



Best Practices for Eliminating Risk from Routing Changes



TECHNICAL BRIEF

Table of Contents

Introduction	3
Route Analytics—Intelligence to Meet the Routing Management Challenge	3
Routing Management Best Practices Empowered by Route Explorer	4
Adding a New IGP Route or Routes	5
Pre-Implementation Work	5
Installation Plan Definition	5
Back-Out Plan Definition	5
Approval Process	5
Perform Maintenance	5
How Route Explorer Helps in Adding IGP Routes	6
Upgrading an Existing Router	9
Pre-Implementation Work	10
Installation Plan Definition	10
Back Out Plan Definition	10
Approval Process	10
How Route Explorer Helps in Upgrading Routers	11
Changing BGP Routing Policy Configurations	13
Pre-Implementation Work	13
Installation plan	14
Back out plan	14
Approval process	14
Perform Maintenance	14
How Route Explorer Helps Implement BGP Routing Policy Changes	15
Conclusion	16



Introduction

IP routing is one of network management's most complex domains. And no wonder. Not only are routing protocols highly automated and distributed in nature, but routing errors can have a large-scale, sometimes calamitous, impact on quality and availability across the entire network.

Network engineers performing routine routing management tasks are at a significant disadvantage today because they lack both the global visibility to understand distributed routing dynamics, and the automation to quickly gather and interpret dynamically changing routing state. Without these capabilities, they often find themselves working with inaccurate information when planning and executing changes in the network, leading to costly and time-consuming errors; lower confidence in executing, validating and documenting network changes; and ultimately slower responsiveness to customer requirements. Analyst and academic studies bear this out, noting that routing misconfigurations contribute significantly to network downtime, as well as application and VoIP quality and availability problems, even in carrier-class IP networks with highly disciplined network engineering processes and practices.

Route Explorer is the industry's leading route analytics solution, and provides the first platform for empowering accurate and timely routing management best practices. Deployed by dozens of the largest enterprises, service providers, government and military agencies and educational institutions, Route Explorer offers unprecedented network-wide routing visibility, re-playable routing history, automated analysis, and change modeling capabilities that, integrated into network engineering practices, enable IT departments to deliver greater accuracy, confidence, responsiveness and service quality.

This technical note reviews the challenges of current routing management practices and their implications for IT performance, introduces Route Explorer's routing management capabilities, then provides three detailed examples of how Route Explorer can uniquely empower routing operations best practices.

Route Analytics—Intelligence to Meet the Routing Management Challenge

Before the advent of route analytics technology, the primary tools available to support planning and execution of routing engineering changes were primitive at best. Network engineers used manual snapshots of routing information (such as the output of router CLI "show" commands) from a small set of routers to establish an understanding of the state of routing for planning purposes. Ping, traceroute and other localized CLI commands were the main tools for "real-time" testing of routing state before, during and after execution of routing changes.

Given the lack of capable tools, network engineers have had to exercise a great deal of expertise and insight to ensure accurate changes. Nonetheless, due to lack of actionable routing intelligence, many more errors occur than are ideal. This low accuracy in change operations leads to a lack of confidence and speed in responding to technical or customer requirements, and increases the risk of network disruptions. It



Best Practices for Eliminating Risk from Routing Changes

also locks network engineering into a reactive and fire-fighting stance, rather than a proactive stance that rapidly moves at the speed of emerging business needs.

Route analytics technology introduced network engineers to a ground-breaking combination of real-time and historical network-wide routing visibility and powerful analysis tools. Route Explorer, the industry's leading route analytics solution, records all routing protocol updates and creates an interactive, true-to-life model of the routing topology that is as accurate as the actual network. Route Explorer continuously records the ongoing as-running state of the network, so that the historical state of the network can be "replayed" with full granularity. Using this live model, Route Explorer provides a broad array of analysis tools including interactive network-wide routing topology views, detailed and filterable tabular data on all aspects of routing state, and animations of streams of routing changes over selected timeframes.

Because Route Explorer provides global visibility and complete granularity on routing state, network engineers for the first time can plan and execute routing operations with a high degree of confidence and accuracy. And because documentation of routing state is automatic and continuous – providing a built-in audit trail of operational changes from the point of the network – the system supports not only best practices but also compliance with any regulatory requirements for documented IT control processes, such as Sarbanes-Oxley section 404.

Routing Management Best Practices Empowered by Route Explorer

Best practices for performing routing change operations during a maintenance outage dictate following a standard plan:

- Pre-maintenance work
- Installation plan
- Back out plan
- Approval process
- Perform Maintenance
 - Test changes
 - If tests successful, then end maintenance.
 - If tests fail, either correct issues or back out of maintenance.
- Confirm that only the changes required of the maintenance happened.

The three examples of best-practice processes for routing change operations below show how Route Explorer can specifically aid in increasing network engineering accuracy and confidence, leading to higher success rates and greater customer satisfaction. The first two examples are for Interior Gateway Protocol (IGP) change operations, such as on OSPF, IS-IS, or EIGRP, while the third example focuses on BGP change operations.



Adding a New IGP Route or Routes

When adding new IGP routes, the following best practice steps are recommended:

Pre-Implementation Work

1. Assign the prefix to the project
2. Determine the date for application to the network
3. Verify that the prefix does not exist in the routed infrastructure (unless it is a backup route)
4. If this is a backup route, then confirm if this is primary, secondary, or equal cost path
5. Assign the correct metric to route if different than default
6. Determine if the summary block assigned is summarized for the area or region
7. Determine if the summary block needs a summary statement and where it is needed
8. Note which routers will be affected by the route addition
9. Confirm that no other maintenance is needed on this router in conjunction with this addition (such as upgrade to new version of code, or addition of hardware for this interface or other future additions.)

Installation Plan Definition

1. Verify that the correct router is being changed
2. Re-check that the prefix has not been used in the routed infrastructure
3. Add the prefix as primary or secondary to interface or add static.
4. Add the network statement to the IGP process
5. Confirm that the prefix is active and in the correct format (i.e., prefix and mask are correct)

Back-Out Plan Definition

1. If the prefix exists on another router, either attempt to get another prefix assigned and replace the current prefix with the new prefix, or abort the maintenance until a suitable prefix can be assigned.
2. If the prefix will not come up in IGP, then assure that all the maintenance steps have been completed. Look at routing tables for advertisements. Remove the new interface configuration, or document the change and shut the interface down. Remove static routes if applicable.

