Release Notes for EX Series Version 3.1

23 March 2011

Contents

1 Supported System Information

1.1 Hardware

This release supports the following EX Series models: EX 1000, EX 1100, EX 2100, EX 2110 and EX 2200. Refer to the included EX series documentation for detailed instructions on handling, installing, and configuring your hardware.

1.2 Software

EX Series operates with A10 Networks' Operating System and system software.

2 Upgrade Instructions

If you are using an earlier release version of EX Series software, upgrading is required.

Before upgrading from a prior version, you should backup your existing configuration.

To upgrade the system software:

1. Save the configuration and commit any unsaved changes in the running-config to the startup-config by entering the following command:

   write memory

2. Save a system backup to a remote server by entering the following command:

   backup startup-config *url*
   backup running-config *url*

   The URL can be one of the following:
   - **tftp:**//*host*/*file-name*
   - **ftp:**//**[***user***@]***host***[:***port***]**/*file-name*
   - **scp:**//**[***user***@]**host/*file-name*
   - **rcp:**//**[***user***@]***host*/*file-name*

   You can enter the entire URL on the command line or you can press Enter to display a prompt for each part of the URL. If you enter the entire URL and a password is required, you will be prompted for the password.

   You can enter a path name with the file name.

3. To install the new software image, enter the following command:

upgrade *url*

4. When the prompt appears, enter "yes" to proceed with the upgrade. Note that if the EX is upgraded, the EX will reboot upon completing the upgrade.

For examples, see the "System Upgrade" section in the "Quick Start" chapter of the *EX Series Secure WAN Manager CLI User Manual*.

3 Feature Summary

MODULE	FEATURE	DESCRIPTION
Load Balance	DNAT based on IP	The EX simplifies DNAT configuration and eliminates the use of QoS classes.
Network	IP Address Assignment from DHCP Server	EX interfaces support DHCP IP address assignments.
Network	Asymmetric Flows	The EX now supports asymmetric flows. Previous releases were unable to pass asymmetric traffic.
Network	Semi-session (Preserve pre-existing TCP sessions)	The EX allows traffic to pass through the appliance for TCP sessions started during bootup while the EX was in bypass mode.
Report	Abuser Report Enhancements	Separate reports can now be generated based on specific abuse criteria, rather than appearing in one global report.
Report	Archive Reports to Remote File Server	In addition to emailing reports, the EX now supports the ability to transmit reports using SCP, RCP, TFTP and FTP.
QoS	Enhanced Auto Created Classes	The EX can now Auto-Detect classes based on the IP Protocol such as ICMP and GRE. Users can set a limit on the number of classes created automatically to prevent the creation of an excessive number of Auto-Created classes.
QoS	Bandwidth Management and Reports by Category	Expands traffic shaping in a QoS policy to allow shaping based on QoS category. Adds reporting features based on QoS category.
Network	Improve Hardware Bypass	The hardware bypass feature now allows users to configure the EX appliance to enable hardware bypass whenever the EX is shutting down to minimize traffic interruption.

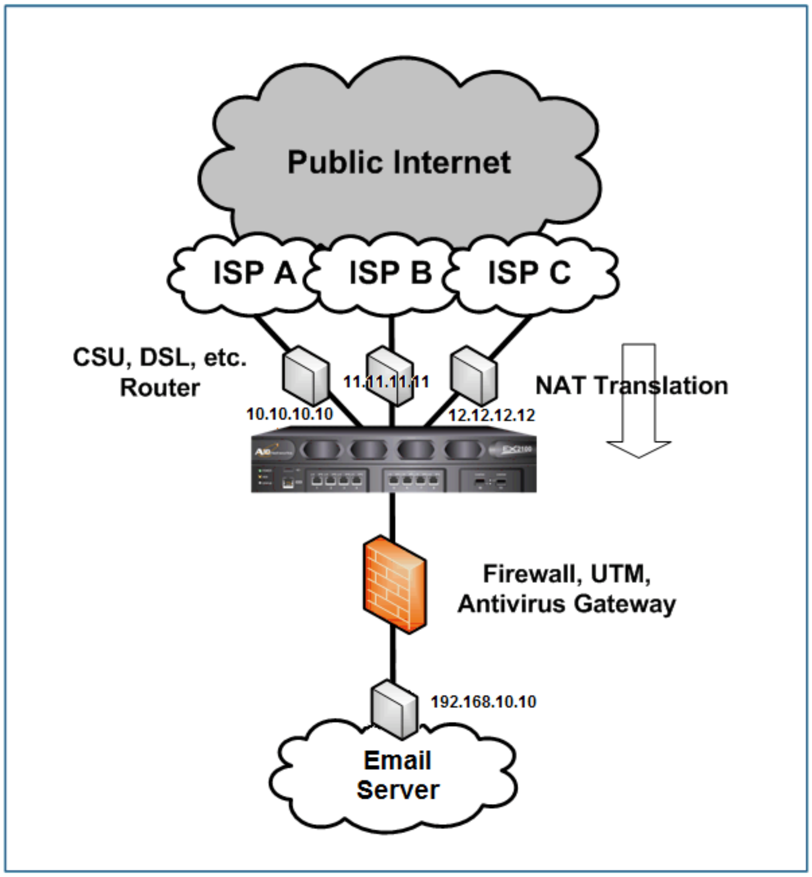
MODULE	FEATURE	DESCRIPTION
System	Enhancement of RADIUS Privilege Option	Enhance the RADIUS authentication to support write privilege of access control and primary and secondary RADIUS servers.
QoS	Easy QoS policy	Allows for Easy QoS policy creation by eliminating the QoS interface definition step.
QoS	L7 Based Rule Exception	Support the ability to define class rules with L7 protocol exception.
System	L7 signature updates	A separate L7 signature library has been created in order to support signature updates without interrupting current connections.
QoS	QoS Classification by DSCP	Enable the user to classify traffic based on DSCP values.
QoS	QoS Policy Action of Connection Limits	Limit the number of total or per-IP connections by defining the limit within the QoS policy.
Report	Report CSV Format	Supports CVS Format for generated reports.
Load Balance	SIP NAT ALG Support	Supports NAT ALG for SIP protocol.
QoS	TCP Window Adjustment	The EX device manages the traffic load of TCP sessions by adjusting the window size.
Health Monitor	Transparent health methods	A new health monitoring option allows a TCP health method to be used to check the health of a link.
Health Monitor	Multiple health methods	A health monitor can now include multiple health methods, rather than being limited to only one method per monitor.
Report	Enhanced Alert Content	Alerts content has been enhanced with correlated rate and connection information.
Report	Report generation progress bar	Web UI shows a progress bar (percent complete) when generating reports.
Report	Template and schedule CLI	Reporting CLI enhanced to allow the configuration of report templates and schedules.
System	New EX 1100 hardware model	Allow software to support a new hardware platform called EX 1100
QoS	L7 New and Enhanced Signatures	Supports new Layer 7 signatures for standard protocols and applications. Enhanced existing Layer 7 signatures.

4 Feature Details

4.1 DNAT Based on IP

DNAT based on IP is an enhancement of the current DNAT feature. While prior releases supported DNAT, the old implementation relied on QoS classes to identify traffic before it could be forwarded to an internal IP address, and there was no support for direct port mapping. Because users no longer need to set up a QoS class to use DNAT, QoS classes can be reserved for other uses. DNAT based on IP directly relates external IP addresses with an internal IP address in order to perform the destination NAT.

The figure below shows a sample DNAT configuration in which users can create a mapping between three external IP addresses (corresponding to three ISPs) and one internal IP address, for an email server that sits behind the corporate firewall. The *external* IP addresses (10.10.10.10, 11.11.11.11, and 12.12.12.12) are mapped to *internal* IP address 192.168.10.10.



Details:

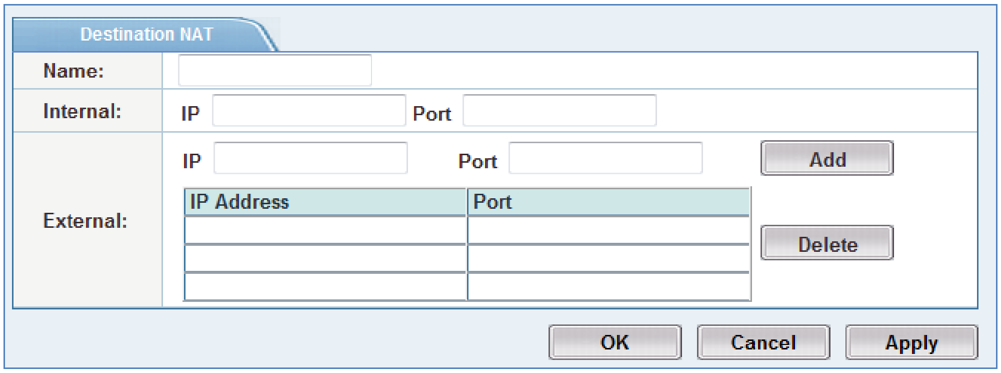
- The EX appliance can support up to 64 DNAT configurations.
- Each DNAT configuration can map up to 8 external IPs with 1 internal IP.

- The old approach of configuring DNAT based on QoS classes will be preserved in order to prevent legacy customers from having to switch to the new approach.
- Some customer may prefer to continue using QoS-Based DNAT, especially in situations where the customer would like to use the Exclude checkbox (located within the QoS Class configuration) to create exceptions for certain types of traffic.
- With the old QoS-Based approach to DNAT, users could select a preconfigured class, such as "aim". However, “aim” classification occurs at Layer 7 while the DNAT feature operates at Layer 4. Thus, the DNAT feature could only be used on Layer 4 classes. As a workaround to this limitation, users could manually create a class and populate it with targeted IP addresses. In contrast, the new approach to DNAT configuration essentially does the same thing as the old workaround, but it removes the requirement of having to create a QoS class within which to package IP addresses.

4.1.1 GUI Config

To configure IP-based DNAT on the EX appliance:

1. Select Config Mode > Load Balance > Destination NAT.
2. On the menu bar, select “Based on IP”, if not already selected.
3. Click the New button. A window similar to the one shown below appears:



4. Enter a name for the DNAT object in the Name field.
5. Enter the internal IP (and optionally, the port) where inbound traffic will be sent.
6. Enter the external IP (and optionally, the port) where inbound traffic will be sent to the internal IP address.
7. Click the Add button to add the mapping to the DNAT object.
8. Repeat the process of mapping external IPs to an internal IP for up to 8 external IPs.
9. Select OK or Apply to save your changes.

4.1.2 CLI Config

To create a new DNAT by IP object, use the following commands from the EX appliance CLI:

```
EX(config)#dnat ?
  name     DNAT private host name
  qos      The QoS class

EX(config)#dnat name test1 ?
  <cr>

EX(config-DNAT)#?
  ...
  external  Add external host IP address
  internal  Add internal host IP address
```

To configure the internal IP address to which external IP addresses will be mapped:

```
EX(config-DNAT#internal ip 10.10.10.10 ?
  port  Set internal host port
  <cr>
```

To configure the external IP address to which the internal IP addresses will be mapped:

```
EX(config-DNAT#external ip 20.20.20.20 port ?
  <0-65535>  Add external host port

EX(config-DNAT)#external ip 20.20.20.20 port 80
```

4.2 IP Address Assignment from DHCP Server

The EX now supports the ability to receive an IP address from an external DHCP server. The DHCP-assigned IP address can be assigned to the following types of interfaces:

- Physical interfaces
- Virtual Ethernet (VE) interfaces
- HA Virtual Group IP address

Details:

- IP address assignment to an interface may be static or dynamic, but not both.
- Default gateway, static routes, and DNS information may be used by the EX device and will automatically be applied to LLB links and/or routing tables.
- Unavailable gateway information will be indicated in the log.

