform its own native layer 3 topology discovery?

Answer: REX performs the layer 3 topology discovery and passes this information to IPRM.

Question: Does IPRM keep track of routing changes in real-time?

Answer: IPRM Topology is updated in real time and spotlighting can be used to view up to date hop-by-hop path composition. Also, IPRM supports related alarm conditions based on the updates from the REX appliance.

Question: How long does it take to remove the disconnected router icon from the topology view?

Answer: Disconnected routers age-out of REX database slowly. The time for the disconnected routers to age out of the REX database is based on the routing protocol being used. In the case of OSPF, it is approximately one hour.

Question: Why would IPv4 prefix count shown in REX GUI differ from IP Subnet count shown by IPRM?

Answer: There could be several reasons for this:

- By default (user configurable) IPRM hides the icons representing User Subnets – IP subnets with one (gateway) or more routers and a number of end hosts and devices served. In this case these models will be completely hidden in OneClick UI (including Topology Tab, List Tab and in the Navigation Tree).
- By default (user configurable) IPRM hides the icons representing IP Subnets used solely to connect two routers. In this case the corresponding IP Subnet models will be hidden in OneClick UI.

- REX's count of prefixes is really count of routes. For example, if the same prefix is announced by two routers it counts it twice. IPRM does not create multiple IP Subnet models for the same subnet.
- In the case of distributed Route Explorer configuration, it's important to make sure IPRM is connected to the REX appliance acting as the 'Modeling Engine' and the replication is turned on to ensure it can have the complete topology picture.

Question: Does IPRM connect to REX via the REX API or directly with the database?

Answer: IPRM uses REX's XML RPC API.

Question: How secure is data transmitted between REX and IPRM?

Answer: As of CA Spectrum r9.2.1, the API password (Query Password) is transmitted encrypted.

Question: Which ports are used between the REX, IPRM Connector and SpectroSERVER?

Answer: Communication between SpectroSERVER and REX Connector uses ports 14002 and 14006 for CORBA, as well as a few dynamically-chosen ports as connection sources from the REX Connector to the Naming Service and to the SpectroSERVER.

REX Connector expects open TCP connection to port 2000 on the Route Explorer appliance.

Question: How secure is REX appliance's communication with the routers?

Answer: REX only uses read-only access and supports both RADIUS and TACACS secure access methods. It also supports MD5 authentication for OSPF and BGP peerings.

User Interface

Question: What kind of UI does REX offer?

Answer: REX UI has two components: Administration & Configuration is available via the Web and all the product features are available via X-GUI. Any standard browser (Mozilla, IE) can be used to access the Web UI while the X-GUI can be accessed either via a X-Manager or a VNC client.

X-GUI is disabled in IPRM-RR, since it is expected you will use CA Spectrum's OneClick GUI.

Question: Without GUI component, how will I be able to configure IPRM-RR traps?

Answer: As of Spectrum r9.2.1, IPRM provides configuration of path change, router state, adjacency state, prefix state, and peering state alerts via CA Spectrum's OneClick GUI.

Question: Is there a context sensitive integration between IPRM and REX GUI?

Answer: No, CA Spectrum OneClick will be the only GUI part of the solution (with the exception of web-based REX administration console used during the installation).

Routing Protocols

Question: What routing protocols does IPRM support?

Answer: REX appliance supports all routing protocols, including the following standard protocols as defined by the IETF RFCs: IS-IS, OSPF, BGP and MP-BGP as well as EIGRP (Cisco proprietary) and static routes.

IPRM will show the full routed topology as discovered by REX appliance. Initial version of IPRM in CA Spectrum r9.2.0 offered navigation-based spotlighting and icon labeling for OSPF protocol and AS groups. As a result of customer feedback, in Spectrum r9.2.1 navigation-based spotlighting was replaced by individually customizable topology maps. Users can still leverage the spotlighting dialog to highlight different routing protocol aspects in their Layer 3 topology view.

Other visualization techniques under consideration for future IPRM releases include display of EIGRP session establishment status, spotlighting for IS-IS levels, display of attributes from BGP packet headers as observed by REX, etc.

