Sample Applications

Prime Analytics includes two sample applications showing examples of network data displayed using the Prime Analytics BI platform dashboard and analytics components. Although the applications are fairly simple, they provide examples to give you an understanding of the general concepts and mechanics that go into dashboard creation, and allow you to begin building applications for your network.

Sample applications are described in the following topics:

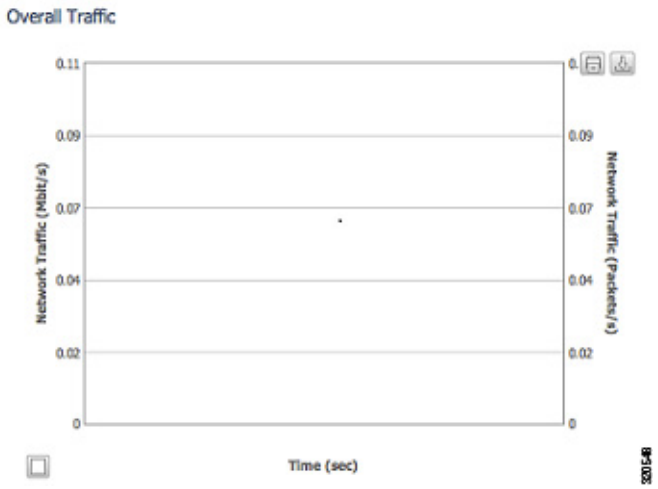
NetFlow Sample Application

The Network Summary sample dashboard shows network traffic based on a continuous NetFlow query stream. The dashboard runs off a local log file to simulate live traffic.

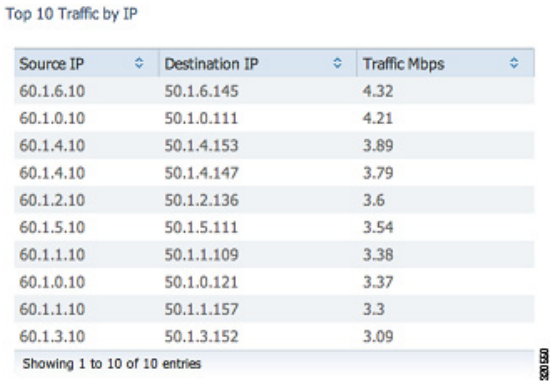
Components

The dashboard includes the following components:

- Overall Traffic—Displays the overall network traffic in the Real Time Dual Y chart component. One Y axis displays overall traffic in megabits per second. The other Y axis displays the overall traffic in packets per second. The data is refreshed every second.



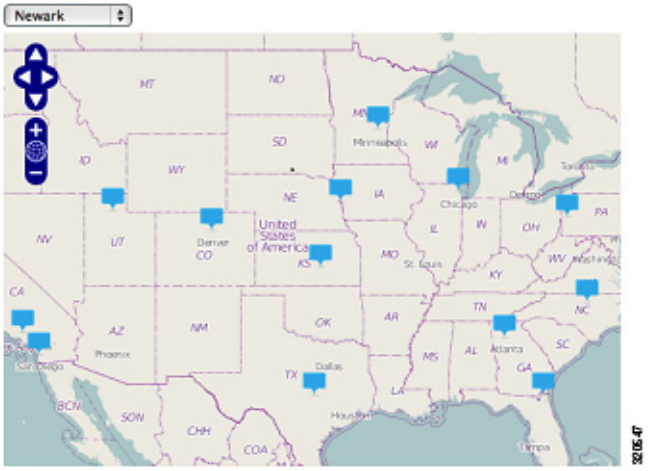
- Top 10 Traffic by IP—Displays the source and destination hosts with the highest traffic in Mb/s. The data is displayed in a three-column table. The data is refreshed every 10 seconds.