4.2.1 CLI Config

This feature uses the following new CLI commands:

- `ip address dhcp`
- `renew`

```
EX(config-if:ethernet3)#ip ?
address    Set the IP address of an interface
nat        Enable nat support
ospf       OSPF
renew      Renew IP
rip        RIP

EX(config-if:ethernet3)#ip address ?
A.B.C.D         IP address
dhcp            Get the ip and network info from DHCP server

EX(config-if:ethernet3)#ip address dhcp ?
options         Accept the options from DHCP server
  <cr>

EX(config-if:ethernet3)#ip renew ?
  <cr>
```

To configure an interface to receive its IP address from DHCP:

```
EX(config-if:ethernet3)#ip address dhcp
```

To also receive options, including the default gateway and DNS server addresses:

```
EX(config-if:ethernet3)#ip address dhcp options
```

To verify the results of the commands above:

```
EX(config-if:ethernet3)#show interfaces ethernet 3
Ethernet3 is up, line protocol is up
  Hardware is Ethernet, address is 001F.A010.031C
  Internet address is 192.168.100.210/24, broadcast is 192.168.100.255
. . .
```

Details:

- The **`ip renew`** command only applies to an IP address acquired from DHCP.
- If the **`ip dhcp`** command is used, the EX will not accept any options from the DHCP server.
- If the **`ip dhcp options`** command is used, the EX will accept the options from the DHCP server.
- The CLI commands for assigning an IP address to a VE or to an HA Virtual Group are similar to those described above for configuring physical Ethernet interfaces.

(Optional) Configure DHCP IP Source NAT

You can use the following CLI commands to specify source NAT without an IP Pool. The EX will use the same DHCP-assigned IP address for the source NAT IP Pool.

The following command tells the EX to use source NAT, even if no IP Pool has been specified. (Traffic output from ethernet 3 will do Source NAT with IP address 192.168.100.210)

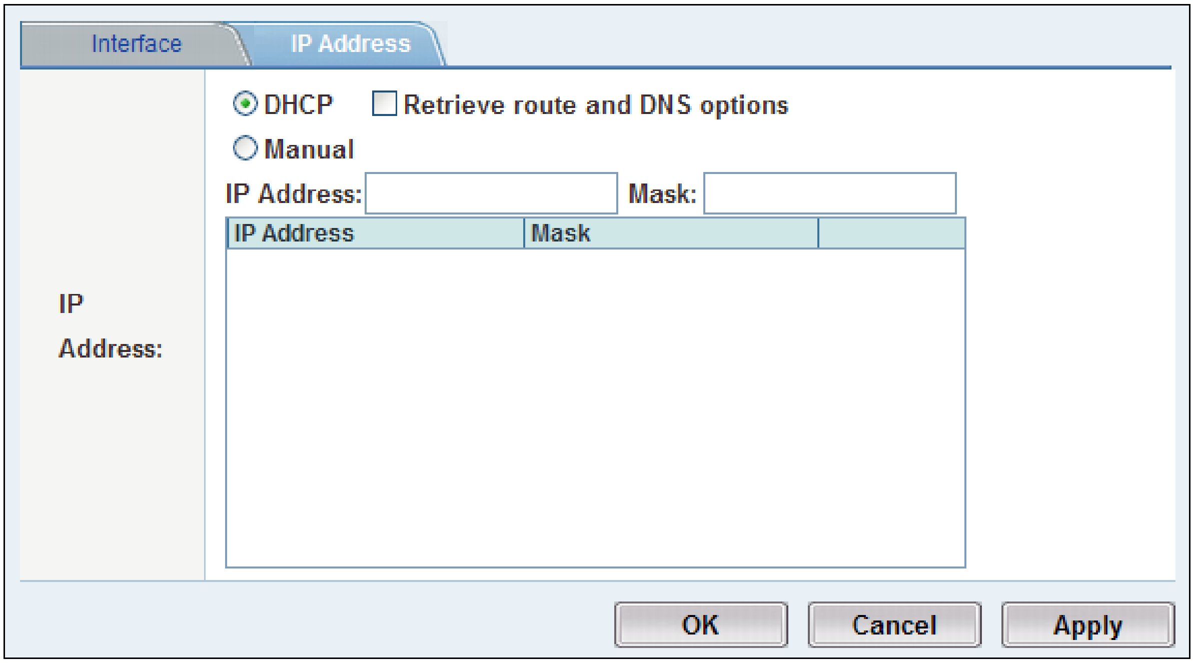
To enable support for NAT for DHCP:

```
EX(config-if:ethernet3)#ip nat
```

4.2.2 GUI Config

To configure the EX to accept an IP address from a DHCP server on a physical interface or VE:

1. Select Config > Network > Interface, if not already selected.
2. On the menu bar, select Interface.
3. Select the hyperlink for the desired physical or VE interface from the Interface column.
4. Select the IP Address tab to display the following screen.



IP Address:

● DHCP ☐ Retrieve route and DNS options

○ Manual

IP Address: Mask:

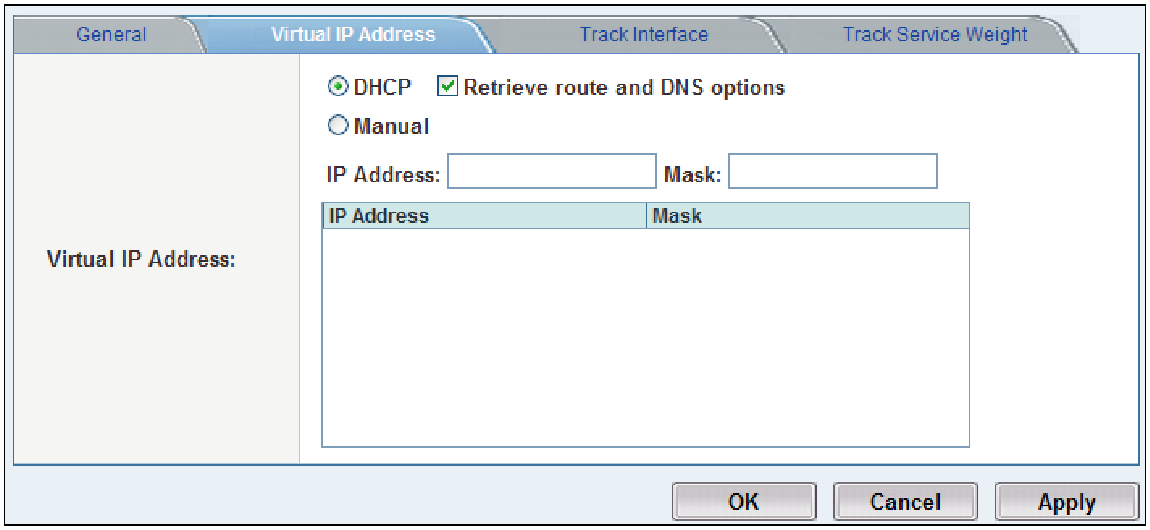
IP Address	Mask	

5. Select the DHCP radio button to receive an IP address.
6. Optionally, you can select the Retrieve route and DNS options checkbox to retrieve information about the routers, static-routes, domain-name, and domain-name-servers when the new IP address is assigned.
7. Click OK to save your changes.

To verify that the IP Address was correctly assigned, redisplay the Interface table or navigate to the IP address tab for the interface.

To configure the EX device to accept an IP address from a DHCP server on an HA Virtual Group:

1. Select Config > HA > Virtual Group, if not already selected.
2. On the menu bar, select Virtual Group.
3. Select the desired Virtual Group hyperlink from the Virtual Group ID column, or click the New button.
4. Select the Virtual IP Address tab to display the following screen.



Virtual IP Address:

● DHCP ☑ Retrieve route and DNS options

○ Manual

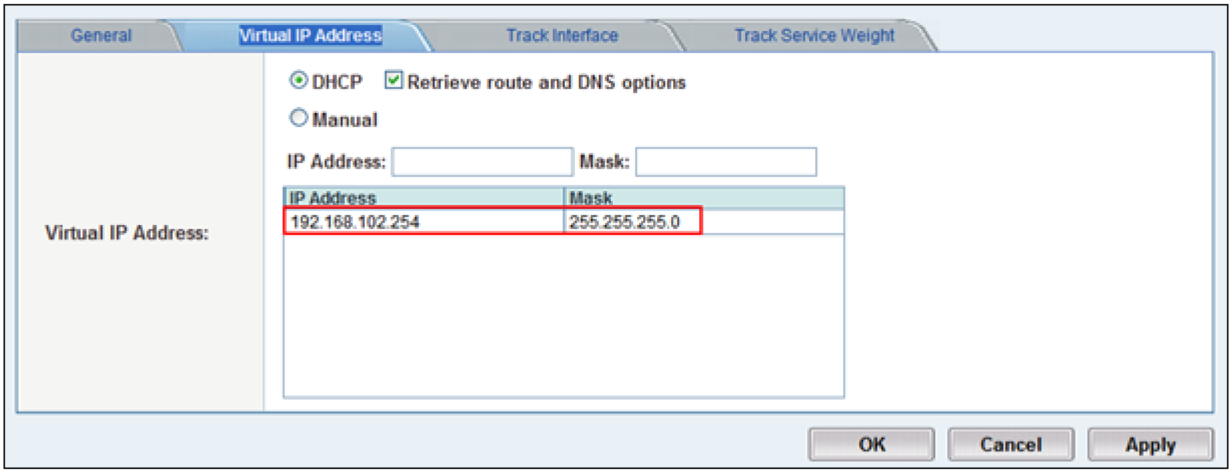
IP Address: Mask:

IP Address	Mask

5. Select the DHCP radio button to receive an IP address.
6. Optionally, you can select the Retrieve route and DNS options checkbox to retrieve information about the routers, static-routes, domain-name, and domain-name-servers when the new IP address is assigned.
7. Click OK to save your changes.