In addition to visualization techniques, protocol support includes display of routing protocol attributes. Here CA Spectrum already offers support for BGPv4 (RFC 1269), RIPv2 (RFC 1724) and OSPF (RFC 1253) SNMP MIBs.

Question: Is monitoring of BGP prefixes supported?

For example, I have configured BGP and are able to see BGP UP/DOWN alarms of most of the devices monitored by CA Spectrum. In case BGP is up on one router, but the number of BGP prefixes received from its peer is 0 (zero), the device will not have complete routing table and as result it will not route the traffic. I would like to know if CA Spectrum can generate an alarm in such case.

Answer: REX appliance can generate necessary alert and forward to IPRM which will then be able to create an alarm from this.

For loss of Peering, between REX and a router, the 'Peering State' alert can be used. For loss of prefixes, the 'BGP Prefix Flood/Drought' alert can be used.

The BGP Prefix Flood/Drought alarms rely on the baseline of BGP prefixes, which is done automatically by the IPRM Route Recorder (no user intervention necessary).

Let the recording go on for 24 hours; IPRM RR would have then established a baseline (containing prefixes expected from each BGP peer). Configure BGP prefix Flood and Drought alert with the following parameters:

a. A watch list (via a router group) containing the peers that need to be watched.

b. Configure prefix drought alert with a threshold of 100%. This will issue an alert when all baselined prefixes being heard from this peer are withdrawn.

For a greater sensitivity (i.e., cause alerts to be fired when some number of prefixes, less than 100%, are withdrawn), change the threshold parameter as required (say 90%).

Question: How can modifying my IPRM Alert Configuration Defaults affect CA Spectrum's performance?

Answer: IPRM Alert Settings *can* be used to tailor the amount of events/alarms you see in IPRM.

For example, if you are monitoring adjacencies, and a link was flapping constantly (coming up and going down), you would see 5 events for that link from each router (both ends of the adjacency) in 60 seconds. For prefix alert, you would see 5 events for that prefix being pulled in 60 seconds. Therefore, with a constantly flapping interface, you would probably see 15 events for that 60 second period, and then 15 more for the next 60 second period. With IPRM's current default settings, users could see up to 15 events/minute for a flapping link. If 'x' links are flapping, then you'd get 'x' times 15 events/minute. This may raise the concern that with a high rate of events was that these events would trigger excessive device polling. However, that is not a problem because IPRM does not poll devices as a result of these events; instead, these events trigger IPRM to re-discover the layer-3 topology so that it can determine what has changed in the topology. Additionally, IPRM leverages a 'rolling timer' to prevent topology re-discovery from happening too frequently. IPRM doesn't re-discover for every event that occurs, it will only re-discover at most once every minute as long as these events are occurring. Since the alerts are all disabled by default in IPRM, it's not until a client site makes changes to the alert configuration that they can expect to start seeing events/alarms in IPRM.

Question: Is multi-protocol BGP supported?

Answer: No, multi-protocol BGP is used for VPN services over Layer 3 and as such is outside the scope of this product.

Question: Does IPRM support route summarization boundaries for EIGRP?

Answer: To correctly model EIGRP networks, REX needs to establish an adjacency behind the summarization boundaries. So knowledge of where the summarization boundaries exist is important for the correct and complete REX configuration.

Question: Are static routes supported?

Answer: REX appliance normally doesn't poll devices, but it can optionally collect static route information (along with other data not distributed in the routing protocols such as interface names, router models, etc) via SNMP polling. This is completely configurable by the customer. The static nature of such data requires very low frequency polling (e.g. once a day or week at most). Note also that REX only polls (potentially only those selected by customers) routers, not every network device.

Question: Protocols that support some form of adjacency setup, such as OSPF or IS-IS, may be used to bootstrap a BFD session. These protocols may then use BFD (Bidirectional Forwarding Detection) to receive faster notification of failing links than would normally be possible using the protocol's own 'KeepAlive' mechanism. Does IPRM support BFD events?

Answer: BFD protocols are not supported.

Question: Is policy based routing supported?