Top 10 Traffic by IP

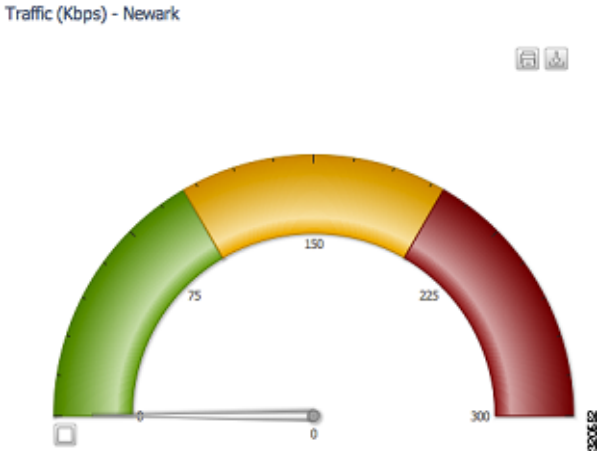
Source IP	Destination IP	Traffic Mbps
60.1.6.10	50.1.6.145	4.32
60.1.0.10	50.1.0.111	4.21
60.1.4.10	50.1.4.153	3.89
60.1.4.10	50.1.4.147	3.79
60.1.2.10	50.1.2.136	3.6
60.1.5.10	50.1.5.111	3.54
60.1.1.10	50.1.1.109	3.38
60.1.0.10	50.1.0.121	3.37
60.1.1.10	50.1.1.157	3.3
60.1.3.10	50.1.3.152	3.09

Showing 1 to 10 of 10 entries

- City Traffic—Displays traffic for individual cities. Dashboard components used to display city traffic include:
  - City Selector—Allows users to choose a city using a map from OpenStreetMap. (See http://www.openstreetmap.org for information.) Using a US map, users can select cities using the city drop down field or choosing a city on the map. (You can implement Google Maps using the GoogleMapAPI. Refer to the Google website documentation for information.)



  - Traffic - [*City*]—Displays traffic in kilobits per second using the Real Time Angular chart.



– Traffic - [*City*]—Displays traffic in kilobits per second using the Real Time Line chart.

– ToS Distribution - [*City*]—Displays a Type of Service distribution using the CCC Pie chart.

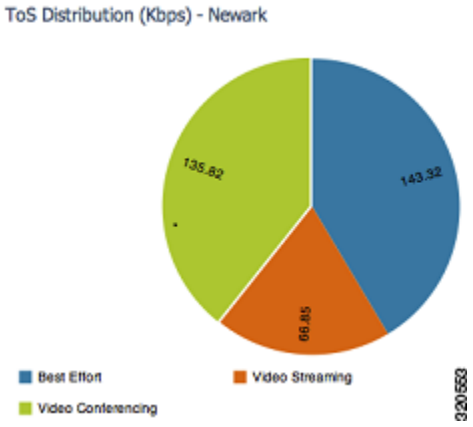


Table B-1 lists the components that comprise the NetFlow Summary sample application.

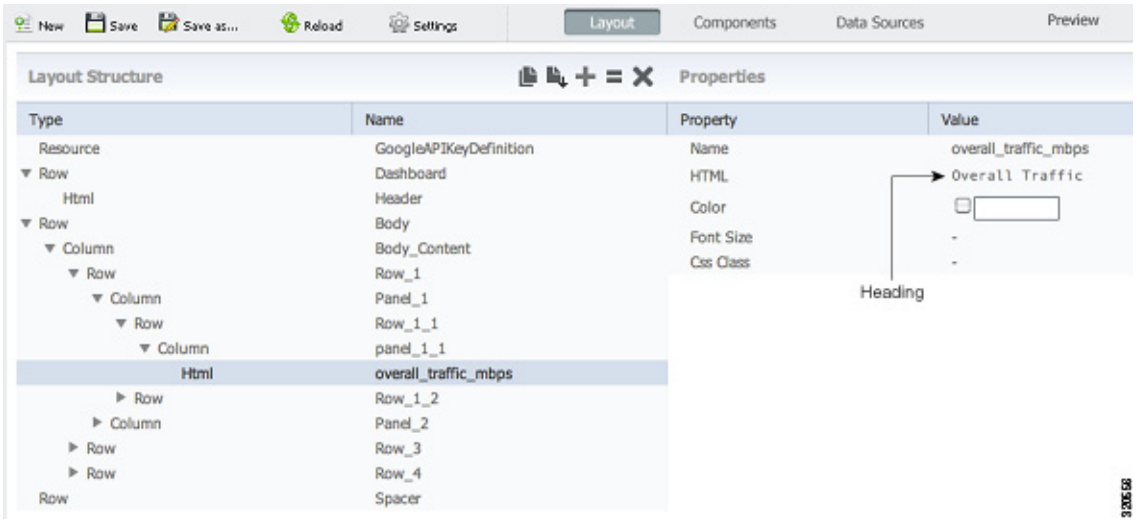
Table B-1 NetFlow Summary Dashboard Components