To verify that the IP Address was correctly assigned:

1. Select Config > HA > Virtual Group, if not already selected.
2. On the menu bar, select Virtual Group.
3. Select the desired Virtual Group hyperlink from the Virtual Group ID column.
4. Select the Virtual IP Address tab to display the following screen:



Virtual IP Address:

● DHCP ☑ Retrieve route and DNS options

○ Manual

IP Address: Mask:

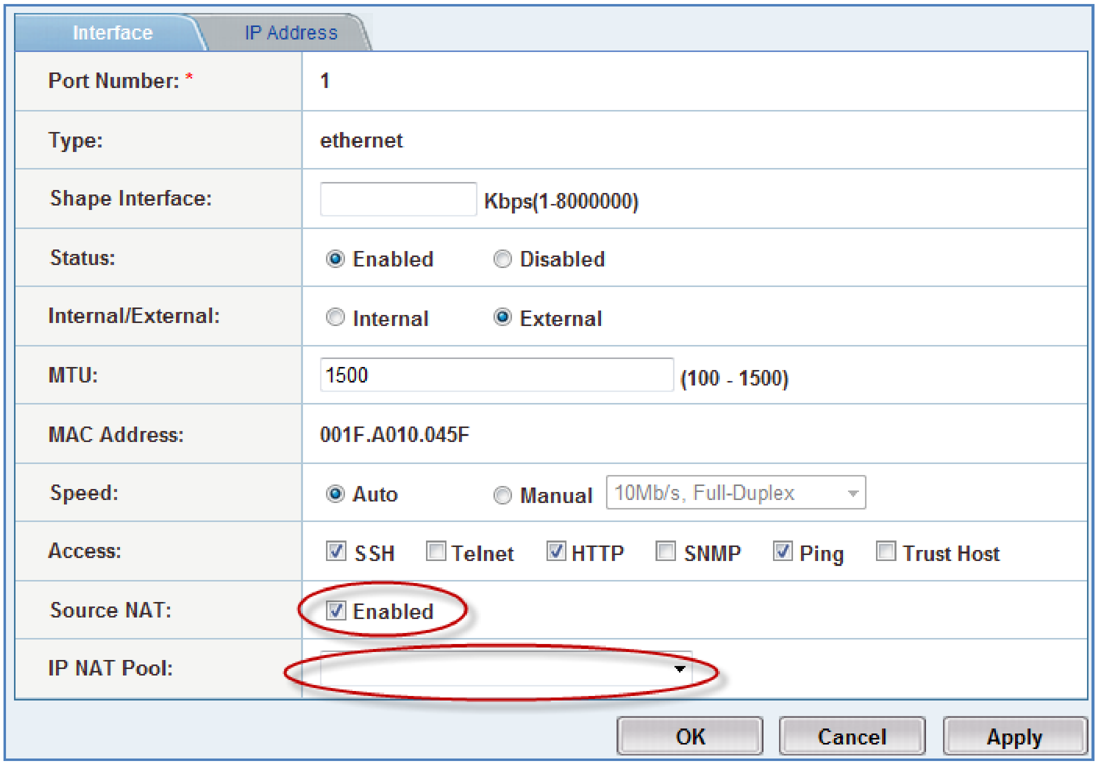
IP Address	Mask
192.168.102.254	255.255.255.0

The Virtual Group IP Address and Mask appear, as shown in the screenshot above.

(Optional) Configure DHCP IP Source NAT

To enable NAT without IP Pool:

1. Select Config Mode > Network > Interface.
2. Select Interface from the menu bar, if not already selected.
3. Select the desired hyperlink from the Interface column (e.g. ethernet1).
   A window similar to the one shown below appears:



Port Number: *	1
Type:	ethernet
Shape Interface:	Kbps(1-8000000)
Status:	● Enabled ○ Disabled
Internal/External:	○ Internal ● External
MTU:	1500 (100 - 1500)
MAC Address:	001F.A010.045F
Speed:	● Auto ○ Manual 10Mb/s, Full-Duplex
Access:	☑ SSH □ Telnet ☑ HTTP □ SNMP ☑ Ping □ Trust Host
Source NAT:	☑ Enabled
IP NAT Pool:	

4. Select the Source NAT checkbox, as shown above.
5. Leave the IP NAT Pool drop-down menu blank.
6. Select OK or Apply to save your changes.

4.3 Asymmetric Flows

Asymmetric routing occurs when packets take a path through the network from host A to host B and then uses a different path to return from host B back to host A. In prior releases, asymmetric TCP sessions were not supported and the EX required TCP traffic between host A and host B (in both directions) to pass through the EX. This feature is enabled by default.

Note: Asymmetric flows may have trouble being properly classified by classes that rely on L7 protocols for their match criteria because the EX only has traffic visibility in one direction.

4.3.1 GUI Config

N/A – Feature cannot be configured via GUI.

4.3.2 CLI Config

By default, asymmetric routing is enabled. To disable asymmetric routing on the EX device, use the following command:

```
EX(config)#no flow asymmetric
```

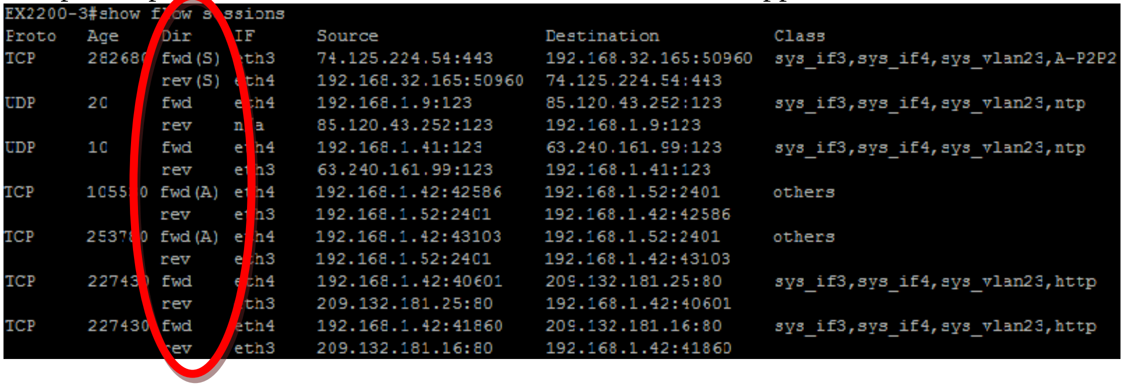
To re-enable asymmetric routing on the EX device, use the `flow asymmetric` command:

```
EX(config)#flow asymmetric
```

To display session information for asymmetric sessions, semi-sessions, or normal sessions, use the following command:

```
EX(config)#show flow sessions
```

Sample output for the **`show flow sessions`** command appears below:



```
EX2200-3#show flow sessions
Proto   Age     Dir     IF      Source               Destination          Class
TCP     282680  fwd(S)  eth3    74.125.224.54:443    192.168.32.165:50960 sys_if3,sys_if4,sys_vlan23,A-P2P2
                rev(S)  eth4    192.168.32.165:50960 74.125.224.54:443
UDP     20      fwd     eth4    192.168.1.9:123      85.120.43.252:123    sys_if3,sys_if4,sys_vlan23,ntp
                rev     n/a     85.120.43.252:123    192.168.1.9:123
UDP     10      fwd     eth4    192.168.1.41:123     63.240.161.99:123    sys_if3,sys_if4,sys_vlan23,ntp
                rev     eth3    63.240.161.99:123    192.168.1.41:123
TCP     105510  fwd(A)  eth4    192.168.1.42:42586   192.168.1.52:2401    others
                rev     eth3    192.168.1.52:2401    192.168.1.42:42586
TCP     253780  fwd(A)  eth4    192.168.1.42:43103   192.168.1.52:2401    others
                rev     eth3    192.168.1.52:2401    192.168.1.42:43103
TCP     227430  fwd     eth4    192.168.1.42:40601   209.132.181.25:80    sys_if3,sys_if4,sys_vlan23,http
                rev     eth3    209.132.181.25:80    192.168.1.42:40601
TCP     227430  fwd     eth4    192.168.1.42:41860   209.132.181.16:80    sys_if3,sys_if4,sys_vlan23,http
                rev     eth3    209.132.181.16:80    192.168.1.42:41860
```

Note that the third column from the left, (entitled “Dir”) lists the direction of the session (forward or reverse). A letter appears in parentheses, indicating that the session is one of the following session types:

- A – Asymmetric session
- S – Semi-session (discussed in section 4.4)
- Absence of “A” or “S” means the session is a normal session

Instead of displaying all sessions together, you can choose to display only the asymmetric sessions using the following command:

```
EX(config)#show flow sessions asymmetric
```

You can display the number of currently active sessions (asymmetric and others) using the following command:

```
EX(config)#show flow counters
```

4.4 Semi-session (Preserve pre-existing TCP sessions)

The semi-session feature preserves previously-created TCP sessions while the EX device is booting up for a period of time. In prior releases, the EX would drop packets for which it could not see the full TCP handshake. These dropped packets would, in turn, cause the associated TCP sessions to be dropped.

By default, the semi-sessions will last for a period of 5 minutes. When this period ends, semi-session traffic will be dropped. This interval can be modified as needed.

4.4.1 GUI Config

N/A – Feature cannot be configured via GUI.

4.4.2 CLI Config

To modify the time interval for the semi-session feature, use the following CLI command:

```
EX(config)# flow semi-session timeout ?
  <0-60>  Timeout in minutes (0: always enabled)
```

To disable support for passing traffic with no session, use the following command:

```
EX(config)# no flow semi-session
```

To display flows that do not have a session, use the following command:

```
EX(config)# show flow sessions semi-session
```

To display the number of sessions marked with “semi-session”, use the following command:

```
EX(config)# show flow sessions counters
```

4.5 Abuser Report Enhancements

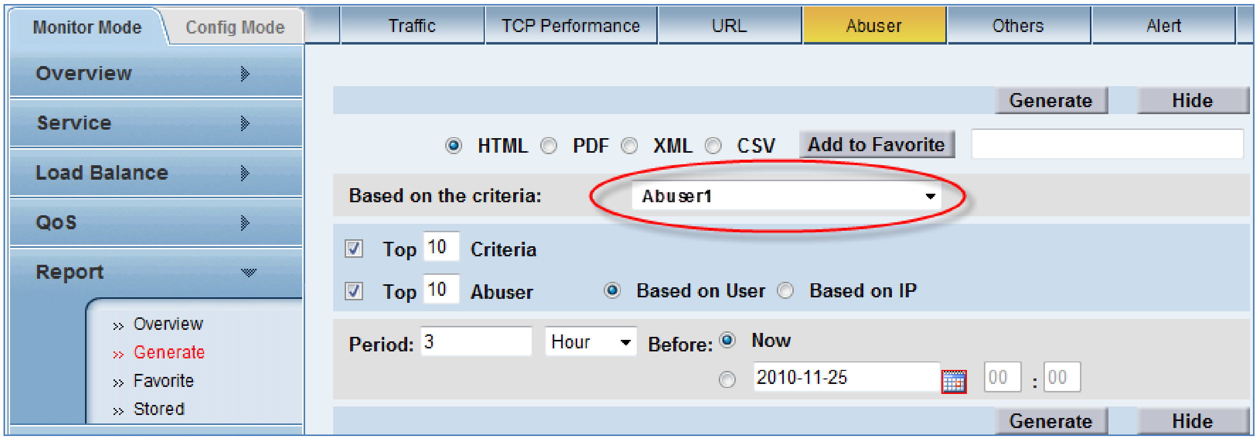
Abuser Reports enhancements list:

- While prior releases offered a single global report, which contained information that was frequently unrelated, this latest release allows the user to create separate reports based on specific abuser criteria.
- Abuser logs are separated from system logs to prevent the system logs from being flooded.
- The administrator will now have the option to search and filter abuser logs based on string.