Answer: No, the information about policy based routing is not advertised in routing protocols, the primary source of information for REX.

Question: How are routing loops supported?

Answer: Unfortunately, REX does not track routing loops. Routing loops are transient issues in the network. Most routing loops occur as protocols converge and hence are short-lived (milliseconds to seconds). For example, a routing loop may occur because of reordering of the protocol packets received by a router. REX does not (in most cases cannot) track such transient issues. REX assumes that all protocols have converged and accordingly compute the Routing Information Bases at different routers.

There could be some long lived routing loops that can be analyzed in REX. If you try to find a path and a routing loop exists along the way, REX will show that depending on the root-cause of the routing loop. However, it is virtually impossible for REX to dynamically track and alert on this condition as this would require REX to track all possible paths in the network (even for a medium size network this could mean tens of thousands of paths).

Question: Does IPRM support IPv6 addressing?

Answer: No, the first release of IPRM doesn't support IPv6 addressing. REX appliance does support this and IPRM will be extended to support this as well in one of the upcoming upgrade releases.

Managed Path

Question: Can I create managed path between routers from different OSPF areas?

Answer: Yes, you can monitor paths from one OSPF area to another. It supports paths from one AS to another.

Question: Can I create managed path between user IP subnets?

Answer: The source of the managed path has to be a router; the destination can be IP Subnet. Currently, REX restricts managed path source to routers only, however this restriction may be lifted in the future and IPRM updated accordingly.

Question: Can IPRM display path change history between any two end points?

Answer: Yes, IPRM can display path change history between any two end points.

Question: Why does the hop count for managed path differ between IPRM and REX? (This question is ONLY applicable for CA Spectrum r9.2 and REX 8.5.x.)

Answer: In REX, pseudo-nodes represent IP Subnets, in line with IS-IS and OSPF protocols modeling.

The REX GUI distinctly displays pseudo-nodes in its topology view and IPRM follows the suit representing them as IP Subnet models in its own topology view

When it comes to Layer 3 path modeling, REX continues treating pseudo-nodes as distinct hops. For example, for a path between 3 routers (A, B, and C), there will be two IP Subnets (X and Y) with one between each router. REX would consider this path to have 4 hops:

1. A -> X
2. X -> B
3. B -> Y
4. Y -> C

IPRM takes a different approach and treats pseudo-nodes as something that data simply travels through to get to the next hop. So, for the path above, IPRM shows the path having only 2 hops:

1. A -> X -> B
2. B -> Y -> C

Question: Does IPRM support routing changes simulation?

Answer: No. This capability is supported by Route Explorer's GUI which is not directly leveraged by IPRM. If you already have a full REX appliance, you will continue to be able to benefit from this capability.

Question: Does IPRM expose any other Packet Design add-on capabilities such as MPLS LDP LSPs and traffic monitoring?

Answer: No, IPRM integrates CA Spectrum with REX only at this stage.

Question: Why is the path cost value different from the sum of the metrics in the Path Hop Details table?

Answer: The path may traverse an internal router hop, for which the metric value will not be displayed in the Path Hop Details table (or the Path View tab).

IPRM Deployment

Question: What versions of REX appliance are supported?

Answer: CA Spectrum r9.2.0 IPRM supports REX firmware 7.5.56-R through 8.5.X-R. CA Spectrum r9.2.1 will support firmware version 9.3.16-R.

Note: Additional future versions of REX firmware *may* be supported by CA Spectrum IPRM r.9.2.1 based upon API compatibility.

Question: How many REX appliances will I need?

Answer: One REX appliance is sufficient (2600 unit with 8 GB of RAM). If you have multiple REX appliances, IPRM connects to the master modeling engine that aggregates all of the data from multiple REX appliances.

Question: I already have HP RAMS deployed. Can I use it with IPRM?

Answer: Yes, if you are considering moving from HP NNM to CA Spectrum, you can take advantage of any investment they have made in HP RAMS. IPRM is compatible with HP RAMS 8.11 and newer.

Question: I have a distributed Route Explorer installation, i.e. a modeling engine and one or more route recorders. The route recorder is responsible for collecting routing information, and the modeling engine provides GUI and a central database. How is CA Spectrum IPRM integrated in this case?

