

Network Traffic Analysis Tools

User Guide

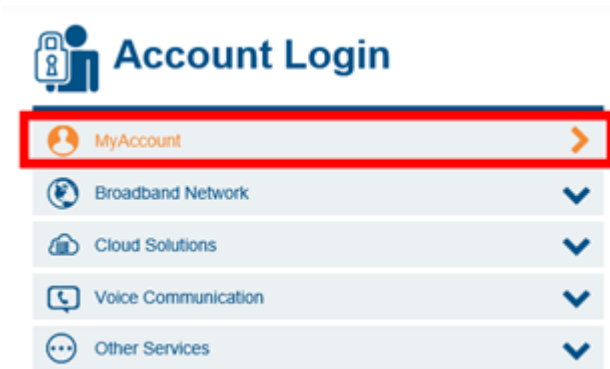
Table of Content

1. To access the Network Traffic Analysis tools.....	3
2. The Network Snapshot View.....	5
3. The Interface View.....	6
3.1. Status description.....	6
3.2. Icon/ Button descriptions	7
4. To view detailed Network Traffic Analysis report of an interface.....	8
4.1. Traffic	8
4.2. Application.....	9
4.3. Source.....	10
4.4. Destination	11
4.5. QoS.....	11
4.6. Conversation	12
5. More Reports	13
5.1. TroubleShoot Reports	13
5.2. Consolidated Reports.....	14
5.3. Search Reports	15
5.4. Compare Reports.....	16

Remarks:

The NBAR, CBQoS and Google Map View functions are not applicable in this Network Traffic Analysis Tools.

1. To access the Network Traffic Analysis tools



Step 1

Go to
<http://hkbnes.net/en/accountservices>

Click **MyAccount**

Account Type : [Login Guideline](#)

Username : [Forgot Account No. / Username](#)
☒ Remember Username

Password : [Forgot Password](#)

Step 2

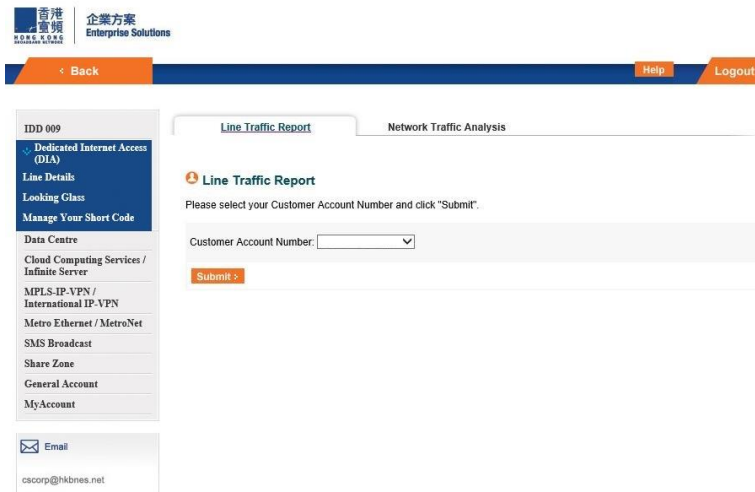
- Choose **eCS/ManagedBiz** in Account Type
- Enter **Username** and **Password**
- Click **Login**.



Step 3

Click the **ManagedBiz** icon.

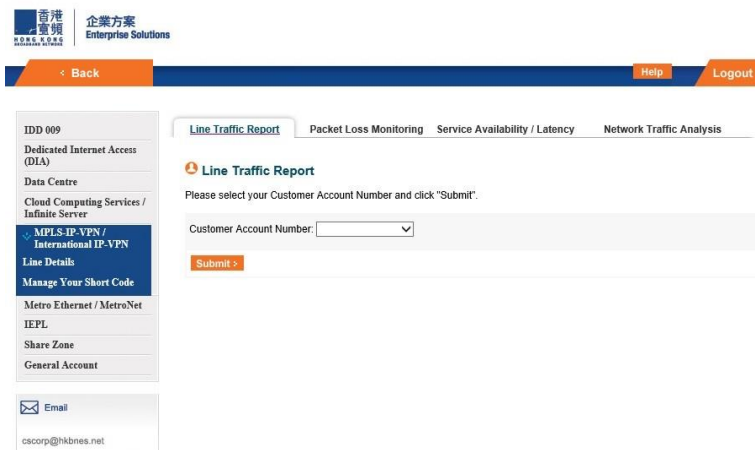




Step 4

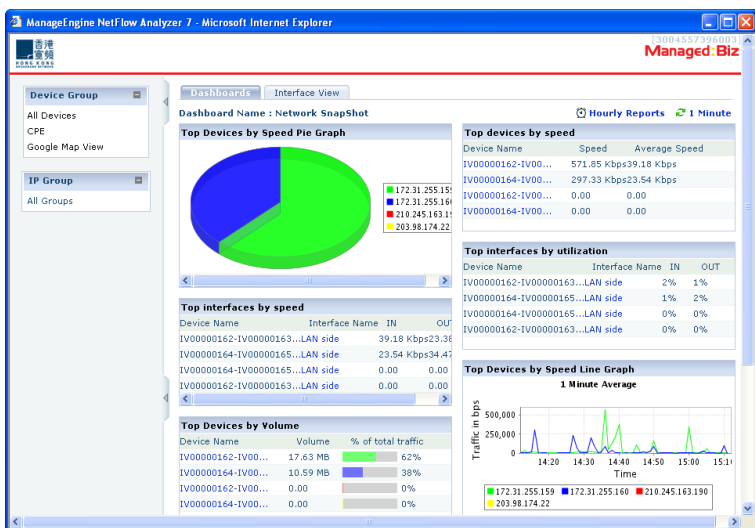
To view Network Traffic Analysis report of **Dedicated Internet Access (DIA)**:

- Click **Dedicated Internet Access (DIA)**.
- Click on the tab **Network Traffic Analysis**.
- Select account number and click **Submit**.