Approval Process

1. Obtain approval through the local process for the maintenance with the above plan specifications

Perform Maintenance

1. Notify the Network Operations Center (if applicable) that maintenance is beginning
2. Work through the maintenance procedure to conclusion



Best Practices for Eliminating Risk from Routing Changes

3. Test all new prefixes to confirm that they are advertised correctly
 - d. If not, then troubleshoot
 - e. If it cannot be fixed, back out
4. If everything checks out correctly, then close the maintenance with NOC

How Route Explorer Helps in Adding IGP Routes

Route Explorer has full knowledge of all routed prefixes, metrics and netmasks, and provides a network-wide prefix list (see Figure 1) that shows all routes that are active in the network, providing 100% assurance that the prefix and mask do not already exist in the current infrastructure.

Prefix	Router/Net	Attributes	State	Area or AS
216.169.105.0/24	128.32.1.3	AS Path: 11423 209 4200 13680 (IGP) Local-Pref: 80 MED: 5 Communities: 209:888 209:889 11423:65350 11423:65352 Next Hop: 128.32.0.66	Up	UCBJul03a.BGP/AS25
216.169.105.0/24	128.32.1.200	AS Path: 11423 209 4200 13680 (IGP) Local-Pref: 70 MED: 10 Communities: 209:888 209:889 11423:65350 11423:65352 Next Hop: 128.32.0.90	Up	UCBJul03a.BGP/AS25
0.0.0.0/0	128.32.1.221	AS Path: (INCOMPLETE) Local-Pref: 100 MED: 101 Next Hop: 128.32.0.249	Up	UCBJul03a.BGP/AS25
0.0.0.0/0	128.32.1.222	AS Path: (INCOMPLETE) Local-Pref: 100 MED: 101 Next Hop: 128.32.0.249	Up	UCBJul03a.BGP/AS25
0.0.0.0/0	128.32.1.3	Metric: 1 (AS Ext.Comparable)	Up	UCBJul03a.OSPF/169.229.128.128
0.0.0.0/0	128.32.1.3	Metric: 1 (AS Ext.Comparable)	Up	UCBJul03a.OSPF/169.229.128.168
0.0.0.0/0	128.32.1.3	Metric: 1 (AS Ext.Comparable)	Up	UCBJul03a.OSPF/169.229.128.176
0.0.0.0/0	128.32.1.3	Metric: 1 (AS Ext.Comparable)	Up	UCBJul03a.OSPF/Backbone
211.63.96.0/19	128.32.1.3	AS Path: 11423 209 701 9848 9697 (INCOMPLETE) Local-Pref: 80 MED: 5 Communities: 209:888 11423:65350 11423:65352 Next Hop: 128.32.0.66	Up	UCBJul03a.BGP/AS25
211.63.96.0/19	128.32.1.200	AS Path: 11423 209 701 9848 9697 (INCOMPLETE) Local-Pref: 70 MED: 10 Communities: 209:888 11423:65350 11423:65352 Next Hop: 128.32.0.90	Up	UCBJul03a.BGP/AS25
203.116.83.0/24	128.32.1.3	AS Path: 11423 209 4637 4657 (IGP) Local-Pref: 80 MED: 5 Communities: 209:888 11423:65350 11423:65352 Next Hop: 128.32.0.66	Up	UCBJul03a.BGP/AS25
203.116.83.0/24	128.32.1.200	AS Path: 11423 209 4637 4657 (IGP) Local-Pref: 70 MED: 10 Communities: 209:888 11423:65350 11423:65352 Next Hop: 128.32.0.90	Up	UCBJul03a.BGP/AS25
207.13.89.0/24	128.32.1.3	AS Path: 11423 209 701 10916 (IGP) Local-Pref: 80 MED: 5 Communities: 209:888 11423:65350 11423:65352 Next Hop: 128.32.0.66	Up	UCBJul03a.BGP/AS25
207.13.89.0/24	128.32.1.200	AS Path: 11423 209 701 10916 (IGP)	Up	UCBJul03a.BGP/AS25

126351 top level entries, 364294 total entries

Start Route Explorer: UCBJul03a List of Prefixes: UCBJul03a Reload Close

Figure 1: Network-wide prefix list aids in ensuring that a proposed added route doesn't already exist in the network.

Using the same prefix view, network engineers can also confirm the summary block that holds this prefix and where it is advertised from. This will ensure the summary will be advertised correctly.

Before the maintenance, network engineers can utilize Route Explorer to confirm that the router and region that is to be changed is not experiencing significant churn, by viewing the router and region's routing event streams. Route Explorer provides a per-router and per-area view of routing activity. For example, engineers can click on a particular router (Figure 2) to launch the events list (Figure 3) and view the level of activity on the router. If there is significant churn, the network engineer can then work with the respon-



Best Practices for Eliminating Risk from Routing Changes

sible person on call to see if these events can be remedied to return the router and region to a quiescent state. This is important, since starting maintenance while other problems are occurring in a region can impact diagnostic efforts for another engineer who might be working in the region. In addition, this avoids the change operation becoming the unwitting scapegoat for problems that were already occurring before the maintenance.

