

7. Get a summary of the routing events in a time period

When diagnosing a network outage or doing forensic analysis after one, having complete historical data and analysis capability can be invaluable. In the previous section we showed how Route Explorer's History Navigator shows event churn in a timeline and analyzes the state of the RIB before and after network churn. In this section we show how Route Explorer can help you narrow down the event churn to the root cause.

Figure 14 shows high churn that lasts for more than an hour. Using Route Explorer's Event Analysis, we have focused on a small part of the total churn period (between the blue vertical lines). The lower part of the figure shows the analysis of all events in the chosen time period. Selecting to look at the MEDs affected, we see that a small number of them (three) have a very large number of events associated with them. We suspect this may be a "MED Oscillation"¹.

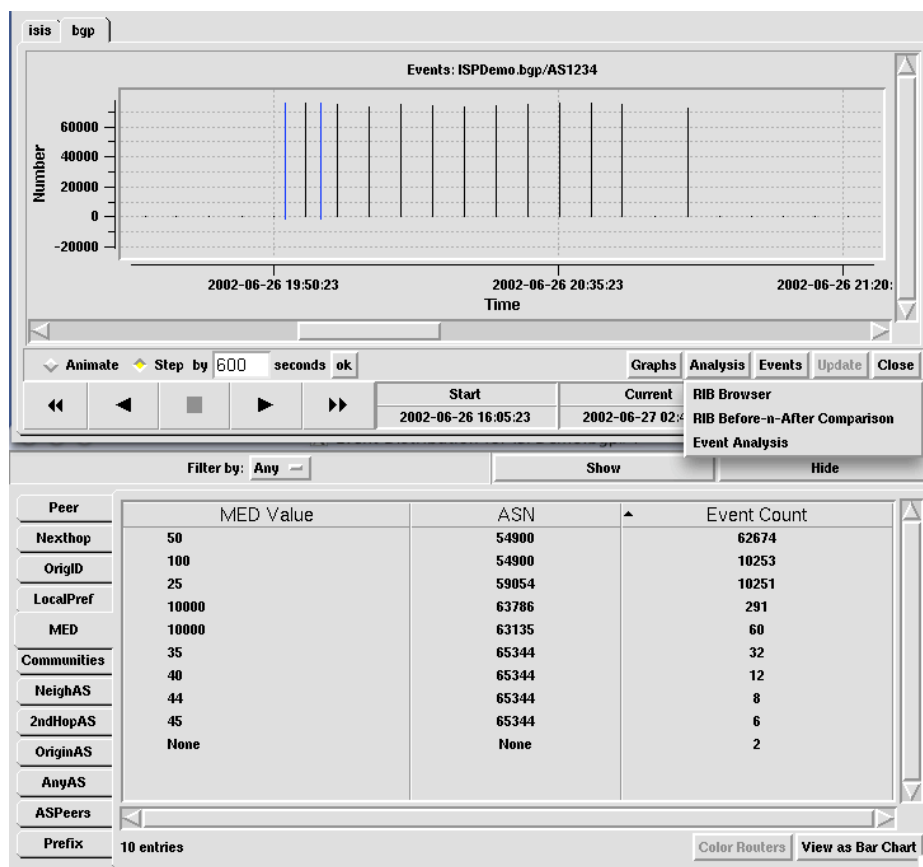


Figure 14

¹ BGP attribute "Multi-Exit Discriminator" is used to signal preferred exit points from one AS to neighbor ASes with whom there are has multiple connections. Different MED values learned for the same prefix can sometimes cause multiple route reflectors in an AS to repeatedly learn and advertise them into the IBGP mesh, causing a severe route flap.

To identify the prefix affected by this possible MED oscillation, we select the “Prefix” tab of the analysis. Figure 15 shows what we see:

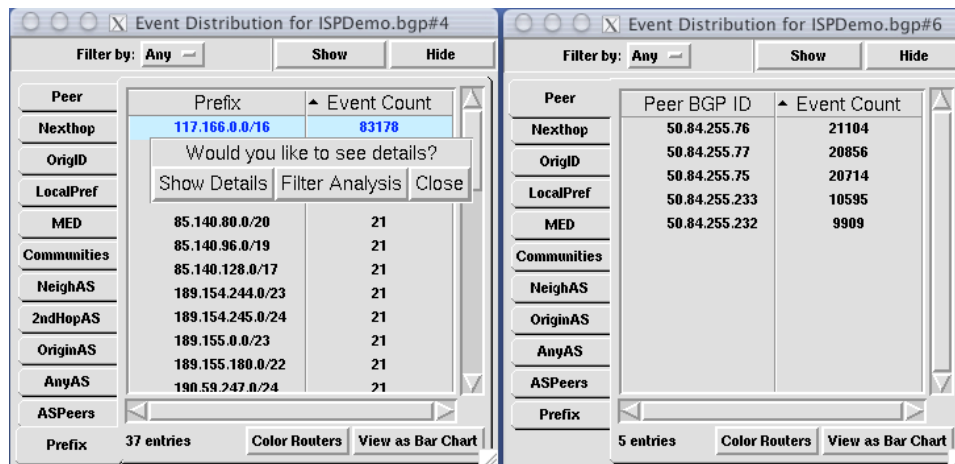


Figure 15

A single prefix has a huge number of events associated with it – 83,178 events in less than 10 minutes! To see which BGP peers have generated these events we drill down to see the details. Route Explorer can do a second pass of event analysis focused only on events associated with the selected prefix. The results are shown at the right side of Figure 15.

It seems that three peers have generated the majority of the events and each has generated about a third of them. Our suspicion of a MED oscillation grows stronger. To confirm it, we need to look at the actual events. We show how in the next section.

HOW TO:

1. Select the “DemoTier1ISPJun02” topology and open History Navigator (see above)
2. Zoom the timeline to the time period of the series of spikes near the center of the events timeline: Control-Right-Click and Drag to select the zoom area. Control-Right-Click to end selection and affect the zoom of the timeline.
3. From Analysis drop-down, select “Event Analysis”
4. Select the time period around the first spike, using blue crosshair cursor.
5. Resulting tables can be filtered, sorted and viewed as bar graphs (see above)
6. Select the “MED” tab to see the oscillation.
7. Next, select the “Prefix” tab to identify the prefix oscillating.
8. Drill down on a particular table entry: Right-Click on the prefix entry with the high event count to show the “Would you like to see details?” popup.
9. Select “Filter Analysis” to do iterative events analysis with the selection as a filter criteria.