Answer: In this case, you should configure IPRM's REX integration settings to connect to the Modeling Engine and enable replication so that all data is copied to the Modeling Engine.

Question: What's the performance impact from adding IPRM to the SpectroSERVER?

Answer: There is no precise measurement available. A lot will depend on the amount of IPRM polling configured by the operator (for example, none vs. every 60 seconds).

Question: What is the performance impact on the network devices when REX performs discovery and monitoring?

Answer: Route Explorer operates by passively monitoring the routing protocols exchanges between routers. To do this, Route Explorer 'announces' itself as if it were a router, but doesn't advertise any prefixes, so no traffic flows to/through it (its neither a bottleneck nor a failure point).

When Route Explorer is installed, it is given an IP address and adjacencies are set up with a small number of routers (e.g. REX requires an adjacency with one router in each OSPF area or IS-IS level). If the router is local, this can be a physical connection. Otherwise, REX can connect to remote routers either via GRE tunnels or VLANs. Once these adjacencies are up, REX begins monitoring the protocols and is able to present a complete, network-wide map within minutes.

The only messages Route Explorer sends out to its neighbors are periodic 'KeepAlive' messages to maintain these adjacencies. Thus, there is virtually zero load placed on the real routers or the network, both during discovery and ongoing monitoring.

Question: How does REX establish routing adjacency with remote autonomous systems?

Answer: In these cases GRE tunnels or VLANs can be configured to establish secure links to remotely located routers.

In cases where the network policy, architecture or devices don't allow or support this, you can deploy multiple REX appliances (Route Recorders) at the appropriate places in the network to establish direct adjacencies/peerings with the routers. In this distributed architecture, routing information collected by multiple Route Recorders is combined into a single topology view at the 'master' REX appliance (Modeling Engine). IPRM accesses the Modeling Engine to get the complete topology view of the network.

Question: Does REX appliance always work in passive mode?

Answer: In the majority of cases routing topology and management information is obtained from listening to routing protocol exchanges. However one routing protocol works in a different way from others – Cisco EIGRP. In this case only the change in distance to a given subnet can be determined. Based on this information alone REX uses its sophisticated algorithms to work out the routing topology and path state changes, and then uses some non-privileged CLI commands (and screen scraping) to validate its calculations.

Optionally, REX also uses SNMP or CLI commands to collect information about Static routes; since static routes don't change frequently, SNMP polling is done at very low frequency (typically, once a day; this is configurable).

Question: How does REX achieve scalability?

Answer: Packet Design have done quite a bit of scalability testing, both in-house and based on real world usage by their customers, and they can provide more details. That said, in 99%+ of the cases, a single appliance will be more than adequate. The reason Packet Design is so confident is due to the fact that under recommended deployment conditions REX will not have any users (i.e. GUI sessions).

The limitation for scalability has to do with memory since REX requires a separate copy of the topology model for each user session (as well as another copy for monitoring/alerting). Large networks (# of routes and routers) can require very large models, and therefore take up a significant amount of memory. But without the need to support any direct users, Packet Design believes they have not seen a network that would not easily fit within a single appliance. And they have production deployments at some of the largest routed networks in the world. To put some parameters around that, Packet Design is already supporting networks comprised of over 7,000 routers and more than 8 million routes with a single box.

Note: Only routers are counted as nodes, whereas the number of devices monitored by a large CA Spectrum deployment includes many non-routing devices.

Question: Does REX support NAT'ed environment?

Answer: No, REX does not support this environment type.

Question: Does IPRM support subnets configured with overlapping IP addresses?

Answer: Route Explorer and CA Spectrum take different approaches to supporting this network configuration, and as such the initial release of IPRM does not support it. However, in future IPRM may be extended to support this deployment scenario.

Question: Does IPRM support fault tolerant CA Spectrum deployment?

Answer: Yes, secondary SpectroSERVER will take over communication with REX in case of failover, and pass control back to primary when it goes back online.

Question: Does REX support fault tolerant deployment?