To view Network Traffic Analysis report of **MPLS-IP-VPN / International IP-VPN**:

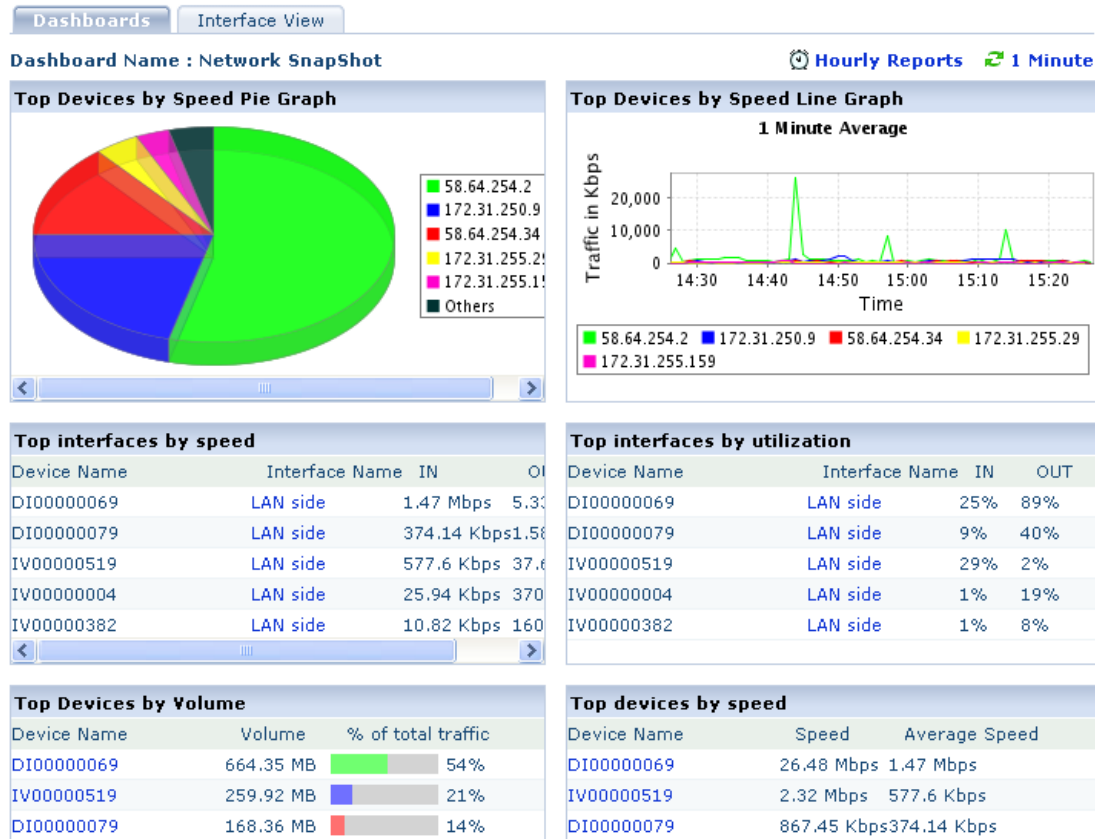
- Click **MPLS-IP-VPN / International IP-VPN**.
- Click on the tab **Network Traffic Analysis**.
- Select account number and click **Submit**.



Network Traffic Analysis tools shown in pop-up window.

2. The Network Snapshot View

The Network Snapshot View is the default page after logging in to the Network Traffic Analysis Tools. It displays the information of top devices, top interfaces and top IP groups.



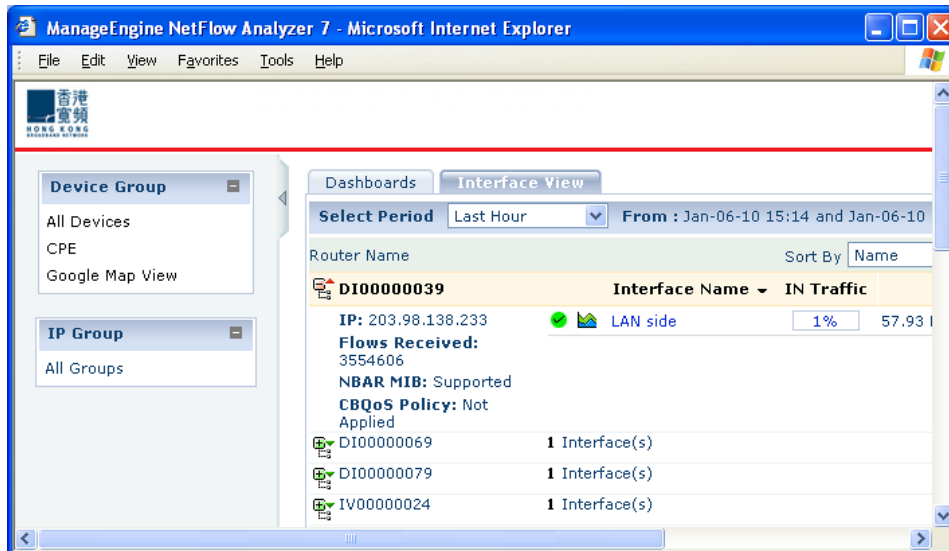
The time period of the report can be modified using the select period icon . You can select "Last Hour", "Last 6 Hours", "Today" or "Last 24 Hours".

The time period to update the report can be modified as well, you may click the icon to select "Never", "Every 1 minute", "Every 5 minutes" or "Every 10 minutes".

Clicking any Device Name will link to the Interface View of that particular device, while clicking any Interface Name will link to the Network Traffic Analysis reports of that interface.

3. The Interface View

The Interface View lists all the interfaces from which the Network Traffic Analysis tools have received.