4.5.1 GUI Config

To generate a report from the EX appliance based on a specific Abuser Criteria:

1. Select Monitor Mode > Report > Generate.
2. On the menu bar, select Abuser, if not already selected.
   A window similar to the one shown below appears:



● HTML ○ PDF ○ XML ○ CSV

Based on the criteria: Abuser1

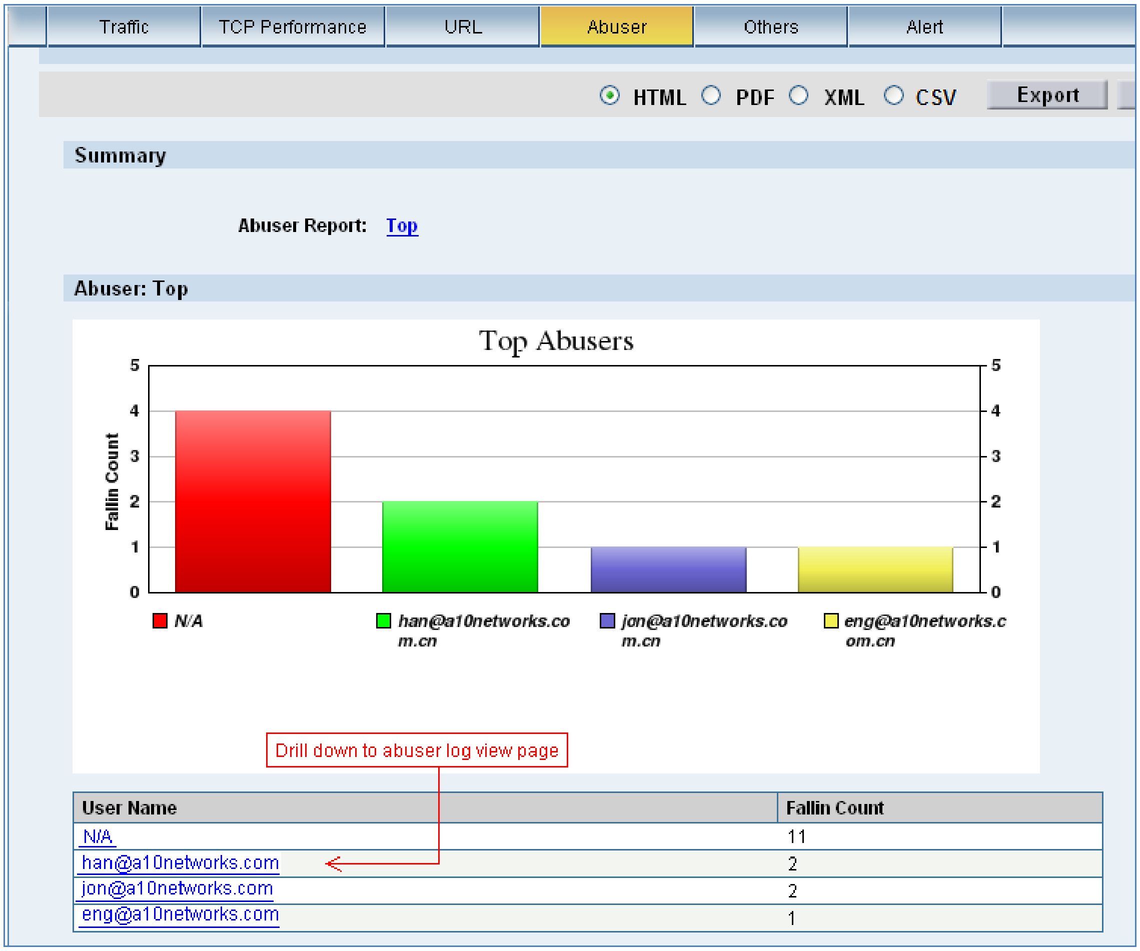
☑ Top 10 Criteria

☑ Top 10 Abuser ● Based on User ○ Based on IP

Period: 3 Hour Before: ● Now

○ 2010-11-25 00 : 00

3. Click the Based on the criteria drop-down menu and select an existing Abuser Criteria.
   - By default, this field is blank, in which case the generated report will be based on the global scope.
   - If you select "example_criteria" the generated abuser report will be based on the associated rules.
   - To create a new set of Abuser Criteria, select Config Mode > QoS > Class, select Abuser Criteria from the menu bar, and then clicking the New button and configuring the period, scope, and Fall In/Fall Out criteria.
4. Click the Generate button to create the report based on Abuser Criteria.
5. Once the report is generated, a window similar to the one shown below appears:



Summary

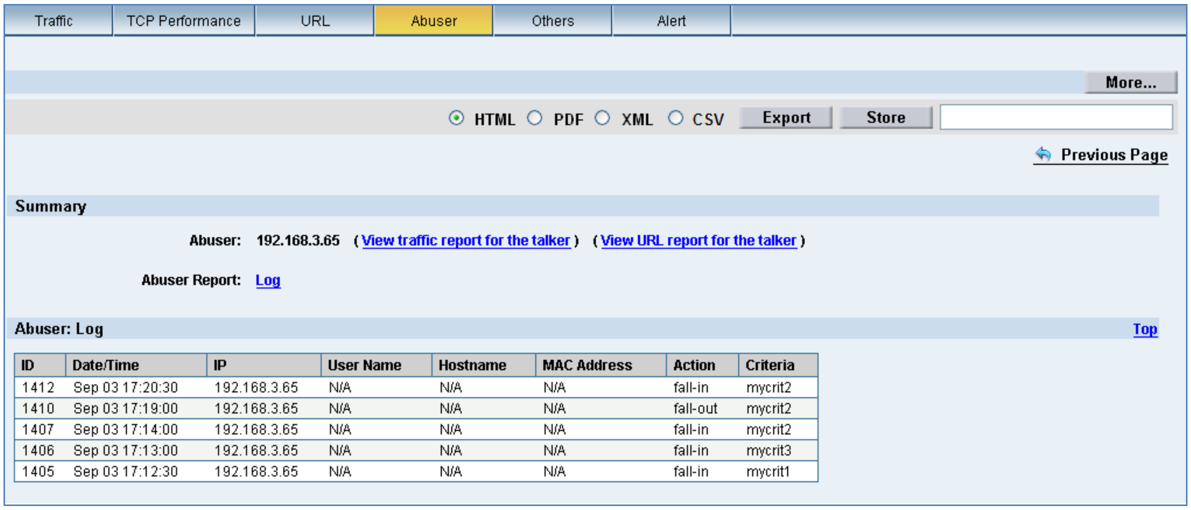
Abuser Report: Top

Abuser: Top

Drill down to abuser log view page

User Name	Fallin Count
N/A	11
han@a10networks.com	2
jon@a10networks.com	2
eng@a10networks.com	1

6. Optionally, click a user name or IP to display information from the abuser logs page.
7. Optionally, click View Traffic Report for the Talker to display the traffic report page.



Summary

Abuser: 192.168.3.65 (View traffic report for the talker) (View URL report for the talker)

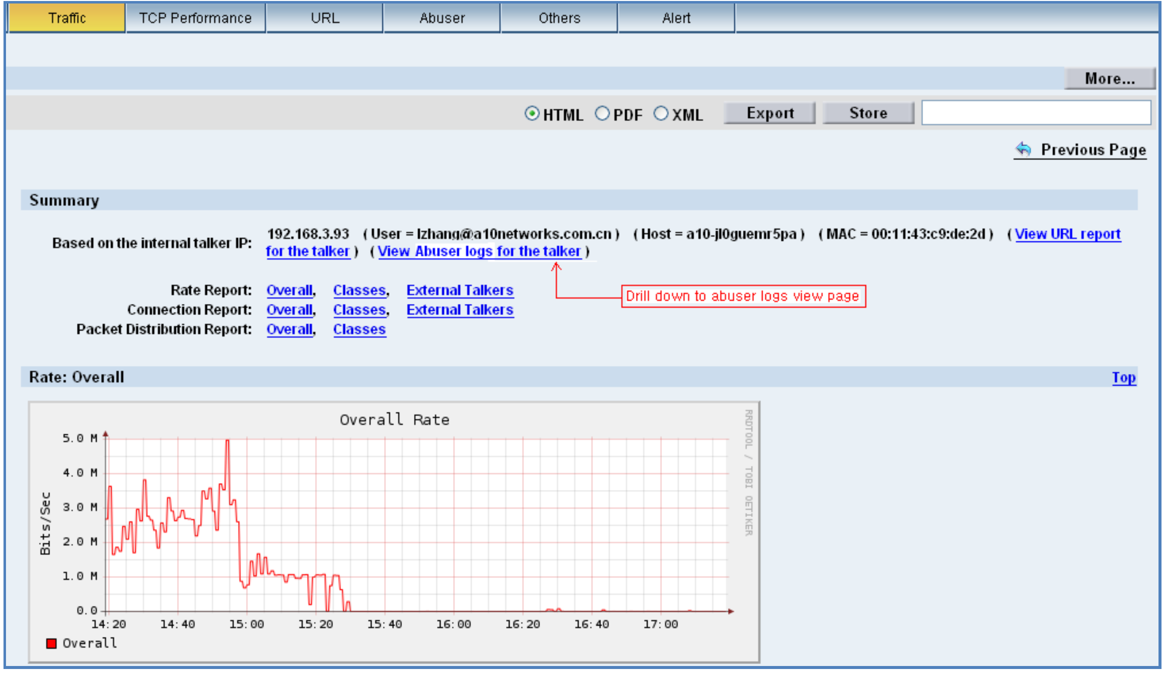
Abuser Report: Log

Abuser: Log Top

ID	Date/Time	IP	User Name	Hostname	MAC Address	Action	Criteria
1412	Sep 03 17:20:30	192.168.3.65	N/A	N/A	N/A	fall-in	mycrit2
1410	Sep 03 17:19:00	192.168.3.65	N/A	N/A	N/A	fall-out	mycrit2
1407	Sep 03 17:14:00	192.168.3.65	N/A	N/A	N/A	fall-in	mycrit2
1406	Sep 03 17:13:00	192.168.3.65	N/A	N/A	N/A	fall-in	mycrit3
1405	Sep 03 17:12:30	192.168.3.65	N/A	N/A	N/A	fall-in	mycrit1

8. To return to the Abuser Report window, click the Previous Page link (at upper right).

9. To display the logs view, click the View Abuser Logs for the Talker link, as shown below:



Summary

Based on the internal talker IP: 192.168.3.93 (User = lzhang@a10networks.com.cn) (Host = a10-jl0guemr5pa) (MAC = 00:11:43:c9:de:2d) (View URL report for the talker) (View Abuser logs for the talker)

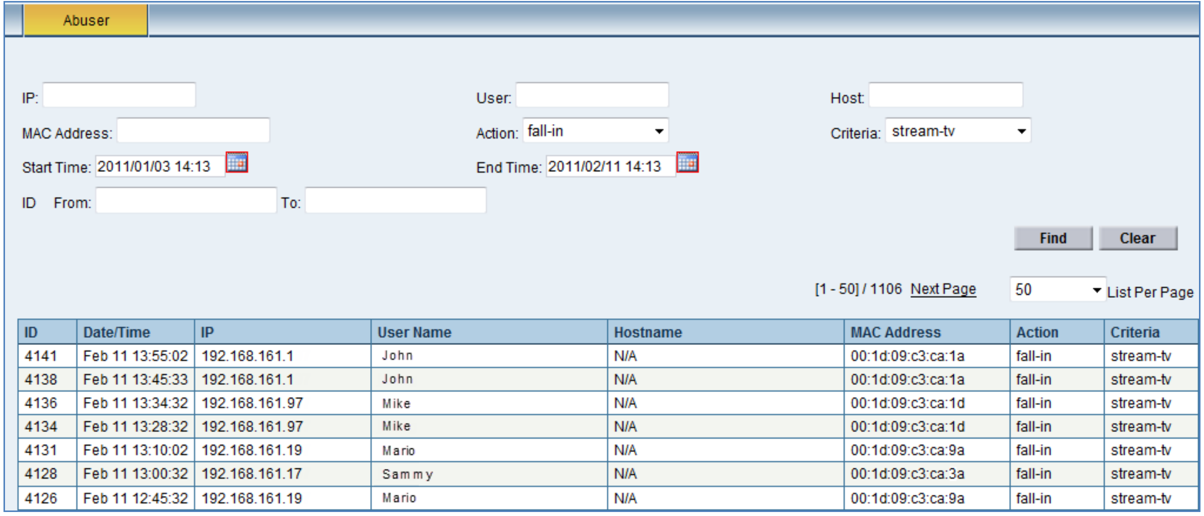
Drill down to abuser logs view page

Rate Report: Overall, Classes, External Talkers
Connection Report: Overall, Classes, External Talkers
Packet Distribution Report: Overall, Classes