Dashboard Component	Component Name	Type	Group
General Traffic	overall_traffic	Real Time Line Dual Y	Real Time Charts
Top 10 Traffic by IP	top_10_traffic_table	Table Component	Others
Map	map_header	Text Component	Others
	traffic_map	Map Component	Custom
	param_city_name	Parameter	Generic
	select_city	Select Component	Selects
Traffic - [*city*]	traffic_gauge_header	Text Component	Real Time Charts
	city_traffic_gauge_kbps	Real Time Angular Gauge	Real Time Charts
Traffic - [*city*]	traffic_column_chart_header	Text Component	Others
	city_traffic_kpbs	Real Time Column	Real Time Charts
Tos Distribution	tos_pie_header	Text Component	Others
	tos_by_city	CCC Pie Chart	Charts

Layout

The layout, shown below, is based on a 4x4 template with an additional row added. When creating layouts for your dashboards, a good approach is to choose a template that is closest to your needs, and then customizing it.

To provide uniform labeling placement, labels are placed in separate rows.In the example below, An HTML element with the text, Overall Traffic, is placed in the Row_1_1 row and panel_1_1 column, If you expand the second column: Panel_2 > Row_1_3, Panel_2_1, you will see an HTML component with the second column heading text, Top 10 Traffic by IP. If desired, you can link the HTML element to a Cascading Style Sheet so all text is displayed uniformly.



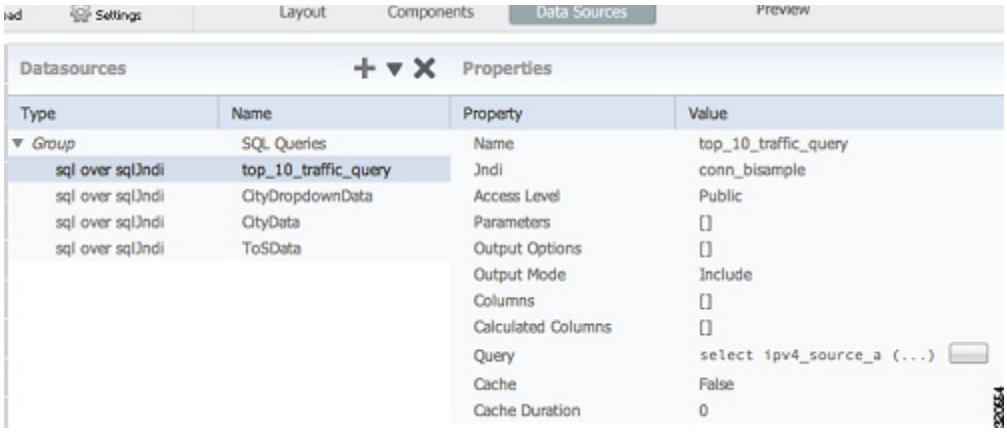
Data Source

The data sources for the sample NetFlow application are shown below. The data source captured in the screen below is only for static content:

- top_10_traffic_query
  - Top 10 Traffic by IP Table
  - CityDropdownData: City dropdown
  - CityData: Map Component
  - ToSData: ToS Distribution (Kbps) - City Pie Chart

The data source for real-time charts are selected on the Components tab. Choose **Edit Components > Real Time Charts > Real Time Line Dual Y (overall_traffic)**. Under Path Property, click **View SQL** to see a list of available continuous queries. At the bottom click ^ to select the continuous query that you want to use for the chart.

NOTE: You might have to take a few screenshots for selecting the Continuous Query datasource Data sources are defined outside the BI platform. In the sample application, SQL Queries list the data files used to simulate continuous query data. When you set up actual continuous query data sources, you will not set it up under the User Console Data Sources workspace. For information, see Setting Up Continuous Query Data Sources, page 4-8.



Changing Open Street to Google Maps

The following steps show you how to replace the existing Open street map component in the sample NetFlow application with Google maps. Before you begin, you need to get a Google Maps API key. The key is available from Google. See the Google website for details.

Step 1 Open the Network Summary dashboard in Edit mode:

a. Under Browse, click **NetFlow**.

b. Under Files, click **Network Summary**.

c. Click the **Edit** tool.

Step 2 Click the **Layout** tab.

Step 3 Click the **Add Resource** tool (+).

Step 4 Select the Resource Type, **JavaScript**, and the value **Code Snippet**.

Step 5 Click **OK**.

Step 6 In the Name field, enter **GoogleAPIKeyDefinition.**

Step 7 In the Resource Code field, click the button to the right.

Step 8 In the Edit window, enter your Google maps API key as follows:

var API_KEY = 'YOUR_ KEY'; (*Your corporate/personal Google API map key provided by Google*).