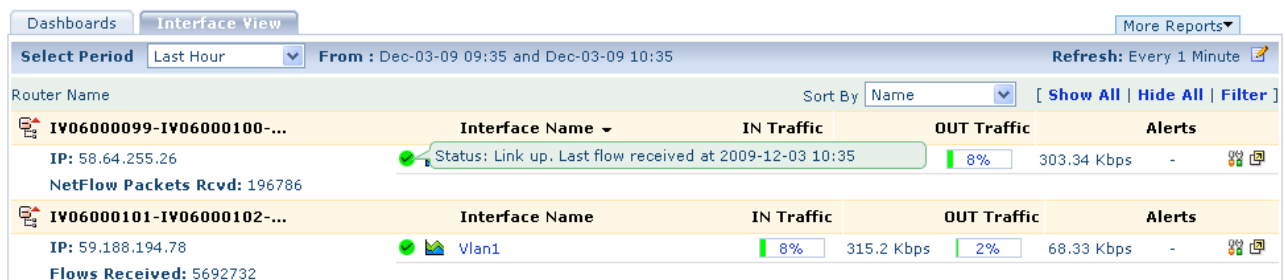


Click on the tab **Interface View** or click **All Devices** under **Device Group** to view all interface.

OR

Simply click on any **Device Name** to access the Interface View of a particular device.






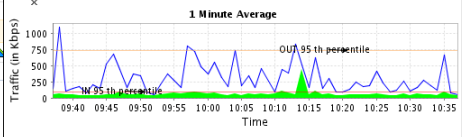


3.1. Status description



Icon	Description
	The Status of the interface is unknown and no flows have been received for the past 10 minutes. The interface is not responding to SNMP requests.
	The interface is responding to SNMP requests and the link is up, but no flows have been received for the past ten minutes.
	The link is up, and flows are being received.
	The interface is responding to SNMP requests and the link is down and no flows are being received.

3.2. Icon/ Button descriptions

Dashboards		Interface View		More Reports	
Select Period		Last Hour	From : Dec-03-09 08:38 and Dec-03-09 09:38		Refresh: Every 1 Minute
Router Name		Sort By		Name	[Show All Hide All Filter]
IV06000099-IV06000100-...		Interface Name		IN Traffic	OUT Traffic
IP: 58.64.255.26		Vlan1		2%	79.66 Kbps
NetFlow Packets Rcvd: 196380				14%	550.4 Kbps
IV06000101-IV06000102-...		1 Interface(s)			

Icon/ Button	Purpose
	Click this icon, or the router name, to view the interfaces corresponding to the router.
	Click this icon to hide the interfaces corresponding to the router.
	Click this icon to set the time period for refreshing the page contents.
	Click this link to troubleshoot an interface. You can troubleshoot only one interface at a time.
	Click this icon to have a preview of the traffic graphs without drilling down in to each interface. <div data-bbox="518 1025 1396 1272">  </div>
	Click this icon to see all traffic details of an interface at one glance.
Show All	Click the Show All link to display all routers' interfaces on the Dashboard.
Hide All	Click the Hide All link to hide all interfaces and show only the router names in the Router List.
Filter	You can set filters on the Dashboard view to display only those interfaces whose incoming or outgoing traffic values exceed a specified percentage value. Click the Filter link to specify minimum percentage values for IN or OUT traffic. Click the Set button for the changes to take effect. The filter settings are then displayed beside the Filter link. Click the  icon any time to clear the filter settings and display all interfaces on the Dashboard again.

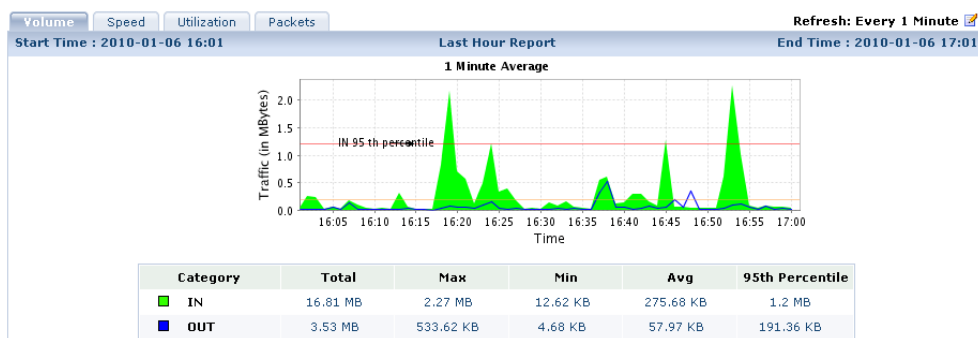
4. To view detailed Network Traffic Analysis report of an interface

4.1. Traffic

The **Traffic** tab shows real-time traffic graphs for incoming and outgoing traffic. Tabs above the traffic graph allows you to view the graph in terms of volume of traffic, speed, link utilization and number of packets received.

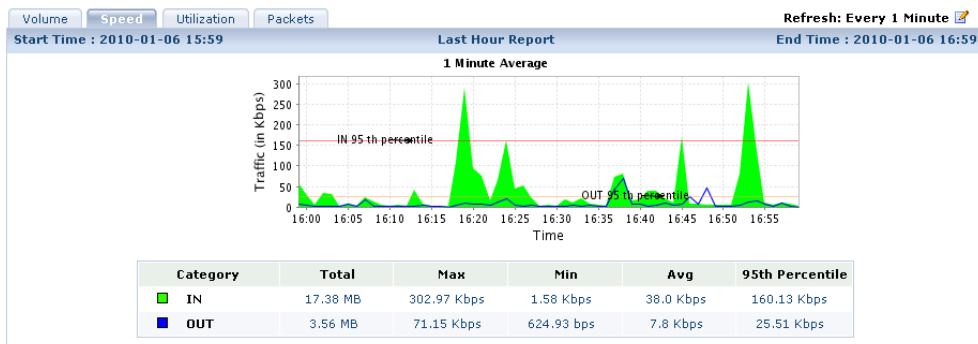
The table shows the legend, along with total, maximum, minimum, and average traffic values for this interface or IP group, for the selected time period.