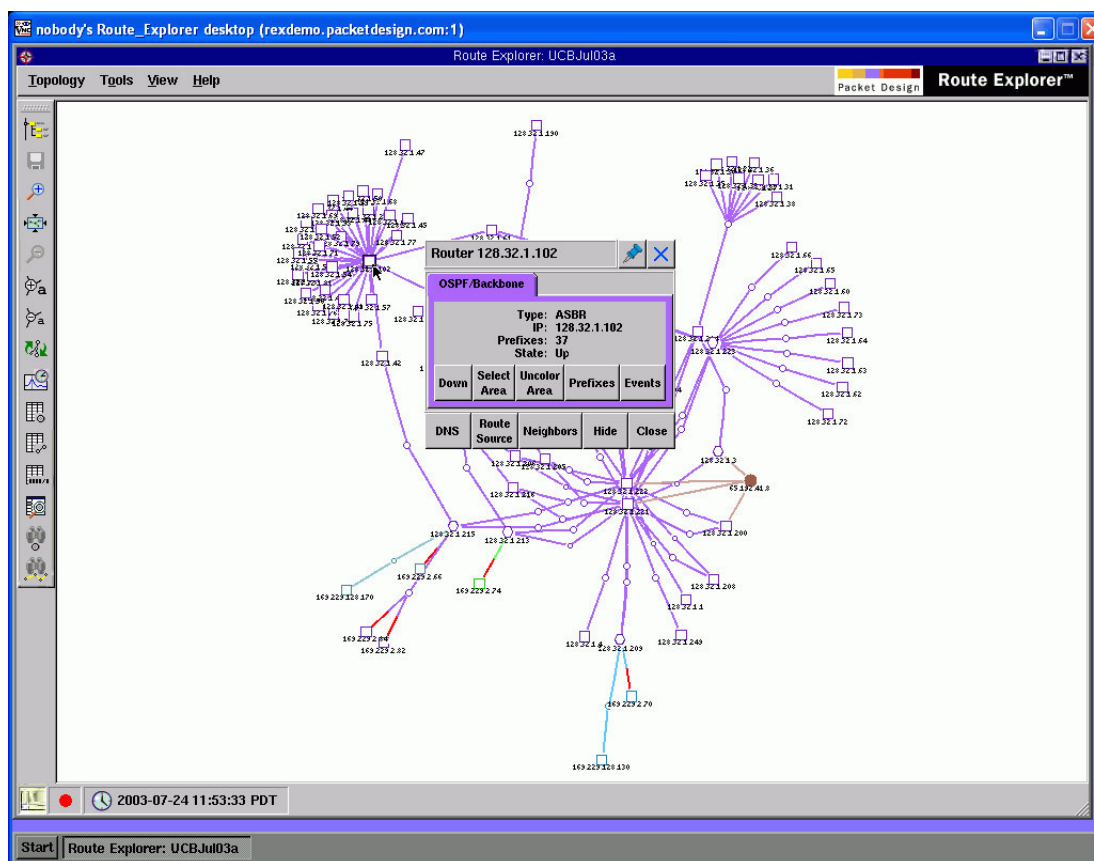
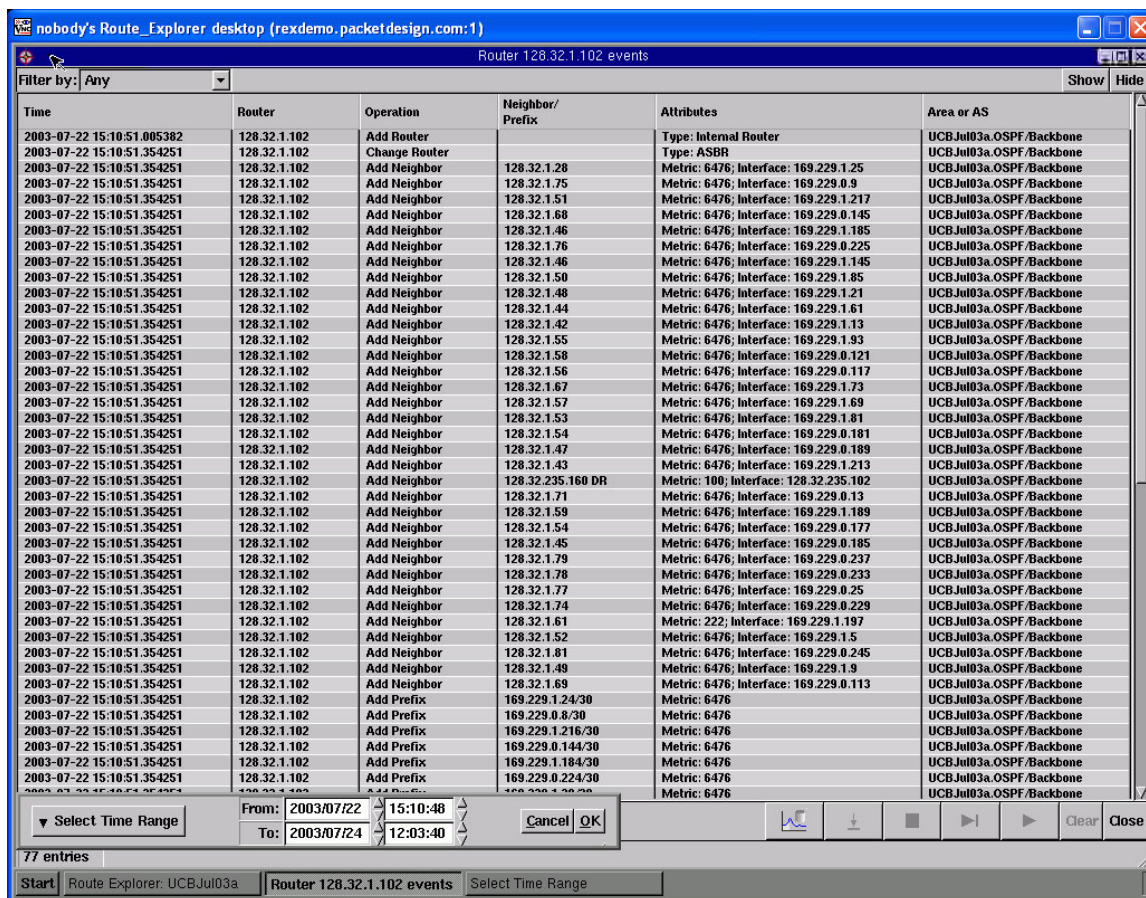


Figure 2: The topology view of Route Explorer provides the actual state of routing at any point in recorded time, and offers full interactivity—including the ability to drill down by clicking on a router and seeing its prefixes, events, and neighbors.