Answer: Yes, primary REX appliance can be configured with secondary 'warm' standby REX appliance. In case of primary REX failure the switchover will have to be done manually, but the secondary REX will have complete routing history from prior to the switchover event.

Question: Does IPRM support distributed CA Spectrum deployment?

Answer: Yes, all user configuration and interaction is performed on the main location server (MLS).

Useful Tips

The following presents useful tips for CA Spectrum's IP Routing Manager for the CA Spectrum r9.2.1 release:

- REX Connector should run on separate CPU from SpectroSERVER if possible to reduce impact on SpectroSERVER. This is because when Layer 3 discovery is performed, the REX Connector causes additional CPU usage. This is primarily applicable to Windows, which can be adjusted by using Task Manager's 'Set Affinity' option. UNIX/Linux applications handle the load balancing better.
- You must disconnect from REX to change REX configuration settings (for example, REX administrative domain), and then re-connect for the changes to take effect.
- When using Monitoring Mode = 'Off', you must manually configure topology and path-related change notifications (traps) within REX GUI beforehand.
- Disconnected routers age-out of REX database slowly. The time for the disconnected routers to age out of the REX database is based on the routing protocol being used. In the case of OSPF, it is approximately one hour.
- Use 'Clear Layer 3 Topology' button to start over. This deletes all IPRM modeling in MLS, including subnets, paths, and UnmanagedDevice models.
- An AutonomousSystem in IPRM is equivalent to an 'Administrative Domain' in REX.
- Source and destination of Layer 3 paths must be within REX's visibility.
- When tracing a path to a router loopback IP, the last internal hop is used in cost calculation and number of hops, but not included in path hop details nor topology view. This last internal hop is not represented visually in topology view.
- In OneClick, the 'View Layer 3 Path Change History', 'Create Layer 3 Path' and 'Select as Layer 3 Path Source' menu items may be disabled in the Tools, Utilities menu. These items are enabled/disabled based on what is currently selected in the Explorer tab.

  For example, if you select a router model under the 'Layer 3 Devices' container in the Explorer tab, all three of these menu items will be enabled under Tools, Utilities.

Chapter 7: IP Routing Manager Troubleshooting

This section contains the following topics:

Known Anomalies

CA Spectrum's IP Routing Manager for the CA Spectrum r9.2.1 GA release contains the following known anomalies:

- Modeling your Packet Design appliance in CA Spectrum will prevent IPRM-related traps and alarms from working properly.
- LANs/subnets cannot be used as the source for IP Subnet paths. This is a limitation of Route Explorer. In some cases, multiple routers route to the same subnet so REX is unable to determine the source router for the path.

  Therefore, IPRM cannot discover forward-and-return paths when a LAN/subnet is used as the path destination.
- Some interface information may appear 'missing' from the Path Hop Details table. In some cases, particularly with IS-IS, REX cannot determine the interface IP address for a hop in the path.
- Paths that have an internal router as the final path hop do not show this hop in the Path Hop Details table or in the path topology view. An internal router hop cannot be visualized in the topology and is therefore omitted from the topology view and the Path Hop Details table, but the cost of the internal hop is included in the path's total cost calculation.
- IPv6 is not supported.
- Overlapping IP address and AS ranges are not supported.
- If IP Routing Manager is connected to a Packet Design appliance that is running version 9.2 or greater of the Packet Design/Route Explorer software, the Path Change History's 'Link Prefix' column may be missing values.

- **Problem:**

  If a particular IP address is configured on the interface of more than one router and these routers are modeled in CA Spectrum, but at least one of the routers is modeled as a Pingable; IP Routing Manager may create links to the wrong model. In particular, there may be a link connecting one router model to another when that link should instead be connecting the Pingable model (which represents a different router) to another router model. A side-effect of this issue is a broken Layer 3 path view, where the path through the network is contiguous from source to destination, but the IP Routing Manager topology view displays a disjointed view of the path.

  Solution:

  Replacing the Pingable model with a model of a more appropriate, SNMP-managed model type (for example, Rtr_Cisco) and then re-discovering the Layer 3 topology in IP Routing Manager can resolve the issue.