Volume



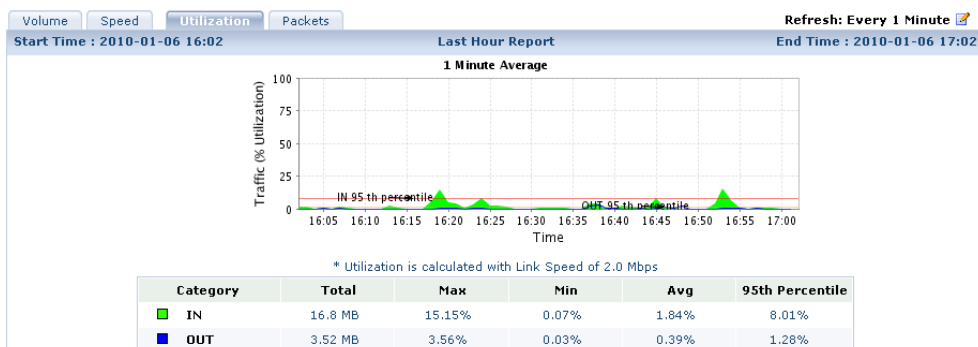
Click on the tab **Volume** to view graph of network traffic volume.

Speed



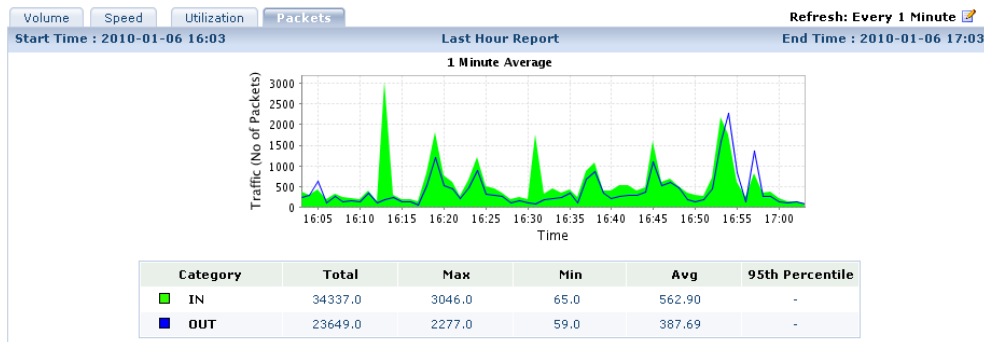
Click on the tab **Speed** to view graph of network traffic volume.

Utilization



Click on the tab **Utilization** to view graph of network traffic volume.

Packets

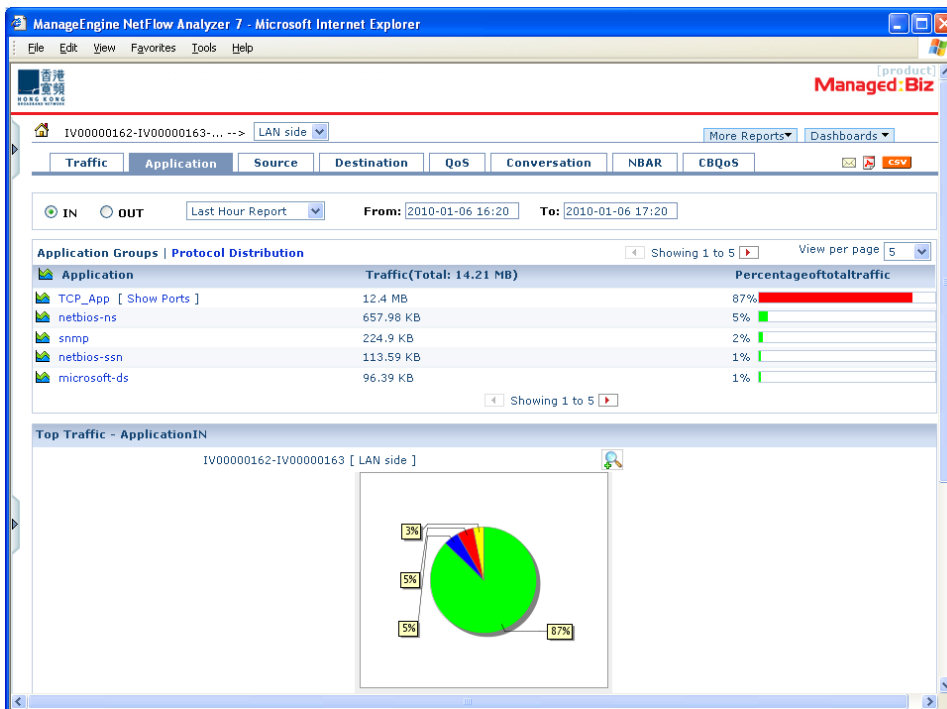


Click on the tab **Packets** to view graph of network traffic volume.

4.2. Application

The **Application** tab shows you the top applications and top protocols for the selected time period. The default view shows the **Top Application IN Report**. This report shows the distribution of incoming traffic application-wise.

Choose **IN** or **OUT** to display the application-wise distribution of incoming or outgoing traffic respectively.

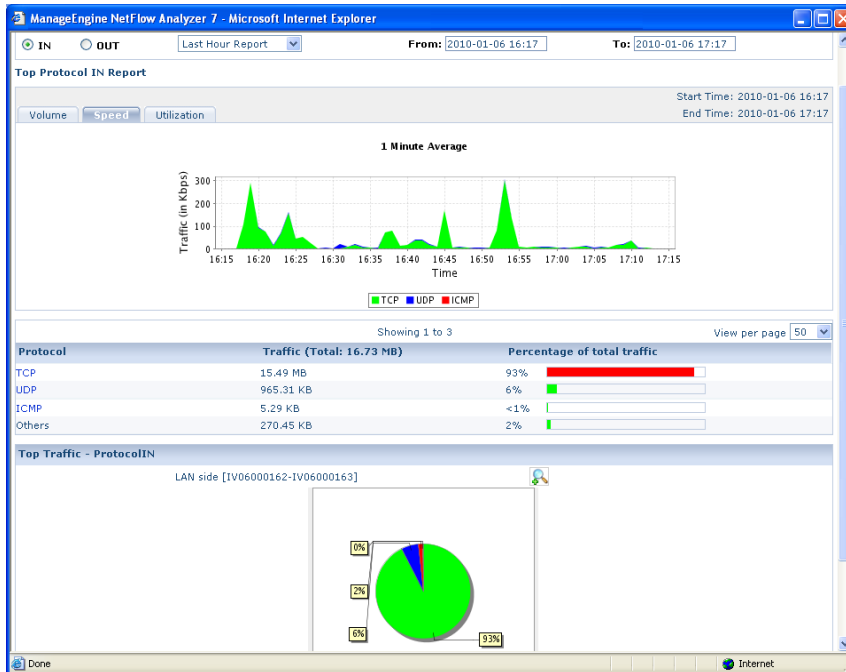


The table shows the distribution of traffic per application. You can see the traffic of each application, and how much of the total bandwidth was occupied by that application.