Best Practices for Eliminating Risk from Routing Changes



Time	Router	Operation	Neighbor/Prefix	Attributes	Area or AS
2003-07-22 15:10:51.005382	128.32.1.102	Add Router		Type: Internal Router	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Change Router		Type: ASBR	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Add Neighbor	128.32.1.28	Metric: 6476; Interface: 169.229.1.25	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Add Neighbor	128.32.1.75	Metric: 6476; Interface: 169.229.0.9	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Add Neighbor	128.32.1.51	Metric: 6476; Interface: 169.229.1.217	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Add Neighbor	128.32.1.68	Metric: 6476; Interface: 169.229.0.145	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Add Neighbor	128.32.1.46	Metric: 6476; Interface: 169.229.1.185	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Add Neighbor	128.32.1.76	Metric: 6476; Interface: 169.229.0.225	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Add Neighbor	128.32.1.46	Metric: 6476; Interface: 169.229.1.145	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Add Neighbor	128.32.1.50	Metric: 6476; Interface: 169.229.1.85	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Add Neighbor	128.32.1.48	Metric: 6476; Interface: 169.229.1.21	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Add Neighbor	128.32.1.44	Metric: 6476; Interface: 169.229.1.61	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Add Neighbor	128.32.1.42	Metric: 6476; Interface: 169.229.1.13	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Add Neighbor	128.32.1.55	Metric: 6476; Interface: 169.229.1.93	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Add Neighbor	128.32.1.58	Metric: 6476; Interface: 169.229.0.121	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Add Neighbor	128.32.1.56	Metric: 6476; Interface: 169.229.0.117	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Add Neighbor	128.32.1.67	Metric: 6476; Interface: 169.229.1.73	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Add Neighbor	128.32.1.57	Metric: 6476; Interface: 169.229.1.69	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Add Neighbor	128.32.1.53	Metric: 6476; Interface: 169.229.1.81	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Add Neighbor	128.32.1.54	Metric: 6476; Interface: 169.229.0.181	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Add Neighbor	128.32.1.47	Metric: 6476; Interface: 169.229.0.189	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Add Neighbor	128.32.1.43	Metric: 6476; Interface: 169.229.1.213	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Add Neighbor	128.32.235.160 DR	Metric: 100; Interface: 128.32.235.102	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Add Neighbor	128.32.1.71	Metric: 6476; Interface: 169.229.0.13	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Add Neighbor	128.32.1.59	Metric: 6476; Interface: 169.229.1.189	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Add Neighbor	128.32.1.54	Metric: 6476; Interface: 169.229.0.177	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Add Neighbor	128.32.1.45	Metric: 6476; Interface: 169.229.0.185	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Add Neighbor	128.32.1.79	Metric: 6476; Interface: 169.229.0.237	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Add Neighbor	128.32.1.78	Metric: 6476; Interface: 169.229.0.233	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Add Neighbor	128.32.1.77	Metric: 6476; Interface: 169.229.0.25	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Add Neighbor	128.32.1.74	Metric: 6476; Interface: 169.229.0.229	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Add Neighbor	128.32.1.61	Metric: 222; Interface: 169.229.1.197	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Add Neighbor	128.32.1.52	Metric: 6476; Interface: 169.229.1.5	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Add Neighbor	128.32.1.81	Metric: 6476; Interface: 169.229.0.245	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Add Neighbor	128.32.1.49	Metric: 6476; Interface: 169.229.1.9	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Add Neighbor	128.32.1.69	Metric: 6476; Interface: 169.229.0.113	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Add Prefix	169.229.1.24/30	Metric: 6476	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Add Prefix	169.229.0.8/30	Metric: 6476	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Add Prefix	169.229.1.216/30	Metric: 6476	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Add Prefix	169.229.0.144/30	Metric: 6476	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Add Prefix	169.229.1.184/30	Metric: 6476	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Add Prefix	169.229.0.224/30	Metric: 6476	UCBJul03a OSPF/Backbone
2003-07-22 15:10:51.354251	128.32.1.102	Add Prefix	169.229.1.28/30	Metric: 6476	UCBJul03a OSPF/Backbone

Figure 3: Events view for an individual router, over a specified period of time.

When the route is added to the protocol on the router, the same events view can be used to verify that the router has propagated the change. In addition, Route Explorer can be utilized to increase the accuracy of the change operation by executing the following steps:

- Examine prefix lists from within the area or level, and from outside to see if the summary is working correctly
- Verify from which router the route is originated, where it is summarized, what netmask and metric is associated with it and how traffic from other parts of the network will use the route to get data across the network.

If the route is not behaving in the network, Route Explorer can be utilized to model metric changes to route traffic correctly. The network engineer highlights a routed path across the network in the topology view, then clicks on the relevant link, adjusts the metric, and finally observes how the path changes. Figure 4 shows an example of highlighting a path and changing a metric in an EIGRP network.



Best Practices for Eliminating Risk from Routing Changes

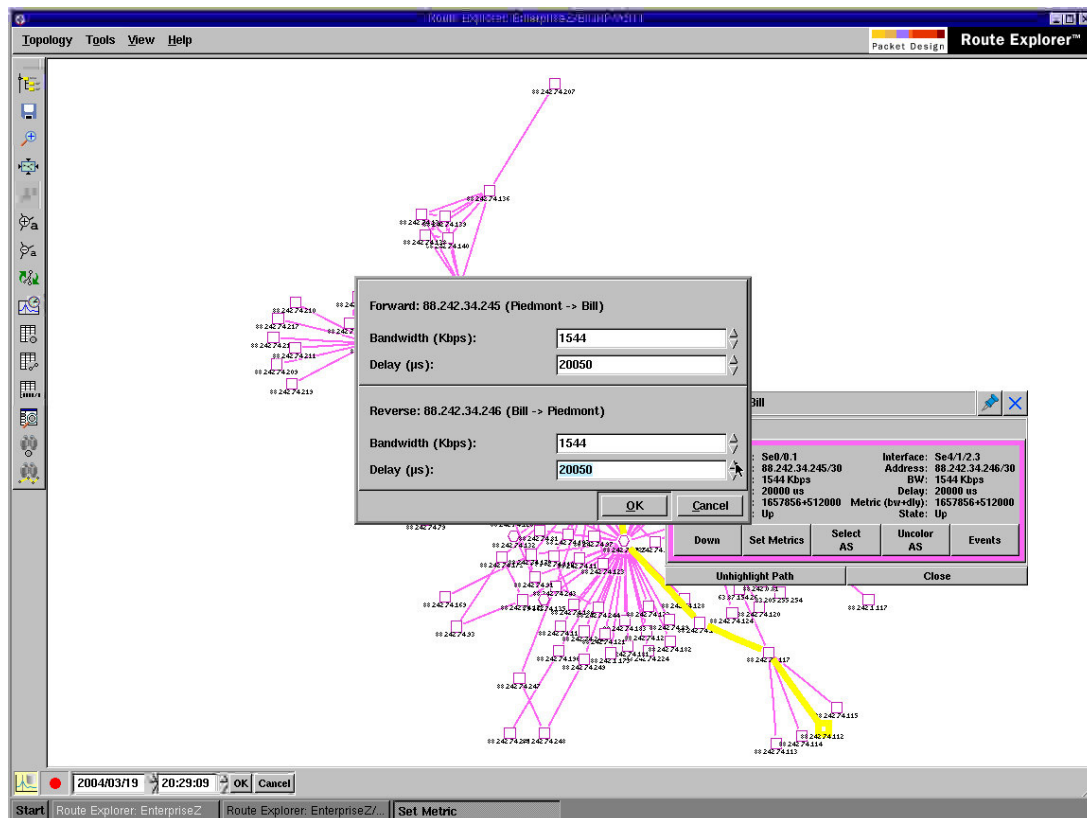


Figure 4: Modeling metric changes in Route Explorer is as easy as selecting a path (shown highlighted in yellow above), clicking on a path and typing in new metrics. Once the metrics are changed, Route Explorer displays precisely how the routed path will change as a result.

Upgrading an Existing Router

There are several reasons to upgrade a router: more ports, more CPU/memory, or more bandwidth on line cards or the backplane. In general, when an existing router is being replaced with a more powerful one, it is recommended to first upgrade the existing routing state, without yet making major changes to the configuration of the router. Then, once all current routing functions are verified as working correctly, it is safe to begin making routing configuration changes. The stability time needed to verify proper function of the configuration in the upgraded router can be as short as a half hour or as long as several days, depending on the organization's level of experience with the router vendor's equipment and the stability of the infrastructure being replaced.