IP Routing Manager Traceability Events

IP Routing Manager creates CA Spectrum events when any of the following occurs in IPRM so that users have visibility into what led to the current state of the IPRM. All events will be generated on the IP Routing Manager model.

DISCOVER_BUTTON_PRESSED_EVENT (0x564001e)

This event will be generated whenever the user presses the Discover button in OneClick. The name of the user will be included in the event.

CLEAR_BUTTON_PRESSED_EVENT (0x564001f)

This event will be generated whenever the user presses the Clear button in OneClick. The name of the user will be included in the event.

CONNECT_TO_REX_BUTTON_PRESSED_EVENT (0x5640020)

This event will be generated whenever the user presses the Connect button in OneClick. The name of the user will be included in the event.

DISCONNECT_FROM_REX_BUTTON_PRESSED_EVENT (0x5640021)

This event will be generated whenever the user presses the Disconnect button in OneClick. The name of the user will be included in the event.

REX_HOSTNAME_CHANGED_EVENT (0x5640022)

REX_QUERY_PASSWORD_CHANGED_EVENT (0x5640023)

REX_ADMINISTRATIVE_DOMAIN_NAME_CHANGED_EVENT (0x5640024)

REX_HEARTBEAT_INTERVAL_CHANGED_EVENT (0x5640025)

The above events will be generated whenever the user changes one of the corresponding REX Configuration values OneClick. The name of the user will be included in the event.

TRAP_BASED_TOPOLOGY_POLL_EVENT (0x5640026)

This event will be generated whenever IPRM performs a Layer 3 topology poll based on receiving a trap from REX.

STARTUP_BASED_TOPOLOGY_UPDATE_EVENT (0x5640027)

This event will be generated whenever IPRM performs a Layer 3 topology update when the SpectroSERVER is restarted, or when regaining contact with REX after a communication problem.

MON_MODE_CHANGE_BASED_TOPO_UPDATE_EVENT (0x5640028)

This event will be generated whenever IPRM performs a Layer 3 topology update based on changes to the Topology Monitoring Mode in OneClick.

IF_RECONFIG_BASED_TOPOLOGY_UPDATE_EVENT (0x5640029)

This event will be generated whenever IPRM performs a Layer 3 topology update based on CA Spectrum router model interface reconfigurations. This is done to keep the Layer 3 topology in sync with CA Spectrum device modeling.

TOPOLOGY_UPDATED_EVENT (0x564002a)

This event will be generated whenever a Layer 3 topology update has been completed. Situations in which this is done outside of other events include topology changes detected by the REX Connector in Active mode.

TOPOLOGY_MONITORING_MODE_CHANGE_EVENT (0x564002b)

This event will be generated whenever the user changes the Topology Monitoring Mode in OneClick. The name of the user will be included in the event.

TOPOLOGY_POLLING_INTERVAL_CHANGE_EVENT (0x564002c)

This event will be generated whenever the user changes the Topology Polling Interval in OneClick. The name of the user will be included in the event.

IP Routing Manager Debugging

You have the ability to turn on debugging output for IPRM intelligence running inside the SpectroSERVER. An attribute called DebugLogEnabled exists on the IP Routing Manager model which controls the generation of log files. You can access it via the Attribute Tab of the IP Routing Manager model's Component Details panel.

Upon SpectroSERVER startup, it checks to see if DebugLogEnabled is TRUE. If so, then it opens a new log file in the IPRM/logs/debug directory and begins outputting data when necessary. When you set DebugLogEnabled to FALSE, the log file is closed. When you set DebugLogEnabled back to TRUE, a new log file is created. After that, every night at midnight, the current log file is closed and a new one is opened. The log file names are of the form 'Layer3ModelingDebugLog.<datetime>'.

All Layer 3 topology and path modeling functionality will output modeling details to the debug log. This includes manually-triggered discoveries, discoveries triggered by changes detected, path creation requests, etc. The modeling details we output include data on each router and subnet that exists in the Layer 3 topology, links that were created or removed, UnmanagedDevice models created, attribute value updates, path creation details including hop details, path change information, and so on.