The pie chart shows the percentage of bandwidth used by each application.

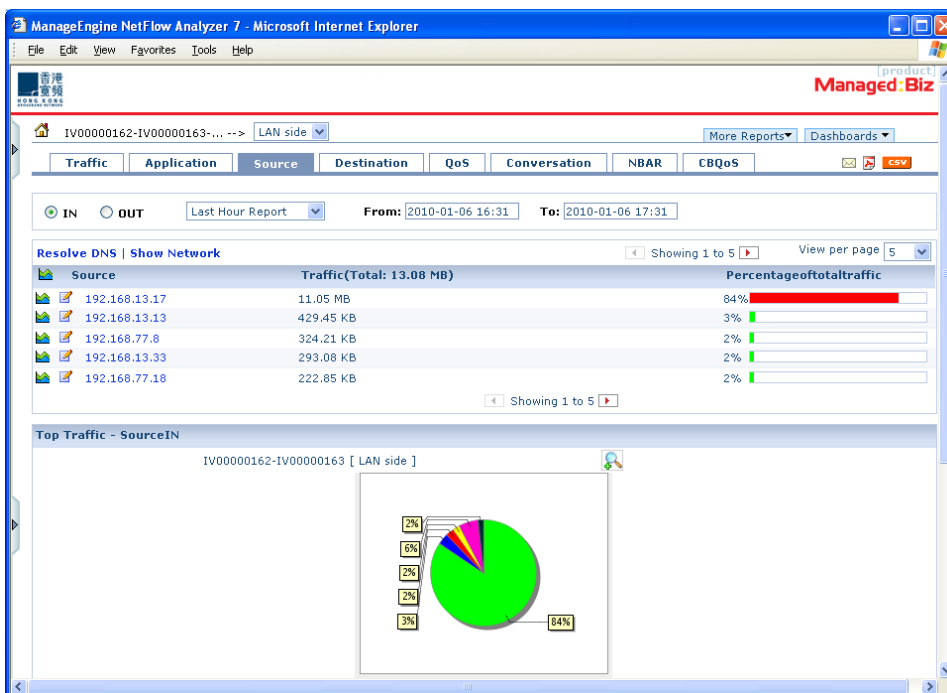
To view top protocols

Click the **Protocol Distribution** link to see the top protocols for the selected interface or IP group, in a new window. Choose **IN** or **OUT** to display the protocol-wise distribution of incoming or outgoing traffic respectively.



4.3. Source

The **Source** tab shows the top source hosts contributing to traffic in the selected time period. The default view shows the **Top Source IN Report**. Choose **IN** or **OUT** to display the top hosts of incoming or outgoing traffic.

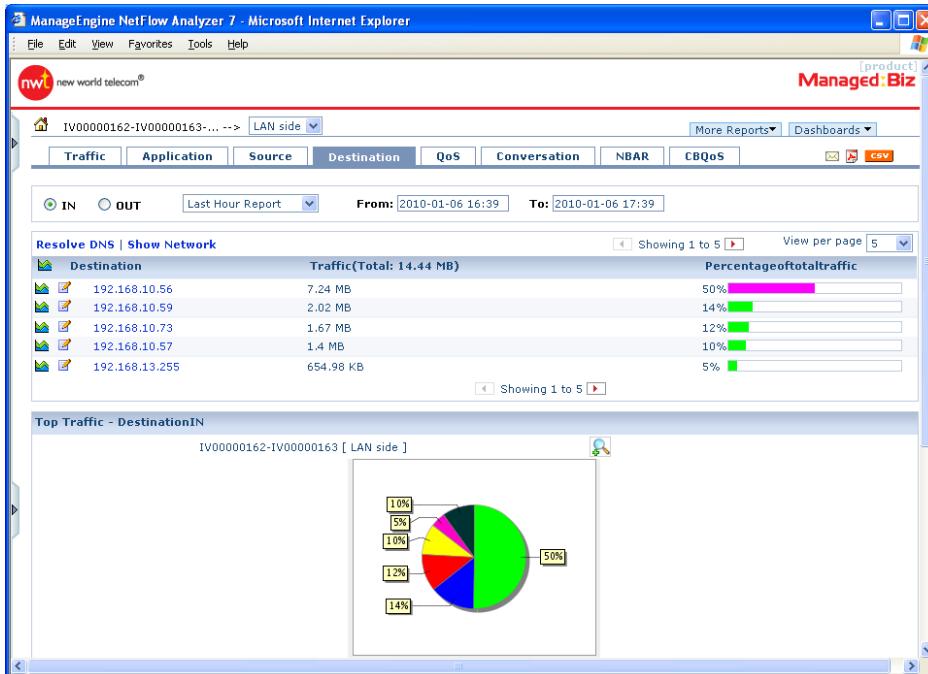


The default report view shows the IP addresses of the hosts. Click the **Resolve DNS** link to see the corresponding DNS values.

Click the **Show Network** link to see the network-wise top sources and destinations.

4.4. Destination

The **Destination** tab shows the top destination hosts contributing to traffic in the selected time period. The default view shows the **Top Destination IN Report**. Choose **IN** or **OUT** to display the top hosts of incoming or outgoing traffic.