There are two methods for installing a new router: swapping out and replacing the equipment in place, or putting new hardware in place and having it run in parallel with the existing hardware until it is certain that the new hardware is working properly. This example models best practices for the first case; the second can be treated as a subset of the first, with similar but different interface addresses.



Best Practices for Eliminating Risk from Routing Changes

Recommended best practice steps include the following:

Pre-Implementation Work

1. Burn in the physical equipment based on company policy.
2. List all active routes and peerings on the router, and the bandwidth associated with each. Make sure that any non-standard metrics are known, and note any comments in the configuration to allow for exact re-creation of the router configuration.
3. If routes do not seem correct or do not seem to flow data correctly, confirm that this is the desired flow. If not, comment for correction (preferably at a later date rather than in this maintenance).
4. Confirm that every interface on the existing router has a corresponding interface of at least equal bandwidth on the new router.
5. Create a configuration that will transition the existing capabilities to the new router.
6. Label each wire with the current and the future port to connect to. This will speed transition and aid if the maintenance meets trouble and has to be backed out.

Installation Plan Definition

1. There are two parts: loading the configuration (which can be done beforehand) and wiring the new router.
2. Confirm that no new prefixes are being advertised by this router and that no new adjacencies have been added. If necessary, modify the new router configuration to take these into account before starting the maintenance.
3. If there are not enough ports on the new router for any changes, stop maintenance until this can be corrected.
4. Make all ports passive to stop routing and remove the adjacencies with all routers. Also, make sure that either out-of-band connectivity or telnet access from an adjacent router is available.
5. With the pre-work of marking all the wires accomplished, moving them should only take a few minutes. However, if a longer cable is needed for a port, label it to assist in the back out plan if needed.
6. The router can have the configuration installed before the maintenance starts and then can be powered on and wired during the maintenance.

Back Out Plan Definition

1. Labeled cables are moved back to original router ports.
2. Passive interface statements are removed from the interfaces to form active adjacencies.

Approval Process

1. With the detail above and any company-specific information that is needed, obtain approval for the maintenance.



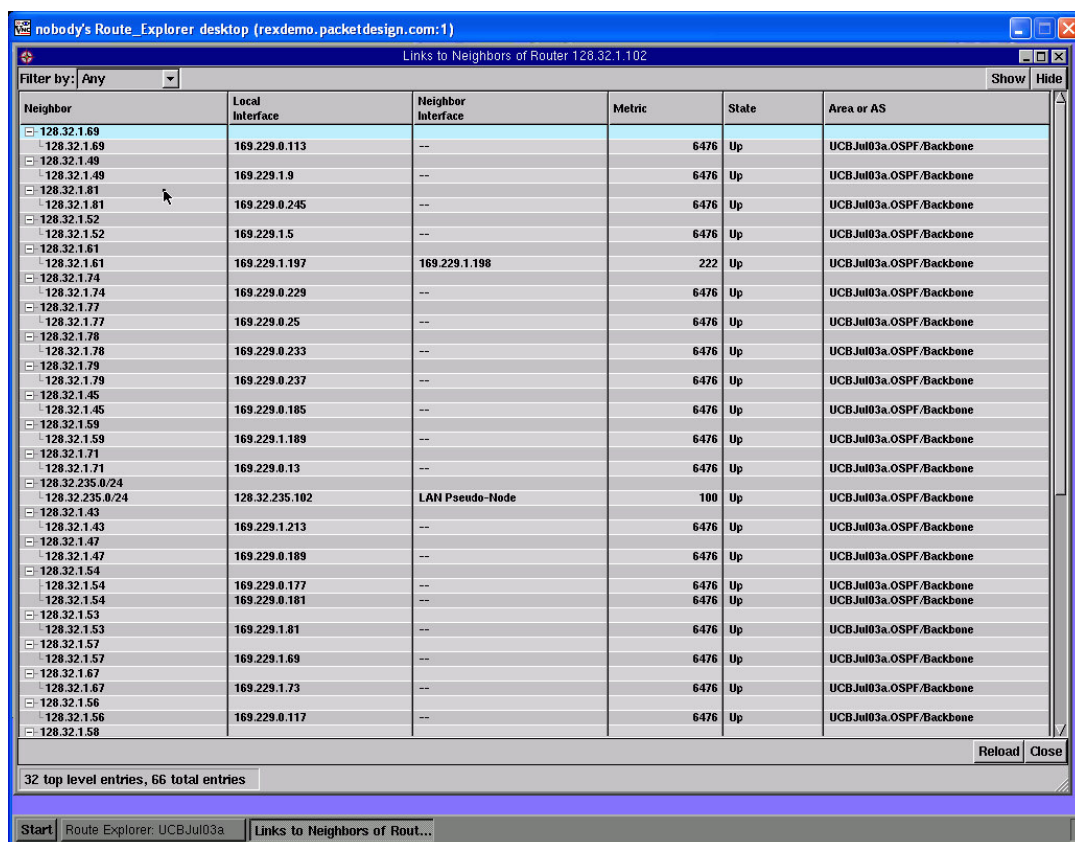
Best Practices for Eliminating Risk from Routing Changes

Perform Maintenance

1. Notify the Network Operations Center (NOC) of the start of the maintenance.
2. Follow the installation plan.
3. Test changes.
4. If tests are successful, monitor for company policy specified amount of time.
5. If tests fail, either correct the issues or back out of the maintenance.
6. Confirm that only the changes required by the maintenance have occurred.
7. End the maintenance by contacting the NOC and confirming that they see the router and see no problems.

How Route Explorer Helps in Upgrading Routers

Before maintenance, Route Explorer can be used to show all the adjacencies with all other routers and what prefixes are on the router (see Figure 5).



The screenshot shows the 'nobody's Route Explorer desktop (rexdemo.packetdesign.com:1)' window. The title bar indicates 'Links to Neighbors of Router 128.32.1.102'. The main table displays neighbor adjacency information with columns: Neighbor, Local Interface, Neighbor Interface, Metric, State, and Area or AS. The table lists 32 top-level entries and 66 total entries. The bottom status bar shows 'Start', 'Route Explorer: UCBJul03a', and 'Links to Neighbors of Rout...'. Buttons for 'Reload' and 'Close' are visible in the bottom right corner.