Step 9 Click **OK**.

Step 10 Click the **Save** tool to save the changes.

Step 11 Click the **Components** tab.

Step 12 Select the Group, Custom, then choose the Map Component, usa_map.

Step 13 Change the value in property Map Engine from open to **google**.

Step 14 Click **Save**.

Step 15 Validate the change by open the dashboard

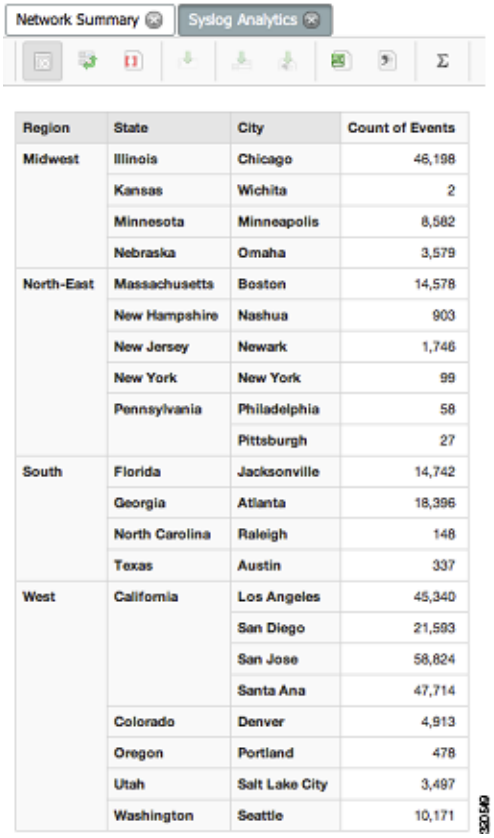
Syslog Analytics Sample Application

The sample syslog application shows how the Prime Analytics BI platform analytics can be used to display network data. Prime Analytics Analytics is based on the Pentaho Mondrian online analytical processing (OLAP) data model. OLAP allows you to drill into and cross-tabulate information in many different ways and from multiple perspectives.

By default, the sample syslog displays the Region, State, and City dimensions with the Count of Events measure. To add additional dates and priorities, select the Syslog Analytics file and choose **Edit**. In the Editing: Syslog Analytics file, add the additional dimensions:

- Date—All, Year, Quarter, Month
- Priority—All, Priority Category, Priority Name

Each added dimension causes a recalculation to occur and results are displayed in the analytics table.



Region	State	City	Count of Events
Midwest	Illinois	Chicago	46,198
	Kansas	Wichita	2
	Minnesota	Minneapolis	8,582
	Nebraska	Omaha	3,579
North-East	Massachusetts	Boston	14,578
	New Hampshire	Nashua	903
	New Jersey	Newark	1,746
	New York	New York	99
	Pennsylvania	Philadelphia	58
		Pittsburgh	27
South	Florida	Jacksonville	14,742
	Georgia	Atlanta	18,396
	North Carolina	Raleigh	148
	Texas	Austin	337
West	California	Los Angeles	45,340
		San Diego	21,593
		San Jose	58,824
		Santa Ana	47,714
	Colorado	Denver	4,913
	Oregon	Portland	478
	Utah	Salt Lake City	3,497
	Washington	Seattle	10,171

320549

Additionally, you can drill down and display the individual syslog data records by clicking **Drill Through on Cell** or **Drill Through on Cell on to CSV** on the Analytics toolbar, then clicking the table. In the dialog, choose the dimensions you want to see, then click **OK**. A second table displays the details of every syslog record for the dimensions you selected.

Region	State	Count of Events
Midwest	Illinois	RP/0/RP1/CPU0:Aug 6 01:19:47.204 EST: spm[371]: %SECURITY-SPM-3-ERR_MSG_GEN : nvram not availab
Midwest	Illinois	*Aug 5 22:31:32.286: %SYS-1-CPUFALLINGTHRESHOLD: Threshold: Total CPU Utilization(Total/Intr) 70%/0
Midwest	Illinois	*Aug 5 23:58:41.802: %SYS-1-CPUFALLINGTHRESHOLD: Threshold: Total CPU Utilization(Total/Intr) 69%/0
Midwest	Illinois	RP/0/RP1/CPU0:Aug 6 06:10:16.068 EST: nvram[75]: %MEDIA-NVRAM-3-CORRUPT : Corrupt nvram. Format with "erase nvram: forma
Midwest	Illinois	DRP/0/4/CPU0:Aug 6 08:38:42.079 : exec[65711]: %SECURITY-login-6-AUTHEN_SUCCESS : Successfully authenticated user 'mbirkner' from '192.168.239.26' on 'vty
Midwest	Illinois	RP/0/RP1/CPU0:Aug 6 18:11:37.590 EST: sysmgr[91]: %OS-SYSMGR-3-ERROR : spm_server(1) (jid 371) exited, will be respawned with a delay (slow-resta
Midwest	Illinois	RP/0/RP1/CPU0:Aug 6 22:02:19.783 EST: nvram[75]: %MEDIA-NVRAM-3-CORRUPT : Corrupt nvram. Format with "erase nvram: forma