Rate: Overall

As an additional enhancement, you can now search through Abuser Logs. To do so:

1. Select Monitor Mode > Service > Abuser Log.
2. On the menu bar, select Abuser, if not already selected.
3. Click the Criteria drop-down menu and select the desired Abuser Criteria.
4. Enter values for any other search parameters you would like to user. You can search or filter results based on the following values:
   "IP", "User", "Host", "MAC", "Action", "Criteria", "Start Time" and "End Time".
5. Click the Find button to begin the search. A window similar to this one appears:



IP:
User:
Host:
MAC Address:
Action: fall-in
Criteria: stream-tv
Start Time: 2011/01/03 14:13
End Time: 2011/02/11 14:13
ID From: To:

[1 - 50] / 1106 Next Page 50 List Per Page

ID	Date/Time	IP	User Name	Hostname	MAC Address	Action	Criteria
4141	Feb 11 13:55:02	192.168.161.1	John	N/A	00:1d:09:c3:ca:1a	fall-in	stream-tv
4138	Feb 11 13:45:33	192.168.161.1	John	N/A	00:1d:09:c3:ca:1a	fall-in	stream-tv
4136	Feb 11 13:34:32	192.168.161.97	Mike	N/A	00:1d:09:c3:ca:1d	fall-in	stream-tv
4134	Feb 11 13:28:32	192.168.161.97	Mike	N/A	00:1d:09:c3:ca:1d	fall-in	stream-tv
4131	Feb 11 13:10:02	192.168.161.19	Mario	N/A	00:1d:09:c3:ca:9a	fall-in	stream-tv
4128	Feb 11 13:00:32	192.168.161.17	Sammy	N/A	00:1d:09:c3:ca:3a	fall-in	stream-tv
4126	Feb 11 12:45:32	192.168.161.19	Mario	N/A	00:1d:09:c3:ca:9a	fall-in	stream-tv

6. A table containing the relevant Abuser Logs appears. Date/Time information is provided, as well as IP, User Name, Hostname, MAC Address, Action, and Criteria.

4.5.2 CLI Config

To show abuser statistics, use the following command:

```
EX1100(config)#show traffic abuser top base-on ?
  ip    Base on ip
  user  Base on user
```

```
EX1100(config)#show traffic abuser top base-on user ?
  criteria            Specify criteria name
  period              Select time period, default is 3 hours
  top-num             Top number, default is 10
  |                        Output modifiers
  <cr>
```

```
EX1100(config)#show traffic abuser top base-on user criteria ?
  WORD<length:1-31>  Specify criteria name
```

```
EX1100(config)#show traffic abuser top base-on user criteria test1
Top abuser statistics
=========================================
Start Time          : 2010-12-16 18:51:30
End Time            : 2010-12-16 21:51:30
No abuser statistics
```

To show abuser logs, use the following CLI command:

```
EX1100(config)#show abuser-log criteria ?
  WORD<length:1-31>   Criteria name filter value, wildcard '*' and '?'
                      are supported
```

```
EX1100(config)#show abuser-log criteria test1
```

4.6 Archive Reports to Remote File Server

In prior releases, EX users could generate reports and then email the reports as a means of exporting them from the appliance. With this latest release, the EX appliance can now export generated report files using the following file transfer methods:

- SCP – Secure Copy (based on SSH)
- RCP – Unix ‘remote copy’ command
- TFTP – Trivial File Transfer Protocol (lightweight version of FTP)
- FTP – File Transfer Protocol (standard protocol for copying files over TCP/IP network)

These protocols can be used to transfer reports to remote file servers now or at a scheduled time.

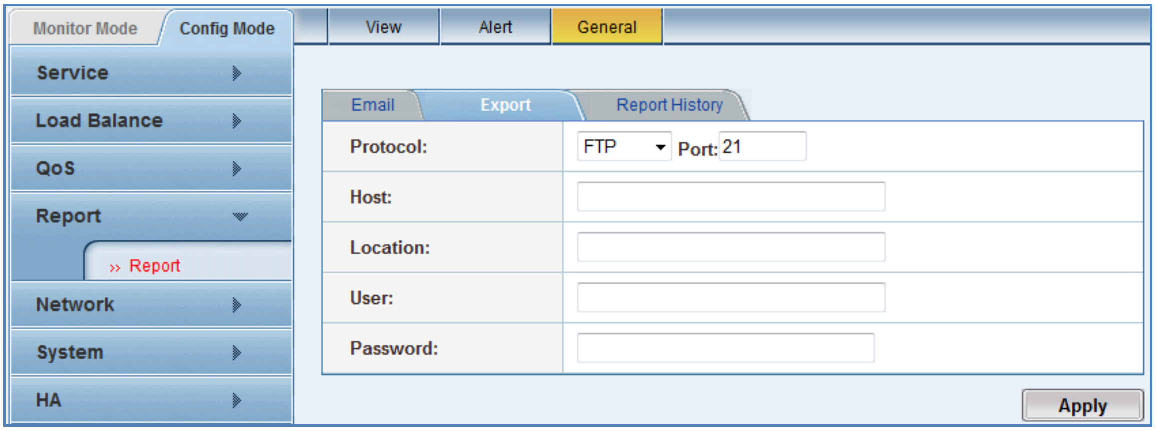
4.6.1 GUI Config

Default Export Settings

Default Export Settings (under Config Mode > Report > General) will be used if a Specific Export Setting (under Monitor Mode > Report > Favorites) is not configured for a specific scheduled report.

To configure the default export settings for a report (while in Config Mode):

1. Select Config Mode > Report > Report.
2. On the menu bar, select General.
3. Click Export tab to display a window similar to the one shown below:



Protocol:	FTP Port: 21
Host:	
Location:	
User:	
Password:	

4. Select the desired file transfer protocol from the drop-down menu: FTP, TFTP, RCP, or SCP.
   If needed, change the protocol port number in the port field. By default, the default port number for the selected protocol is used.
5. In the Host field, enter the directory path and filename.
   Note: The filename is automatically created after the user generates the report and clicks the Export button. The user is prompted to choose a location to save the file, and the

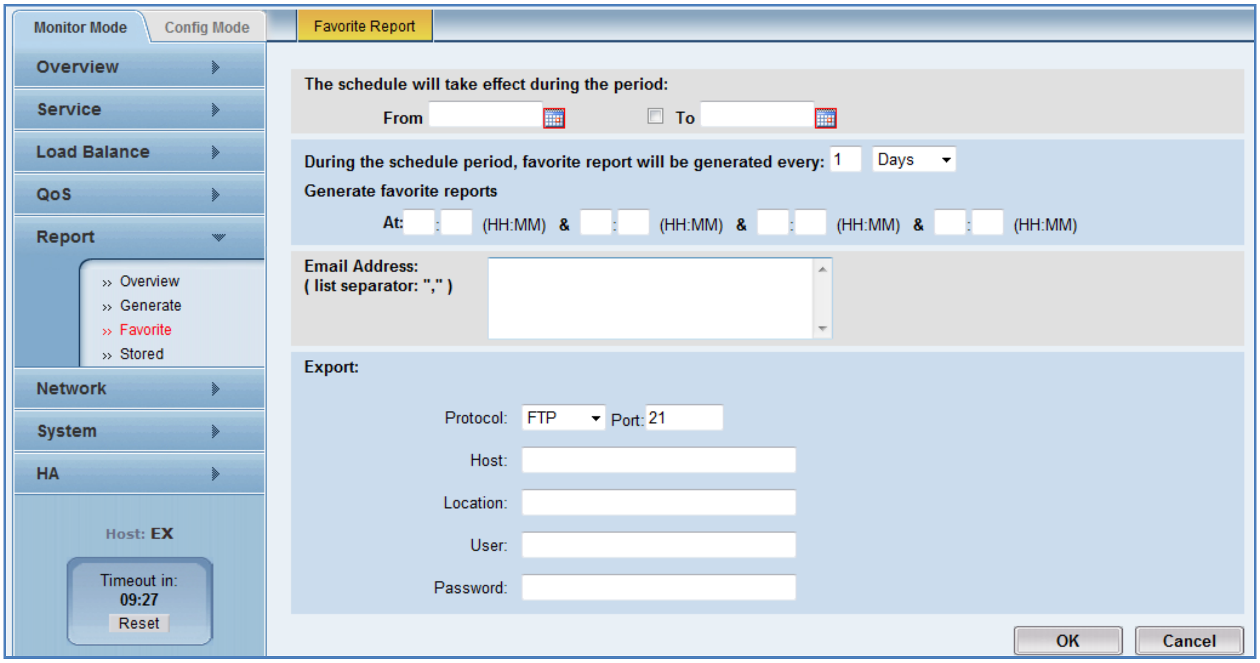
auto-created file name appears similar to this: *traffic_FWKLUQUK_20101208-040139.tgz*

6. In the User and Password fields, enter the username and password required for access to the remote server.
7. Click Apply.

Specific Export Settings

Alternatively, you can configure specific export settings for generated reports in tandem with the scheduling feature (while in Monitor Mode):

1. Select Monitor Mode > Report > Favorite.
2. From the Name column that appears, select the checkbox next to the name of the report you want to schedule and click the Schedule button. A window similar to the one shown below appears:



The schedule will take effect during the period:

From □ To

During the schedule period, favorite report will be generated every: 1 Days

Generate favorite reports

At: : (HH:MM) & : (HH:MM) & : (HH:MM) & : (HH:MM)

Email Address:
(list separator: ",")

Export:

Protocol: FTP Port: 21

Host:

Location:

User:

Password:

3. Select the start and end dates for the schedule.
4. Specify how often to generate the report by clicking the drop-down list and selecting one of the following: (Days, Weeks, or Months)
5. Specify the time(s) of day to generate the reports.
6. Instead of emailing the generated reports, you can export them to a remote server as follows:
   a. Select the desired file transfer protocol from the drop-down menu: FTP, TFTP, RCP, or SCP
   b. If needed, change the protocol port number in the port field. By default, the default port number for the selected protocol is used.
   c. In the Host field, enter the directory path and filename.

   d. In the User and Password fields, enter the username and password required for access to the remote server.

7. Click OK to save your changes.

The favorites list is redisplayed. The schedule information for the report is listed in the Next Run Time and Schedule columns. When a scheduled report is generated, the output is stored on the EX device. If you configured a file transfer protocol, the report is exported to the specified server. If you specified an email address, the report will also be emailed.