Neighbor	Local Interface	Neighbor Interface	Metric	State	Area or AS
128.32.1.69	169.229.0.113	--	6476	Up	UCBJul03a.ospf/backbone
128.32.1.69	169.229.1.9	--	6476	Up	UCBJul03a.ospf/backbone
128.32.1.81	169.229.0.245	--	6476	Up	UCBJul03a.ospf/backbone
128.32.1.52	169.229.1.5	--	6476	Up	UCBJul03a.ospf/backbone
128.32.1.61	169.229.1.197	169.229.1.198	222	Up	UCBJul03a.ospf/backbone
128.32.1.74	169.229.0.229	--	6476	Up	UCBJul03a.ospf/backbone
128.32.1.77	169.229.0.25	--	6476	Up	UCBJul03a.ospf/backbone
128.32.1.78	169.229.0.233	--	6476	Up	UCBJul03a.ospf/backbone
128.32.1.79	169.229.0.237	--	6476	Up	UCBJul03a.ospf/backbone
128.32.1.45	169.229.0.185	--	6476	Up	UCBJul03a.ospf/backbone
128.32.1.59	169.229.1.189	--	6476	Up	UCBJul03a.ospf/backbone
128.32.1.71	169.229.0.13	--	6476	Up	UCBJul03a.ospf/backbone
128.32.235.0/24	128.32.235.102	LAN Pseudo-Node	100	Up	UCBJul03a.ospf/backbone
128.32.1.43	169.229.1.213	--	6476	Up	UCBJul03a.ospf/backbone
128.32.1.47	169.229.0.189	--	6476	Up	UCBJul03a.ospf/backbone
128.32.1.54	169.229.0.177	--	6476	Up	UCBJul03a.ospf/backbone
128.32.1.54	169.229.0.181	--	6476	Up	UCBJul03a.ospf/backbone
128.32.1.53	169.229.1.81	--	6476	Up	UCBJul03a.ospf/backbone
128.32.1.57	169.229.1.69	--	6476	Up	UCBJul03a.ospf/backbone
128.32.1.67	169.229.1.73	--	6476	Up	UCBJul03a.ospf/backbone
128.32.1.56	169.229.0.117	--	6476	Up	UCBJul03a.ospf/backbone
128.32.1.58					

Figure 5: Neighbor adjacency lists are provided on a per-router basis

Route Explorer provides the ability to examine any router's neighbor adjacencies at any point in time by utilizing the History Navigator to move to a specific point in time (Figure 6), making it easy to compare



Best Practices for Eliminating Risk from Routing Changes

the router's adjacencies from the time the maintenance plan was written to the time for the maintenance. This in turn assures that no new prefixes were added and no new adjacencies have been formed. If there are unexpected changes, then the network engineer can abort the change or make modifications to the maintenance to allow it to continue accurately.

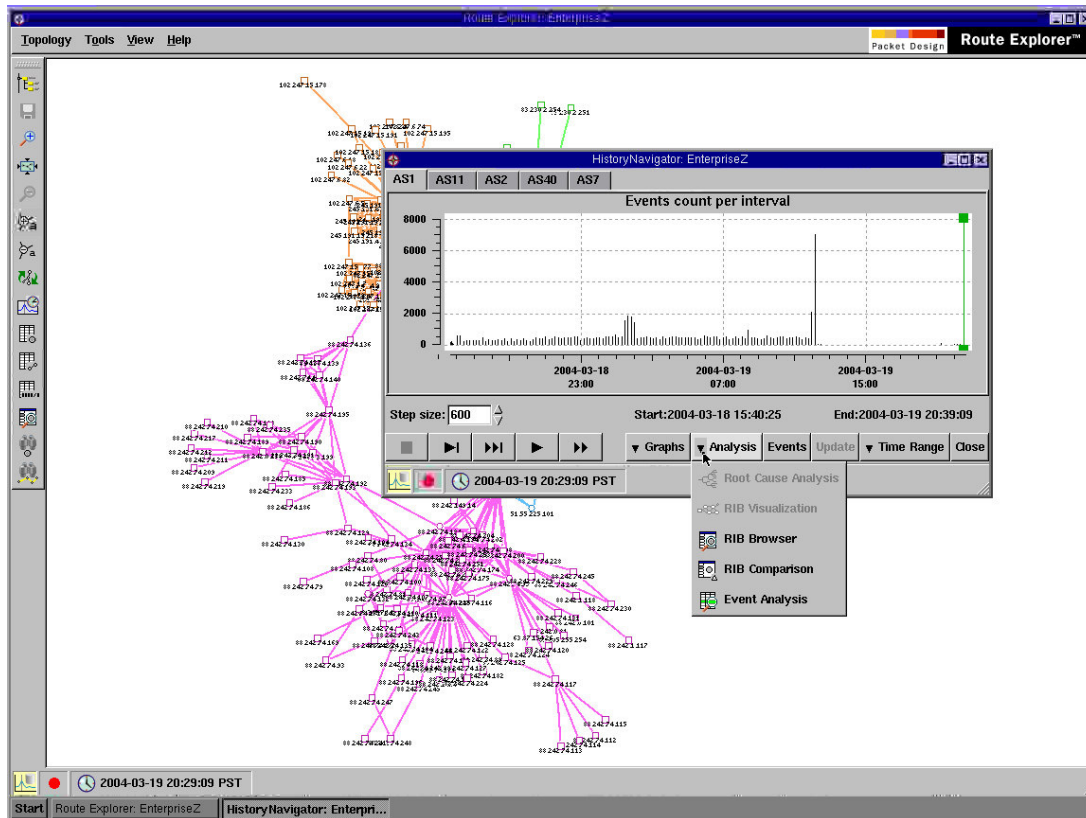


Figure 6: History Navigator allows engineers to go back to any point in time, and examine the precise state of routing at that time period. In addition the routing state can be played back sequentially to examine any changes or events that are relevant to an accurate maintenance operation.

After the maintenance, the adjacency list can be used to confirm that the new router has the same adjacencies as the existing router and that all prefixes are the same.