320555

The strength of the OLAP analytics model is the ability to consolidate or expand and drill down data in many different ways. While the Syslog Analytics sample application includes only a few dimensions and one measure, it should demonstrate the capability of analytics to show network data in a variety of ways.

Syslog and NetFlow Live Sample Application

The Syslog and NetFlow Live Dashboard sample application allows you to view simulated live NetFlow and syslog data, then connect the sample to your NAM and NGA devices and generate live syslog and NetFlow traffic to the sample dashboard.

The NetFlow Syslog Live Dashboard sample is located in the Samples/NetFlow Syslog Live directory in the User Console directory. The sample provides the following data:

- Cisco NetFlow Generator Appliance (NGA)—NetFlow Sum of Bytes and Sum of Packets by Time.
- Cisco Network Analysis Module (NAM)—Syslog Count of Events by Time.
- NGA and NAM
  - NGA NetFlow—Sum of Bytes
  - NAM syslog—Actual Value by Time

The data is displayed using a dashboard comprised of the Real Time Line Dual Y and Real Time Column chart components. (For information about creating and editing dashboards, see Chapter 5, “Creating Dashboards.”)

The NetFlow and syslog data streams are installed on your TruCQ engine. The schema can be viewed in the following location:

$PA_HOME/biplatform/sampledatagenerator/netflow_namsyslog/customizations/db/ nfsyslog.sql

The Syslog and NetFlow Live Dashboard connectors are installed in:

$PA_HOME/biplatform/sampledatagenerator/netflow_namsyslog

You can change these data sources as needed to ensure the fields that are consumed match your input.

Configuring the Syslog and NetFlow Live Dashboard for Live Data

Complete the following steps to connect the Syslog and NetFlow Live Dashboard to NAM and NGA devices generating syslog and NetFlow traffic on your network:

Step 1 Update the NAM_SYSLOG PORT and NGA_NETFLOW PORT in include-handlers.xml, located at:

`$PA_HOME/biplatform/sampledatagenerator/netflow_namsyslog/customizations/templates/include-handlers.xml.`

Port 514 is the default NAM syslog port; Port 3000 is the default NGA NetFlow port.

Step 2 Update the include-handlers.xml for the NetFlow fields that are consumed:

`$PA_HOME/biplatform/sampledatagenerator/netflow_namsyslog/customizations/templates/include-handlers.xml`

Step 3 Update the syslog_parsing_rules.xml for the syslog fields that are consumed:

`$PA_HOME/biplatform/sampledatagenerator/netflow_namsyslog/syslog_parsing_rules.xml)`

Step 4 Log into your NAM device and direct syslog traffic to the NAM_SYSLOG PORT configured in Step 1.

Step 5 Log into your NGA device and direct NetFlow traffic to the NGA_NETFLOW PORT configured in Step 1.

Step 6 As the root user, navigate to the following directory:

`$PA_HOME`/biplatform/sampledatagenerator/netflow_namsyslog

Step 7 Load the environment variables:

```
$PA_HOME/bin/pa_env.sh
```

Step 8 Run the build:

```
$PA_HOME/bin/build-local.sh
```

Note If you receive errors, the most likely cause is the environment variables are not set. Repeat Step 7 to load all the variables.

Step 9 Start the build:

```
$PA_HOME/bin/start.sh
```

The connectors begin listening on the ports configured in Step 1.

Note If you receive an address already in use error, the port configured in Step 1 is already in use. Either choose a new port or stop the service that is using that port.

Note To see if data is flowing into the port, you can use the tcpdump port <*port number*> command, for example, **tcpdump port 514**.

Step 10 Log into the Prime Analytics BI platform (see Logging Into the User Console, page 3-1).

Step 11 Display the Syslog and NetFlow Live Dashboard and observe your live syslog and NetFlow traffic.