All debug output is time-stamped so the user can easily cross-reference it with debug output generated by the REX Connector.

Steps to Take if the REX Connector Is Not Running

Steps to Take if the REX Connector Is Not Running

1. Check the following files for errors:
   `$SPECROOT/IPRM/REX/REXCON.OUT`
   `$SPECROOT/lib/SDPM/processd_log for errors`
2. Use CA Spectrum CLI to manually start the REX Connector:
   `update  action=0x5640002 mh=<mh_of_IPRM>`

Steps to Take if Unable to Connect to Route Explorer

Steps to Take if Unable to Connect to Route Explorer

- The password encryption for API requests may be broken if the Query Password had been set and then a Route Explorer software update had been performed. To alleviate this problem, set the Query Password on each of the Packet Design appliances (via the REX web interface) to a temporary value, save the changes, and then set the Query Password back to the original password and save the changes.
- Verify that 'Queries' are enabled in REX.
- Login to REX web interface and go to Application, 'Administration -> Application -> Queries'.
- Ensure the following are enabled 'XML-RPC Query Server' and 'Enable remote access'.
- Set the password to the same value entered in the IPRM configuration.
- Ensure REX Connector is able to access tcp port 2000 on Route Explorer system.

REX Connector Debug Logging

To Set REX Connector Debug Logging

1. Edit IPRM/REX/config.xml file.

   Note: The REX Connector checks config.xml for changes every 30 seconds, there is no need to restart the connector.

2. Set the <debugging> tag to one or more of these values (comma-separated, case insensitive):

   Off

   No output at all.

   Trace

   Minimal REX Connector startup, shutdown, administrative tasks.

   Comm

   Includes basic information about communication with REX.

   Debug

   Includes useful, human-readable topology and path data that REX provides. Technical Support can use this to cross-reference with modeling debug provided by the SpectroSERVER.

   Max

   Includes raw XML from REX API requests and responses.

   Output is written to:
   `IPRM/REX/logs/debug/debug.log.<timestamp>`

REX Connector Debug Client

A command line utility 'rexcli' simulates SpectroSERVER-based requests to the REX Connector. The 'rexcli' utility provides a picture of the topology or a path at a specified date/time.

To Edit the 'rexcli' Utility

1. Navigate to IPRM/REX and edit 'rexcli' utility.
2. Specify the following supported parameters (if needed):

   -topo <date>

   Retrieves the topology at the given time.

-path <srcIP> <dstPrefix> [forward_and_return] <date>

Retrieves the path at the given time.

- The 'dstPrefix' is specified in 'slash notation'
  (for example, 10.253.5.2/32 for a router destination).
- The 'forward_and_return' (optional) retrieves both the forward and return paths
  (when possible).
- The 'date' is the date/time for which you want to retrieve the IP Subnet topology or path, and is specified as: 2011/07/31T14:56:42; which represents: July 31, 2011 2:56:42 pm.

The output is written to the shell; you can redirect to a file.

By enabling debugging in the REX Connector's config.xml file, you can correlate the output from 'rexcli' utility with the debug output from the REX Connector.

Initiating Layer 3 Topology Discovery Using an Offline Database

The REX Connector can also use 'offline' Route Explorer databases. 'Offline' Route Explorer databases are generally historical databases which have been archived on the Route Explorer unit. This feature allows IPRM to discover the Layer 3 topology stored in an offline database; this is useful for testing different types of networks and for customer support.

An additional XML configuration option can be added to the REX Connector's config.xml file. The additional option is a boolean named 'allow_offline_dbs'. When this option is set to 'true', users may configure the REX integration (via OneClick) to use an offline database.

To initiate Layer 3 topology discovery using an offline database

1. Navigate to the Component Details Panel of the IP Routing Manager model and open the Configuration sub-view.
2. Clear any existing Layer 3 topology data using the Clear button.
3. Set REX Connector options in IPRM/REX/config.xml.
4. Add <use_offline_dbs>TRUE</use_offline_dbs> to file to access offline databases.
5. Press the Discover button in the IP Routing Manager model's Configuration sub-view.

Index