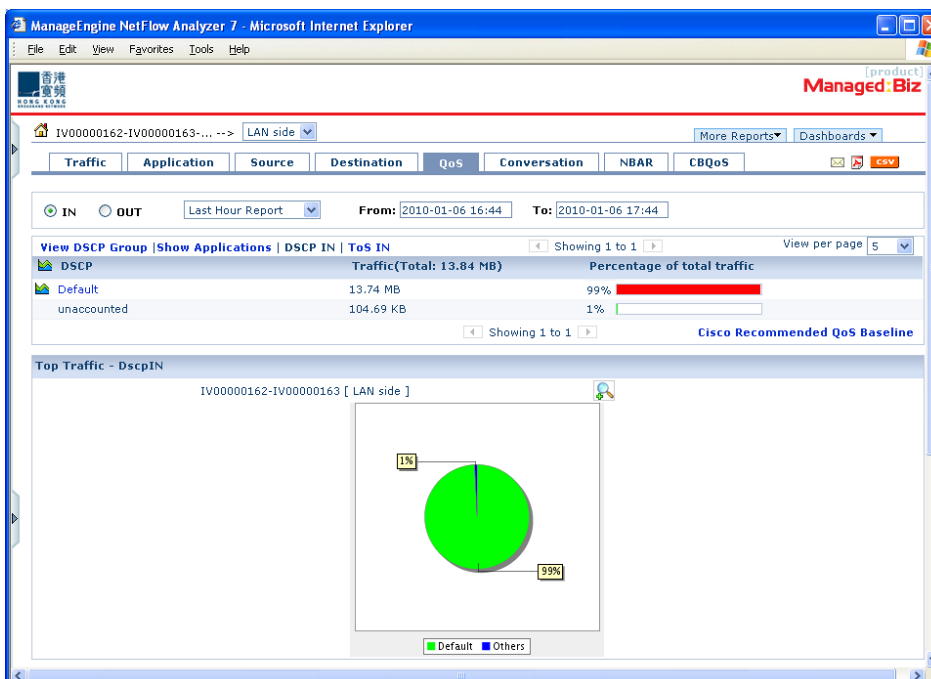


The default report view shows the IP addresses of the hosts. Click the **Resolve DNS** link to see the corresponding DNS values.


Click the **Show Network** link to see the network-wise top sources and destinations.

4.5. QoS

QoS or Quality of service is the most important factor that determines how effective the available enterprise bandwidth is being used in the WAN. It is also an index of the overall User Experience of the available Bandwidth. Choose **IN** or **OUT** to display the top DSCP IN or OUT Report.

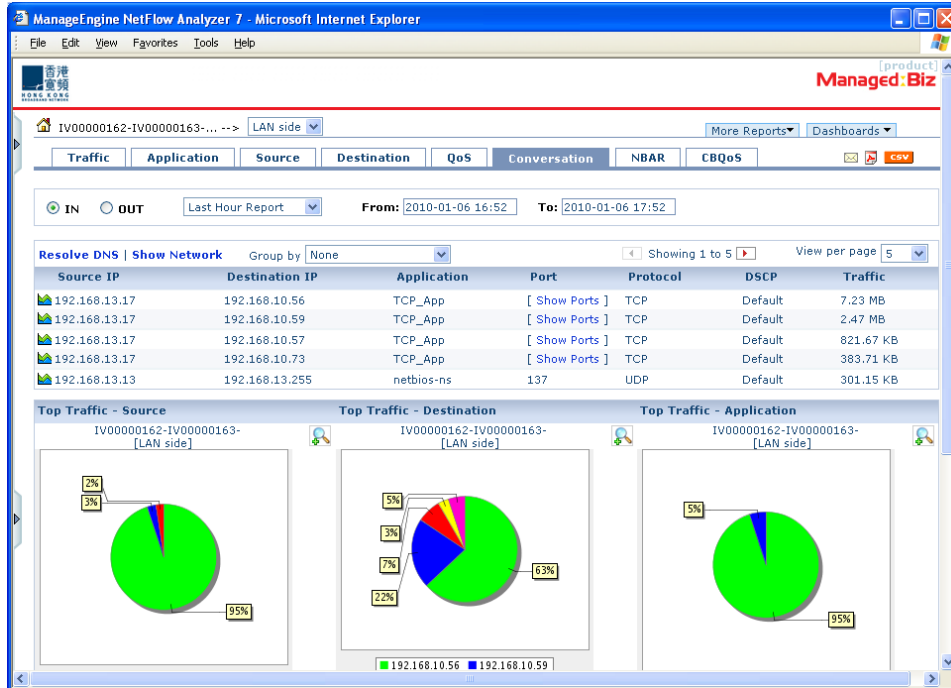


Click the **Show Applications** link to list out the various DSCP values along with the list of applications that comprise the DSCP. It also lists out details on Traffic and percentage utilization of the total traffic by each of the applications and the DSCP group as a whole.

Click the  icon next to the DSCP value for a detailed traffic graph in a pop-up window.

4.6. Conversation

The **Conversation** tab shows the top conversations contributing to traffic in the selected time period. Choose **IN** or **OUT** to display the top conversations of incoming or outgoing traffic.



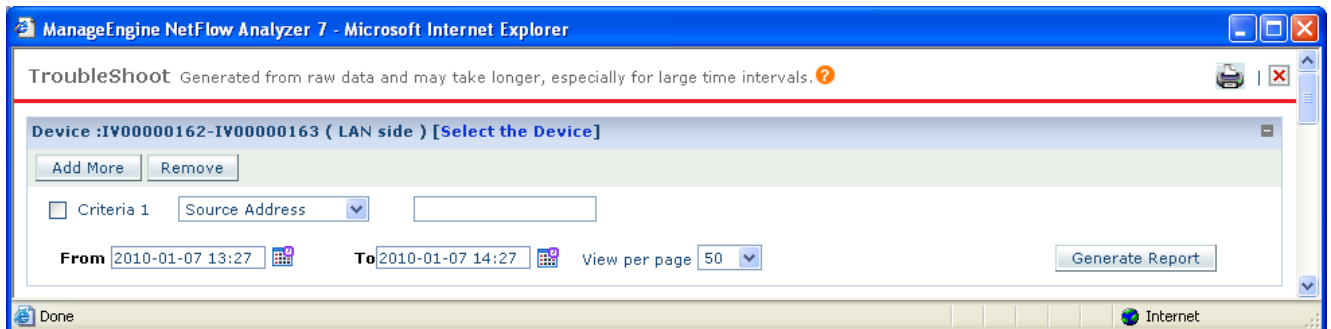
The pie charts below this report show the top sources, destinations, and conversations contributing to traffic for the selected time period.