If there are changes in the metrics associated with the maintenance, this can be shown comparatively before and after the maintenance using Route Explorer's before and after RIB comparison view, as seen in Figure 7 on the following page:



Best Practices for Eliminating Risk from Routing Changes

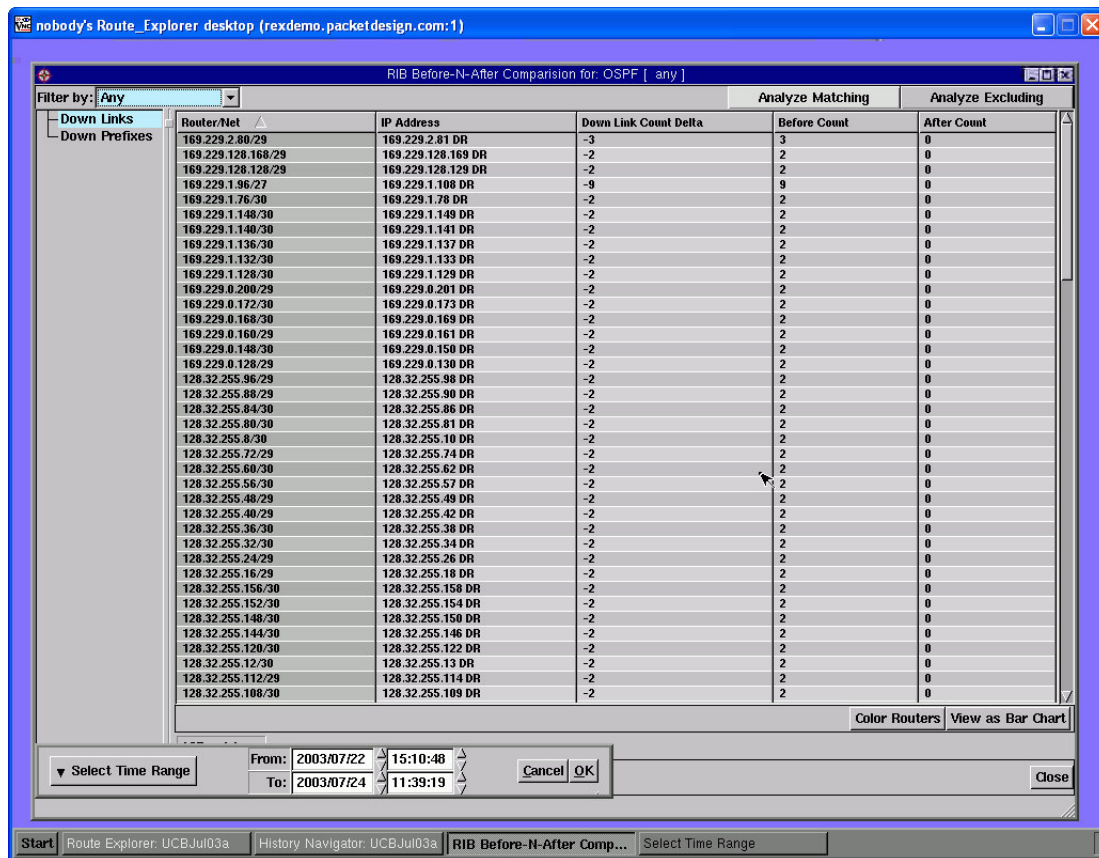


Figure 7: The RIB Before and After Comparison view allows network engineers to specify a time range and see what changed in the network-wide RIB, to verify that only expected changes have occurred.

Since Route Explorer records all routing protocol updates and will not miss changes, it can show the before and after maintenance differences from a network-wide perspective, including the surrounding routers' perspective, to ensure that the newly installed router hardware behaves the same way as the previous router.

Changing BGP Routing Policy Configurations

BGP policy attributes such as local preference (LP), Autonomous System (AS) path, and Multi-Exit Discriminator (MED), are all similar in their interaction with the network. In all these cases, as routes are advertised from a local router or received from a remote AS, the LP, AS path, or MED can be either assigned or rewritten coming into the network. Following are recommended best practice steps for changing BGP routing policy configurations:

Pre-Implementation Work

1. Confirm current policy for MED, LP, etc. to see how traffic flows currently.



Best Practices for Eliminating Risk from Routing Changes

2. Determine the new traffic pattern desired.
3. Determine which changes need to be made to BGP attributes to achieve the desired behavior.
4. Determine the router or routers that will be affected by the maintenance.
5. Confirm address or block of addresses that need to be changed.
6. Find the route map used to assign the current attributes to the routes that need to be changed.
7. Make sure the route map is the same on each router to be changed.
8. Determine the changes or additions to the route map(s) that need to be implemented for the new attributes to take effect.
9. For each router to be changed, create a step-by-step list of all changes needed to complete the maintenance.

Installation plan

1. Confirm before maintenance if any changes have occurred since the pre-work was completed. This will ensure that no routes are missed.
2. Follow the pre-created plan of action on each router in sequence.
3. Test after each change to confirm that routes have new attributes and that the changes have taken effect and have been propagated out of the network. Looking- glass sites should be used to verify propagation out of the network—a sample list of looking glass-sites can be found at:

http://www.bgp4.net/wiki/doku.php?id=tools%3Aipv4_looking_glasses

Back out plan

1. For each step of the plan, have a detailed back out plan so that if testing does not show the desired effect, the changes can easily be removed from the network and the original traffic patterns will return.
2. Confirm that, if the back out plan is implemented, everything does return to its original state, as BGP can sometimes be complex in how it interacts with attempted changes to its configuration.

Approval process

1. Follow company approval process. With the above documentation and any additional company-specific documentation this should be easily obtained.

Perform Maintenance

1. Implement changes on each router in the network.
2. Test changes on each router.
3. If tests are successful, end maintenance.
4. If tests fail, either correct issues or back out of maintenance.
5. Confirm that only the changes required of the maintenance happened.



Best Practices for Eliminating Risk from Routing Changes

How Route Explorer Helps Implement BGP Routing Policy Changes

Route Explorer provides detailed BGP route analytics in the largest service provider and enterprise networks today, including a BGP root cause analysis capability that can isolate the key events within a flood of BGP messages. Route Explorer's automated collection and analysis of BGP routing events is particularly helpful because of the sheer magnitude of BGP protocol messages generated from even relatively simple changes.

One of the primary tools that Route Explorer provides for supporting BGP routing policy change operations is visualizations of how LPs and other BGP attributes in the network affect BGP routing in the network, as seen in Figure 8. These visualizations provide a much more intuitive understanding of effective BGP routing policy, helping to ensure that network engineers' starting assumptions for the network maintenance are accurate.