4.6.2 CLI Config

General Export Settings

You can configure general exporting for generated report files using a file transfer protocol by executing the following command from config mode:

```
EX(config)# report export ?
 tftp:  Remote file path of tftp: file system(Format: 
tftp://host[:port]/file)
 ftp:   Remote file path of ftp: file system(Format: 
ftp://[user:pass@]host[:port]/file)
 scp:   Remote file path of scp: file system(Format: 
scp://[user:pass@]host[:port]/file)
 rcp:   Remote file path of rcp: file system(Format: 
rcp://[user@]host/file)
```

You can enter the entire URL on the command line or press Enter to display a prompt for each part of the URL. If you enter the entire URL and a password is required, you will still be prompted for the password. To enter the entire URL using FTP, you would enter the command as follows:

```
EX(config)# report export ftp://[user@]host[:port]/file
```

Where *user* is the administrative name for the remote host, and `port` is the port number required to access the server, and `file` is the file name.

For example, the following command uses FTP to export a generated traffic report from the EX appliance to a remote server named “reports”. The admin is “john” and the port is 21.

```
EX(config)#report export ftp://john@192.168.1.10:21/reports/traffic-01
```

Specific Export Settings

You can also configure a specific export protocol to use for a “favorites” report by executing the following command from config mode:

```
EX(config-report-favorite)# export ?
  tftp:  Remote file path of tftp: file system(Format: 
tftp://host[:port]/file)
```

```
  ftp:   Remote file path of ftp: file system(Format:
ftp://[user:pass@]host[:port]/file)
  scp:   Remote file path of scp: file system(Format:
scp://[user:pass@]host[:port]/file)
  rcp:   Remote file path of rcp: file system(Format:
rcp://[user@]host/file)
```

4.7 Enhanced Auto Created Classes

4.7.1 IP Protocol Classification

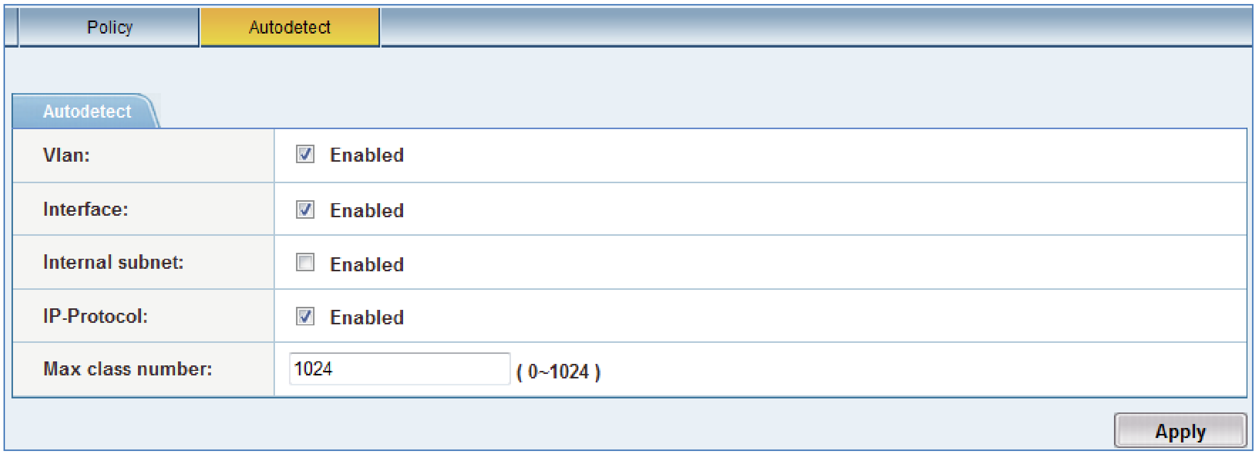
In prior releases, non-TCP and non-UDP IP traffic was classified as “others”. In this release, auto-detected classes now classify non-TCP and non-UDP sessions by their appropriate IP Protocol such as ICMP, GRE, etc.

The new approach to classifying IP Protocols (non-TCP, non-UDP) is enabled by default.

4.7.1.1 GUI Config

Classification of IP Protocols (non-TCP, non-UDP) is enabled by default. To disable the auto-detection of IP Protocols, do the following:

1. Select Config Mode > QoS > Settings.
2. Select Autodetect from the menu bar.
   A window similar to the one shown below appears:



Vlan:	☑ Enabled
Interface:	☑ Enabled
Internal subnet:	☐ Enabled
IP-Protocol:	☑ Enabled
Max class number:	1024 (0~1024)

3. Click the IP-Protocol checkbox to clear it.
4. Click Apply to save your changes.
   Non-TCP and non-UDP IP traffic will no longer be auto-detected by the EX appliance.

4.7.1.2 CLI Config

Classification of IP Protocols (non-TCP, non-UDP) is enabled by default. To disable the auto-detection of IP Protocols via the EX CLI, use the following command:

```
EX(config)#no qos autodetect ip-protocol
```

To re-enable the auto-detection of IP Protocols via the EX CLI, use the following command:

```
EX(config)#qos autodetect ip-protocol
```

4.7.2 Limit Auto-created classes

In previous releases, Traffic classes were either pre-defined by the system, manually configured by the user, or they could be Auto-Created based upon any of the following parameters:

- VLAN
- Interface
- Internal subnet
- IP-protocol

However, as the number of methods that could be used to create classes expanded, this increased the possibility that the user could run into the upper limit of 1,024 classes, depending on which EX model had been purchased. To prevent the user from running out of classes, this release supports the ability to limit the number of auto-detected classes that will be created. By default, auto-created classes are limited to no more than half of the maximum number of classes supported by the EX device.

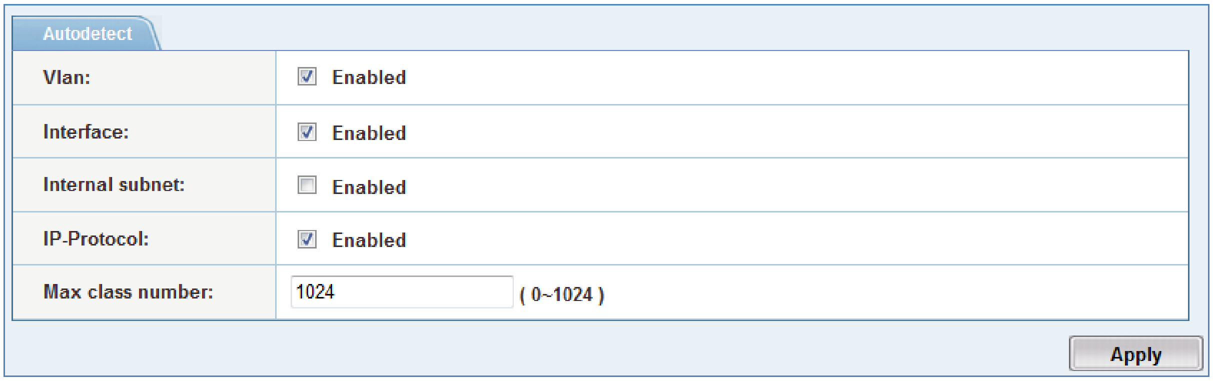
Details:

- To avoid naming conflicts between user-created classes and auto-created class, the auto-created classes will have the following prefix: “sys_”.
- Auto-created classes can be deleted or turned into user-defined classes (although their rules cannot be changed by the user).
- The number of auto-created classes will increase continually if the user does not delete those which are infrequently used. Thus, rarely-used classes will be automatically eliminated by the system if they have not been used for a period of time.

4.7.3 GUI Config

You can configure the EX to automatically create QoS classes based on VLAN, Interface, Internal subnet, or IP-Protocol. You can also prevent the Auto-Created classes from consuming too many of the classes within the 1,024 maximum limit. To do so:

1. Select Config Mode > QoS > Settings.
2. Select Autodetect from the menu bar (if not already selected). A window similar to the one shown below appears:



Autodetect

Vlan:	☑ Enabled
Interface:	☑ Enabled
Internal subnet:	□ Enabled
IP-Protocol:	☑ Enabled
Max class number:	1024 (0~1024)

3. In the Max Class Number field, enter the maximum number of Auto-Created classes to reserve some of the classes for the other classification methods. The default value is 1,024. (For example, if you wanted to reserve half of the maximum 1,024 classes for system-defined and user-defined classes, then you could enter 512 in the Max Class Number field to limit the Auto-Created classes to half of those available.)
4. Click Apply to save your changes.

4.7.4 CLI Config

Use the following command to impose a limit on the number of Auto-Created classes:

```
EX(config)#qos resource-limit class auto-created number ?
  <0-1024>   Configure auto-created class number
```

4.8 Bandwidth Management and Reports by Category

In prior releases, categories were used to view information about traffic classes at a higher level. In this latest release, categories take on a more functional role, as they can now take a more direct role in creating traffic policies and generating reports.

Categories in Bandwidth Control (Enhancement #1)

In prior releases, the administrator had to configure QoS traffic management policies based upon individual classes. The administrator had to create a separate traffic policy rule for each of the different classes of traffic. For example, to create policies to limit P2P traffic, the administrator needed to set up separate QoS policies rules for Limewire, Gnutella, iMesh, etc.

In this latest release, to simplify QoS configuration, administrators can now create traffic policies based on *categories* rather than classes. (Categories are higher-level groupings of classes.) In this way, an administrator can set up a QoS policy based upon a single category (P2P, for example), and that policy will encompass the underlying peer-to-peer traffic classes in order to create a positive match.

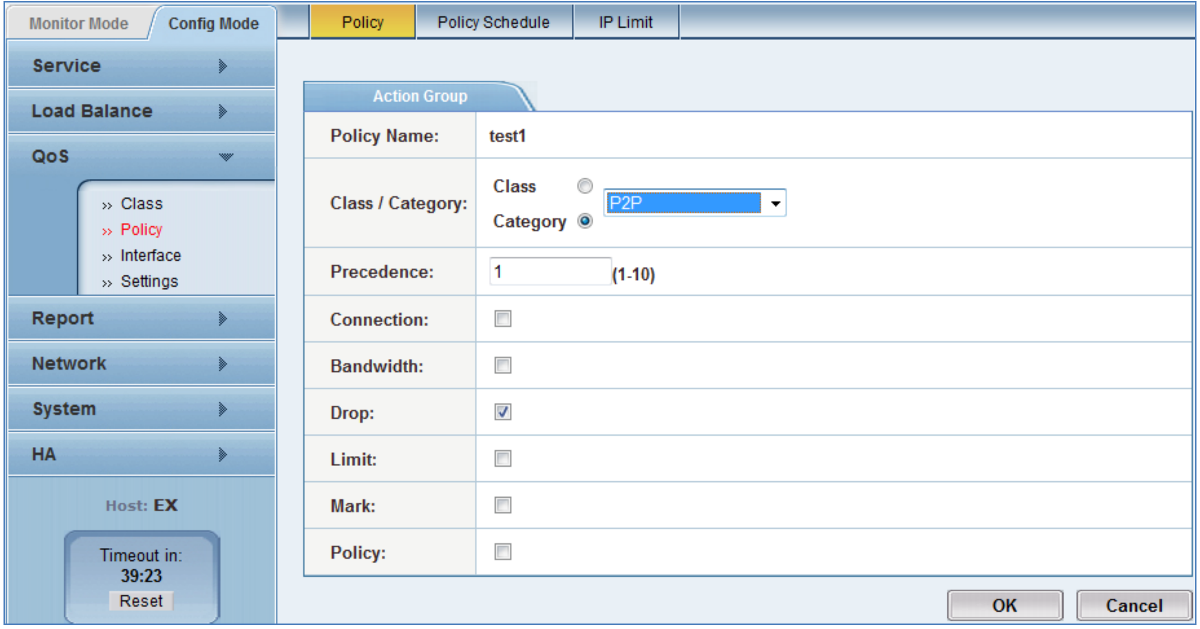
An additional benefit is that when new P2P classes are created and added to the P2P category, they will automatically be applied to the associated traffic policies. This means the administrator will not have to create a new traffic policy for the new P2P classes.