5. More Reports

5.1. TroubleShoot Reports

The **TroubleShoot** link allows you to set criteria and view specific details about the traffic across a single interface. Data for Troubleshooting Reports is taken directly from raw data. Which means that Troubleshooting Reports will be available only for the maximum time period of 1 day.


Click the **TroubleShoot** link under **More Reports** in the detailed traffic report view. Or click the  icon against an interface on the Interface View.



Click the **Select the Devices** link to change the interface that you want to troubleshoot.

Under Search Criteria, enter the criteria on which traffic needs to be filtered. You can enter any of the following criteria to filter traffic:

- Source/Destination Address
- Source/Destination Network
- Source/Destination Nodes
- Application
- Port/Port Range

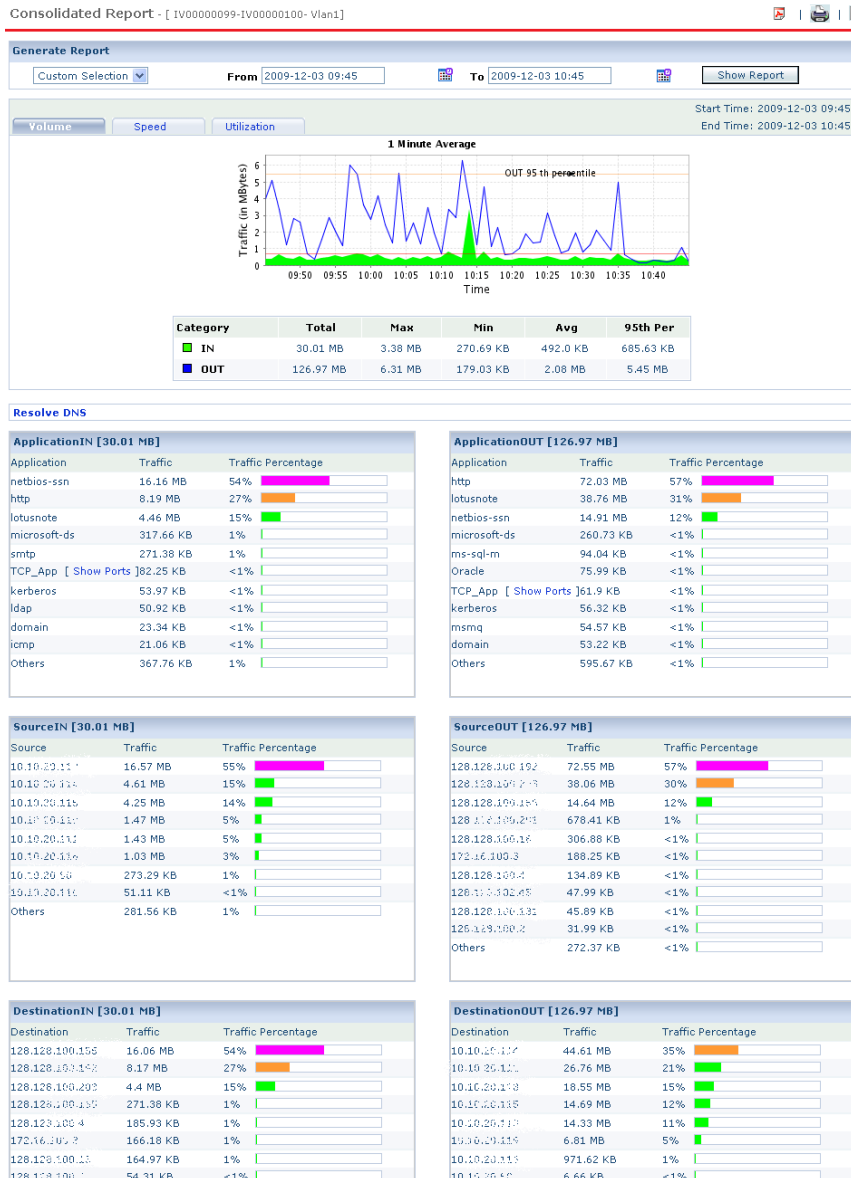
The **From** and **To** boxes allow you to choose specific time periods for the report. You can click the  icon to select the date and time. You should ensure that the time period selected falls within the Raw Data Retention Period of 1 day, otherwise no data will be shown in the graphs.

Once you have set all the desired criteria, click the **Generate Report** button to display the corresponding traffic report.

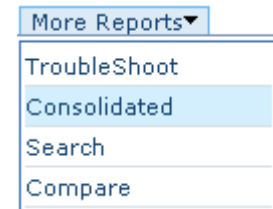
The default report view shows the IP addresses of the hosts. Click the **Resolve DNS** link to see the corresponding DNS values.


5.2. Consolidated Reports

Consolidated Reports allow you to see all the traffic details for an interface or IP group at one glance.




Click the **Consolidated** link under **More Reports** in the detailed traffic report view.



The same report can be accessed from the Interface View when clicking the  icon against an interface or IP group.

The **Custom Selection** box allows you to select different time periods for the traffic data.