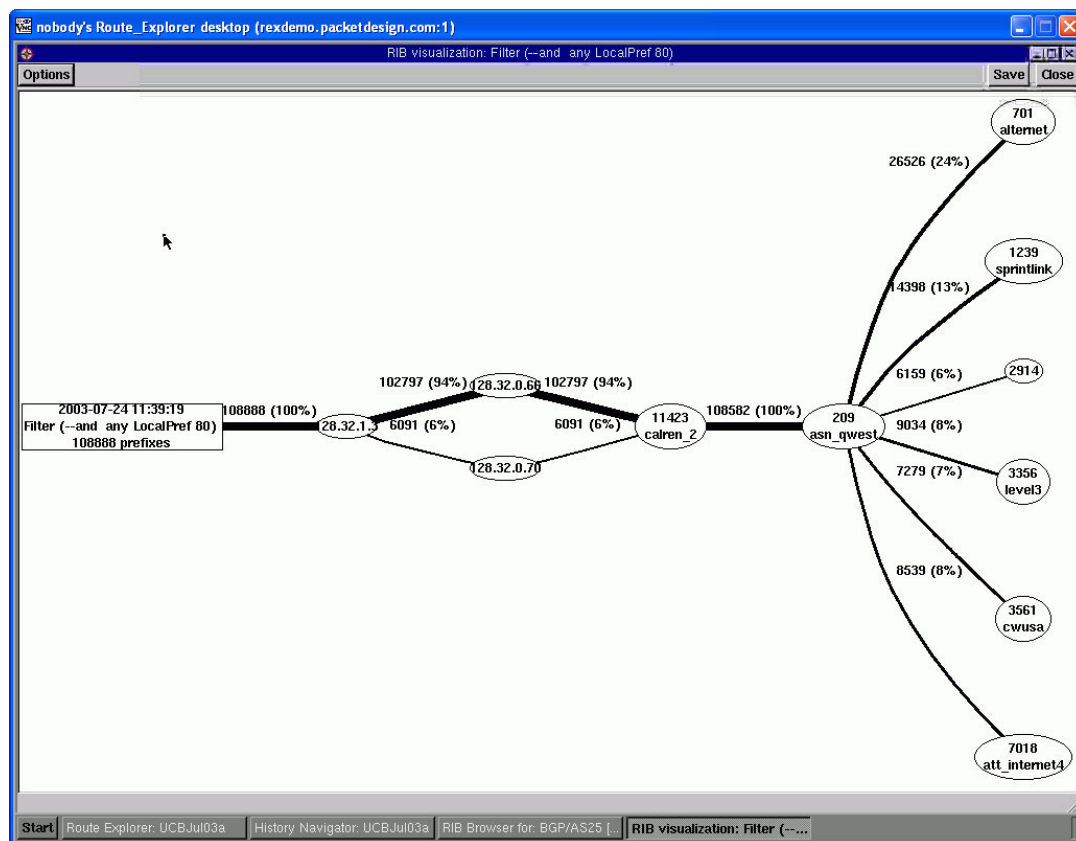


Figure 8: LP visualization shows how the selected LP directs traffic to exit the network

After the maintenance is performed, these visualizations can be used in conjunction with the History Navigator to provide an at-a-glance validation that the routing policy changed was effected properly by looking at visualizations from before and after the maintenance. In addition, Route Explorer can produce a before and after maintenance change table of all prefixes affected by the attribute in question to confirm that each route is tagged with the appropriate value, as seen in Figure 9 on the following page.



Best Practices for Eliminating Risk from Routing Changes

Router Name	Peer BGP ID	Prefix	Before Attributes	After Attributes
---	128.32.1.3	12.173.60.0/23	---	AS Path: 11423 209 7018 26259 (IGP) Local-Pref: 80 MED: 5 Communities: 209:888 209:889 11423:65350 11423:65352 Next Hop: 128.32.0.66
---	128.32.1.3	24.155.4.0/24	AS Path: 11423 209 2914 7459 (IGP) Local-Pref: 80 MED: 5 Communities: 209:888 11423:65350 11423:65352 Next Hop: 128.32.0.66	---
---	128.32.1.3	24.155.5.0/24	AS Path: 11423 209 2914 7459 (IGP) Local-Pref: 80 MED: 5 Communities: 209:888 11423:65350 11423:65352 Next Hop: 128.32.0.66	---
---	128.32.1.3	24.155.6.0/23	AS Path: 11423 209 2914 7459 (IGP) Local-Pref: 80 MED: 5 Communities: 209:888 11423:65350 11423:65352 Next Hop: 128.32.0.66	---
---	128.32.1.3	24.155.8.0/22	AS Path: 11423 209 2914 7459 (IGP) Local-Pref: 80 MED: 5 Communities: 209:888 11423:65350 11423:65352 Next Hop: 128.32.0.66	---
---	128.32.1.3	24.155.28.0/22	AS Path: 11423 209 2914 7459 (IGP) Local-Pref: 80 MED: 5 Communities: 209:888 11423:65350 11423:65352 Next Hop: 128.32.0.66	---
---	128.32.1.3	24.155.32.0/21	AS Path: 11423 209 2914 7459 (IGP) Local-Pref: 80 MED: 5 Communities: 209:888 11423:65350 11423:65352 Next Hop: 128.32.0.66	---
---	128.32.1.3	24.155.40.0/21	AS Path: 11423 209 2914 7459 (IGP) Local-Pref: 80 MED: 5 Communities: 209:888 11423:65350 11423:65352 Next Hop: 128.32.0.66	---
---	128.32.1.3	61.39.255.0/24	---	AS Path: 11423 209 2516 2516 2516 4766 18321 (IGP) Local-Pref: 80 MED: 5 Communities: 209:888 11423:65350 11423:65352 Next Hop: 128.32.0.66
---	128.32.1.3	62.29.0.0/19	---	AS Path: 11423 209 701 702 8513 8513 8513 8513 8513 8513 129 Local-Pref: 80 MED: 5 Communities: 209:888 11423:65350 11423:65352 Next Hop: 128.32.0.66
---	128.32.1.3	62.56.205.0/24	AS Path: 11423 209 701 12491 (IGP) Local-Pref: 80 MED: 5 Communities: 209:888 11423:65350 11423:65352 Next Hop: 128.32.0.66	---
---	128.32.1.3	62.64.64.0/18	AS Path: 11423 11422 209 701 702 5377 12530 (IGP) Local-Pref: 80 MED: 5	---

Figure 9: LP before and after prefix list views show all prefixes affected by the LP to confirm proper LP route tagging based on the maintenance change

Conclusion

IP routing operations are challenging and easily prone to costly misconfigurations. With increasing pressure on IT and network engineering to deliver against service level agreements, implementing well-documented and well supported control processes is more important than ever. Route Explorer provides a platform for best practices in routing maintenance and change operations, helping network engineers to meet rising customer expectations with greater confidence, accuracy and speed than ever before.



Best Practices for Eliminating Risk from Routing Changes

To learn more about Packet Design and Route Explorer, please:

- Email us at info@packetdesign.com
- Visit Packet Design's web site at www.packetdesign.com
- Call us at +1.408.490.1000

Corporate Headquarters

Packet Design

2455 Augustine Drive

Santa Clara, CA 95054

Phone: 408.490.1000

Fax: 408.562.0080