Categories in Report Generation (Enhancement #2)
The second enhancement is related to categories and it impacts how traffic reports are generated. Prior releases allowed the user to generate reports based upon classes, but this latest release allows reports to be generated based upon categories. Users can obtain reports on overall usage by category, or they can get details for a specific category, and they can drill down to the class level from within a detailed category report.

4.8.1 GUI Config

Categories in Bandwidth Control - Enhancement #1
To create a traffic policy using categories instead of classes, follow the procedure below:

1. Select Config Mode > QoS > Policy, and select Policy from the menu bar.
2. Click the New button, enter a name in the Policy Name field, and click the New button to display an Action Group window similar to the one shown below:



Policy Name:	test1
Class / Category:	Class ○ Category ● P2P
Precedence:	1 (1-10)
Connection:	□
Bandwidth:	□
Drop:	☑
Limit:	□
Mark:	□
Policy:	□

3. Select the Category radio button, select the drop-down menu, and then select the desired category that the policy should be based upon.
4. Enter a value from 1-10 in the Precedence field, keeping in mind that policies with lower Precedence values will be used to vet traffic before policies that have higher values.

5. Select the desired Action checkbox (Drop, Limit, Mark, etc.) that you would like to associate with this category of traffic. (See Easy QoS GUI on page 33 for a detailed discussion of the fields associated with each action.)
6. Click OK to save your changes.

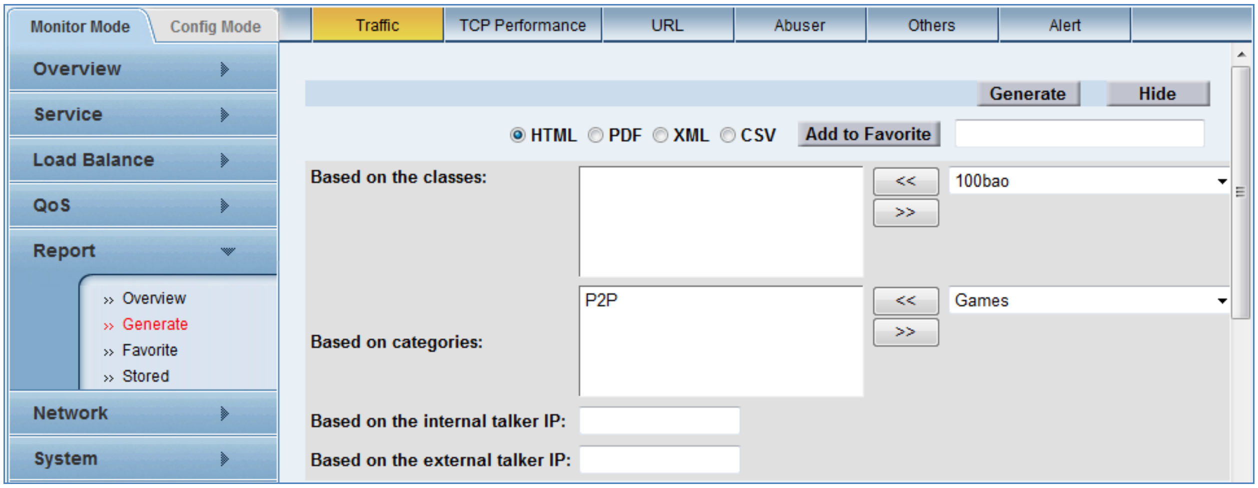
Details:

- All categories are editable, but only categories configured by the user can be deleted. Predefined categories (such as P2P), cannot be deleted.

Categories in Report Generation - Enhancement #2

To generate a Traffic Report that is based upon a Category instead of a Class, follow the procedure below:

1. Select Monitor Mode > Report > Generate.
2. Select Traffic from the menu bar. A window similar to the one shown below appears:



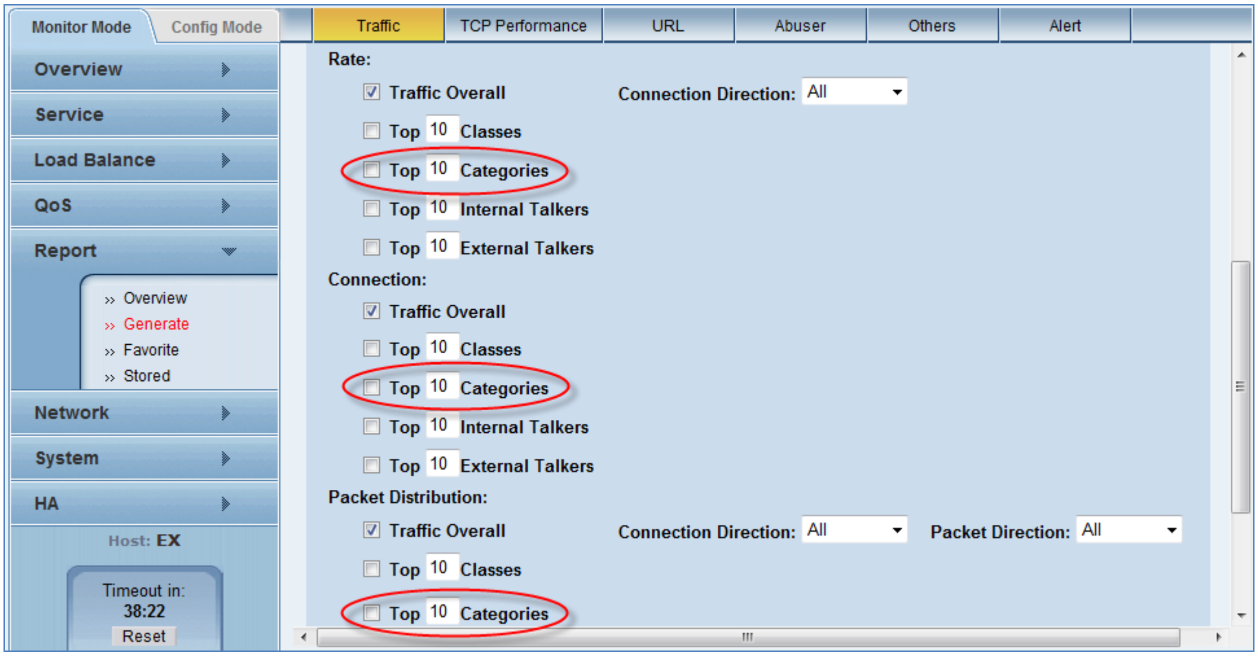
Based on the classes: 100bao

Based on categories: P2P | Games

Based on the internal talker IP:

Based on the external talker IP:

3. In the “Based on categories” section of the window, click on the drop-down menu to the far right and select the desired category that you would like to use to generate the report.
4. Use the arrow button (<<) to move the category over the field on the left.
5. Click the Generate button to create your report.
6. Optionally, you can scroll down to the Rate, Connection, and Packet Distribution sections to view additional category options, as shown below:



Rate:

☑ Traffic Overall Connection Direction: All

□ Top 10 Classes

□ Top 10 Categories

□ Top 10 Internal Talkers

□ Top 10 External Talkers

Connection:

☑ Traffic Overall

□ Top 10 Classes

□ Top 10 Categories

□ Top 10 Internal Talkers

□ Top 10 External Talkers

Packet Distribution:

☑ Traffic Overall Connection Direction: All Packet Direction: All

□ Top 10 Classes

□ Top 10 Categories

7. If desired, select the Top 10 Categories checkbox for Rate, Connection, and/or Packet Distribution. (These options are new in this release.)
   Selecting any of these options will cause information to be included in the generated Traffic report at the Category level.
8. Click the Generate button to create the report based upon the options you have selected.

4.8.2 CLI Config

Using Categories to Create QoS Policies

To create QoS policies based on category via the CLI, use the commands shown below:

```
EX(config)#qos policy ?
  WORD<length:1-31>  Policy name

EX(config)#qos policy test1

EX(config-policy)#?
  category  Category
  class     Class
  do        To run exec commands in config mode
  end       Exit from configure mode
  exit      Exit from configure mode or sub mode
  no        Negate a command or set its defaults
  qos       QoS configuration
  show      Show running configuration
  write     Write configuration
```

```
EX(config-policy)#category intif

EX(config-policy-category)#?
  bandwidth   Bandwidth reservation and shaping
  category    Category
  class       Class
  connection  Connection limiting
  do          To run exec commands in config mode
  drop        Drop packet
  end         Exit from configure mode
  exit        Exit from configure mode or sub mode
  limit       Configure policing/rate-limiting
  mark        Configure packet marking
  no          Negate a command or set its defaults
  policy      Sub policy
  show        Show running configuration
  write       Write configuration
```

Real Time Statistics

The EX appliance supports `show qos top category` and `show qos top class category category-name` via the CLI:

```
EX(config)#show qos top category …

EX(config)#show traffic rate ?
  overall                  Overall statistics
  top-category             Top category statistics
  top-class                Top class statistics
  top-internal-talker      Top internal talker statistics
  top-external-talker      Top external talker statistics

EX(config)#show traffic rate top-class scope ?
  category                  Specify scope of category
  class                    Specify scope of class
  internal-talker     Internal talker
  external-talker     External talker
```

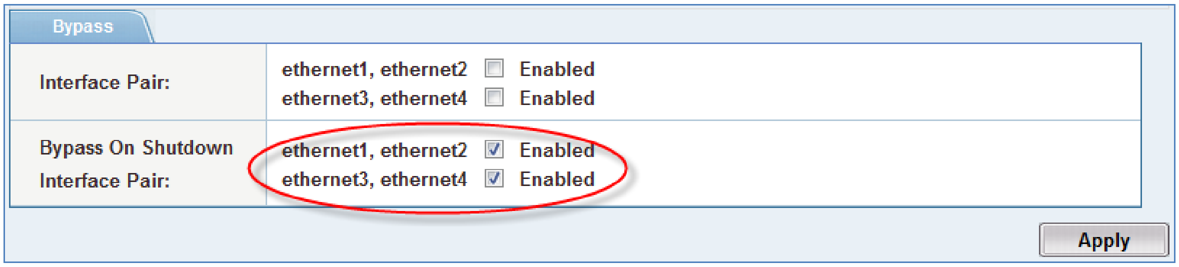
4.9 Bypass On Shutdown

This release introduces a bypass-on-shutdown feature which will enable bypass only when the box is performing a reboot or shutdown. The purpose of this feature is to minimize traffic flow downtime to 2 seconds or less when the EX is in transparent mode. It should be used with hardware bypass enable upon boot up. This feature only applies to EX 1100 and 2110 models.