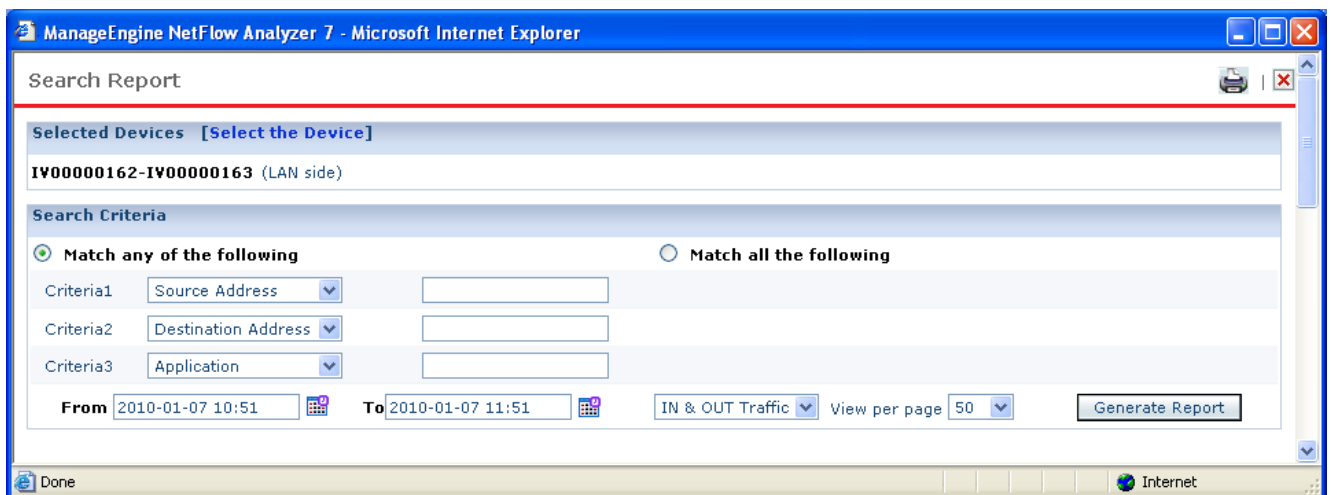
- The 1 Hour Report and 1 Day Report options show you the traffic details over the past one hour and one day respectively.
- The 8AM to 8PM option shows you the traffic details from 8 a.m. to 8 p.m. of the previous day. This is a peak hour report, based on the normal working hours of an enterprise.

Apart from these options, the **From** and **To** boxes allow you to choose specific time periods for the report. You can click the  icon to select the date and time. Once you have set the desired time period, click the **Show Report** button to display the corresponding consolidated report.

The default report view shows the IP addresses of the hosts. Click the **Resolve DNS** link to see the corresponding DNS names.

5.3. Search Reports


The **Search Reports** allow you to set several criteria and view specific reports. This is especially useful in finding out the bandwidth utilization of a specific host or application. Custom reports can also show the details about a certain application and which hosts are using the application, thereby helping to troubleshoot, and even detect virus activities. Click **Search** under **More Reports** in an Interface View or in detailed traffic report view.



Upon clicking the **Search** link, a pop-up window comes up. In the pop-up window, click the **Select the Device** link to choose the interfaces on which the report should be generated.

Under **Search Criteria**, enter the criteria on which traffic needs to be filtered. You can enter any of the following criteria to filter traffic:

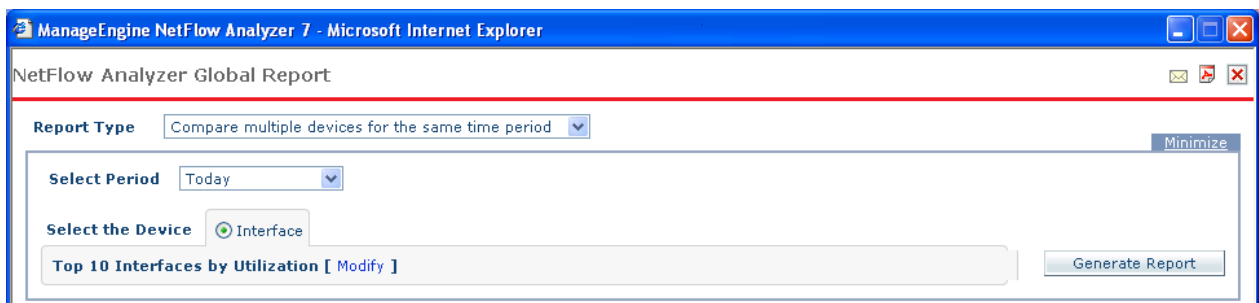
- Source/Destination Address
- Source/Destination Network
- Source/Destination Nodes
- Application
- Port/Port Range

The **From** and **To** boxes allow you to choose specific time periods for the report. You can click the  icon to select the date and time. Use the **IN/OUT** box to display values based on IN traffic, OUT traffic, or both IN and OUT traffic. The **View per page** lets you choose the number of results to display.

Once you have set the desired criteria, click the **Generate Report** button to display the corresponding traffic report. The default report view shows the IP addresses of the hosts. Click the **Resolve DNS** link to see the corresponding DNS values.

5.4. Compare Reports

Compare devices feature lets the user compare multiple devices for the same time period or compare the same device over different time periods. Click **Compare** under **More Reports** in an Interface View or in detailed traffic report view.



Field	Purpose/Description
Report Type	The report type could be: <ul style="list-style-type: none"> Compare multiple devices over the same time period; or Compare same device over different time periods
Select Period	When the Report Type is chosen as - <i>Compare multiple devices over the same time period</i> , the available Periods are <i>Last Hour, Last 6 Hour, Today, Last 24 Hours, Yesterday, Last Week, Last Month, Last Quarter</i> and <i>Custom Selection</i> . Custom Selection allows users to get the report of a specified time period. When the Report Type is chosen as - <i>Compare same device over different time periods</i> , the available Periods are <i>Every Day Report, Every Hour Report, Every Week Report</i> and <i>Every Month Report</i> .
Select Device(s)	This allows the user to select the device (if the same device is to be compared over various time periods) or the set of devices (that are to be compared for a single time period). The Select Devices option allows the user to select the devices in terms of Interface or IP Group which can be modified by clicking the Modify button (by default the top 10 interfaces or IP Group by utilization are chosen).
Generate Report	The Generate Report invokes the report of defined criteria. The Report Options could be: <ul style="list-style-type: none"> Show Speed; Show Utilization; or Show Packets
Maximize	When the Generate Report option is invoked, the filter condition frame is minimized to offer a better view of the graph (report) without scrolling. The filter frame can be restored by clicking the Maximize button.
Minimize	The Minimize button can be used to minimize the filter frame for a better view of the report (graph) generated without scrolling