4.9.1 GUI Config

To enable hardware bypass when shutting down the EX appliance, follow the procedure below:

1. Select Config Mode > Network > Interface.
2. Select Bypass from the menu bar.
   A window similar to the one shown below appears:



Interface Pair:
ethernet1, ethernet2 □ Enabled
ethernet3, ethernet4 □ Enabled

Bypass On Shutdown Interface Pair:
ethernet1, ethernet2 ☑ Enabled
ethernet3, ethernet4 ☑ Enabled

3. Select the Enabled checkbox for pair 1 (eth 1, eth 2) and for pair 2 (eth 3, eth 4).
4. Click Apply to save your changes.

4.9.2 CLI Config

The following command enables the **bypass-on-shutdown** command on pair 1, which consists of Ethernet ports 1 and 2:

```
EX(config)#bypass-on-shutdown interface-pair 1
```

The following command enables the **bypass-on-shutdown** command on pair 2, which consists of Ethernet ports 3 and 4:

```
EX(config)#no bypass-on-shutdown interface-pair 2
```

To enable the **bypass-on-shutdown** command on both pairs, use the following command:

```
EX(config)#bypass-on-shutdown interface-pair all
```

After issuing the **bypass-on-shutdown** commands, you can verify the status of the ports with the following **show** command:

```
EX(config)#show bypass-on-shutdown interface-pair
```

```
Interface                      Bypass-On-Shutdown
---------------------------------------------------------------
ethernet1, ethernet2           Enabled
ethernet3, ethernet4           Disabled
```

4.10 Enhancement of RADIUS Privilege Option

In this latest release, the EX appliance supports authentication and accounting of users through one or more RADIUS servers. The user can specify the necessary parameters for one or more RADIUS servers, and this will, in turn, designate the EX appliance as a Network Access Server (NAS).

While prior releases of the EX Series supported read-only privileges, this latest release introduces support for write privileges. A vendor-specific RADIUS attribute, called "A10-Admin-Privilege” has been defined in order to determine administrative privileges, and it offers two acceptable values: (1) Read only and (2) Read & Write.
In addition, the RADIUS protocol has a standard attribute for the privilege definition known as “Service-Type”. In this release, the EX appliance recognizes the following values:

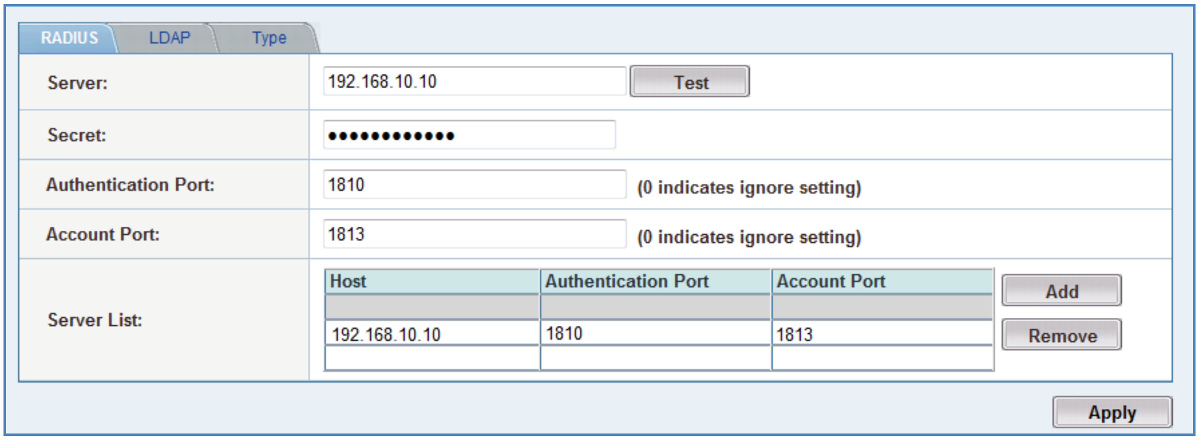
1 – Login (the user should be connected to a host)
6 – Administrative (privileged commands can be executed from the EX)
7 – NAS Prompt (user can execute non-privileged commands from the EX)

If the user passes the authentication but the reply from the RADIUS server does not contain the vendor-specific or Service-Type attribute, then the user will be granted read-only privileges.

4.10.1 GUI Config

To configure one or more RADIUS servers, follow the procedure below:

1. Select Config Mode > System > Settings.
2. Select Authentication from the menu bar.
   A window similar to the one shown below appears:



Server:	192.168.10.10
Secret:	●●●●●●●●●●●●
Authentication Port:	1810 (0 indicates ignore setting)
Account Port:	1813 (0 indicates ignore setting)

Server List:

Host	Authentication Port	Account Port
192.168.10.10	1810	1813

3. In the Server field, enter the IP address or hostname of the RADIUS server.
4. In the Secret field, enter the shared secret configured on the RADIUS server. (The shared secret is used to validate RADIUS requests and replies.)
5. If the server uses non-standard protocol port numbers, edit the numbers in the Authentication Port and Accounting Port fields.
6. Click the Add button to add the RADIUS server to the Server List at the bottom of the window.
7. Repeat this process if you wish to add more than one RADIUS server.
   Note: The RADIUS server that appears at the top of the Server List will be the primary, and the following one will be the secondary. If the primary does not work, the EX appliance will attempt to authenticate users with the second RADIUS server that appears on the Server List.
8. Click Apply to save your changes.

4.10.2 CLI Config

You can add a RADIUS server via the CLI using the following command:

```
EX(config)#radius server <host name> [auth-port <port> | acct-port
<port> | secret <key value>]
```

To remove a specific RADIUS server or all configured RADIUS servers:

```
EX(config)#no radius server [<host name> | cr]
```

To remove the specified authorization port or accounting port for a RADIUS server:

```
EX(config)#no radius server <host name> [auth-port <port> | acct-port
<port>]
```

To show information for all RADIUS servers:

```
EX(config)#show radius server
```

4.11 Easy QoS GUI

The EX Series has been enhanced in this release by simplifying the process of configuring QoS policies. The new “Easy QoS GUI” feature simplifies the configuration of QoS policies by removing the concepts of “ingress” and “egress”, and no longer requires QoS Policies to be bound to QoS Interfaces.

In prior releases, an administrator had to define a QoS policy and a QoS interface to perform bandwidth management. This process of binding a QoS policy to an interface can be confusing for administrators, especially when it comes to applying QoS Policies to ingress and egress interfaces.

This latest release simplifies all settings related to QoS policy and QoS interface configuration. The new approach is based on a hierarchical tree structure. Users simply create a “Class” to identify the different types of traffic and an “Action” to determine how the EX appliance will handle traffic that matches the class.

When the user configures QoS via the new “Easy Mode”, the EX appliance will automatically (and transparently) handle the configuration of the appropriate underlying objects.

Details:

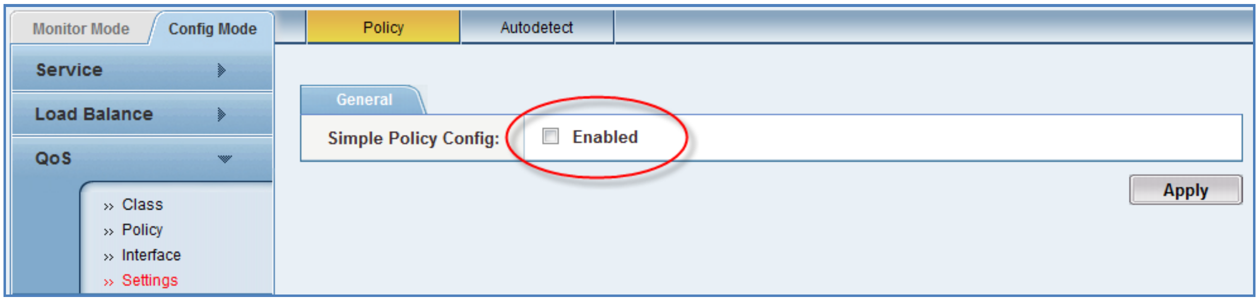
- New EX installations will be in “Easy Mode” by default.
- As a courtesy to legacy users and users looking for more advanced control of traffic, the original QoS configuration method, now known as “Advanced Mode”, will be preserved.
- Due to the difficulties involved in translating an existing QoS configuration file created in “Advanced Mode” into “Easy Mode”, users who have configured their systems while in “Advanced Mode” must remain in “Advanced Mode”.
- Users with existing systems who would like to switch to “Easy Mode” must clear their existing “Advanced Mode” configuration, enable Easy Mode, and then re-configure.
- “Easy Mode” can only be configured via the GUI and cannot be configured via the CLI. Users who wish to use the CLI to configure QoS must do so while in “Advanced Mode”.

4.11.1 GUI Config

Configuring Simple Policy

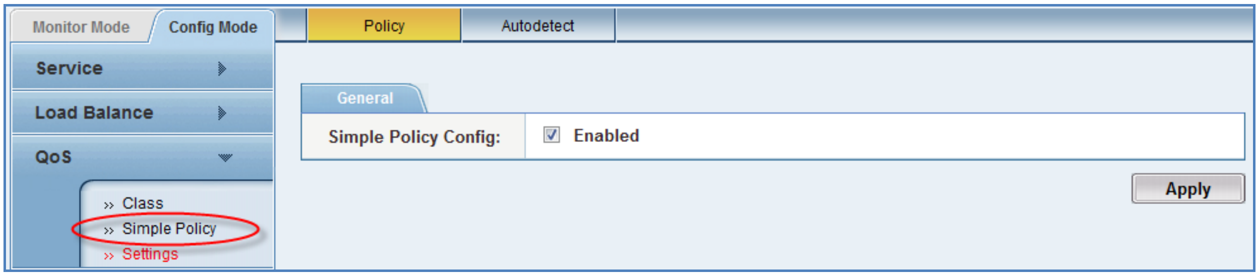
To configure “Easy QoS GUI”, follow the procedure below:

1. Select Config Mode > QoS > Settings.
2. Select Policy from the menu bar (if not already selected).
   A window similar to the one shown below appears:



Simple Policy Config: □ Enabled

3. Select the Enabled checkbox to enable Simply Policy Config (a.k.a. “Easy QoS GUI”).
4. Click Apply to save your changes.
   You will notice that the Policy and Interface hyperlinks (under the QoS module button) are replaced with a hyperlink that says Simple Policy, as shown below:



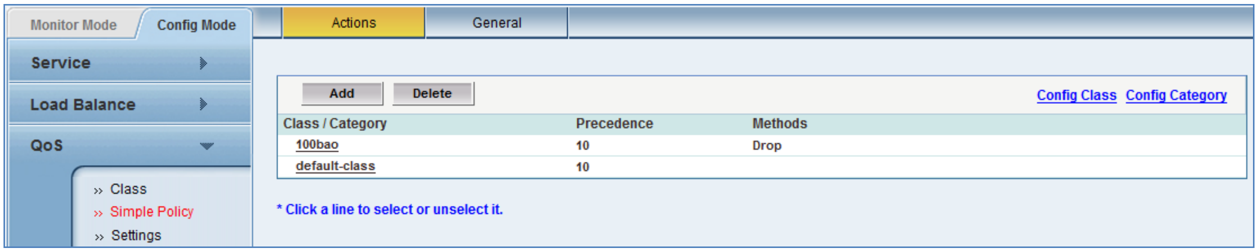
Simple Policy Config: ☑ Enabled

At this point, “Easy QoS GUI” is enabled and you can perform the configurations that follow.

Configuring Shaping with General tab:

To configure the General tab, follow the procedure below:

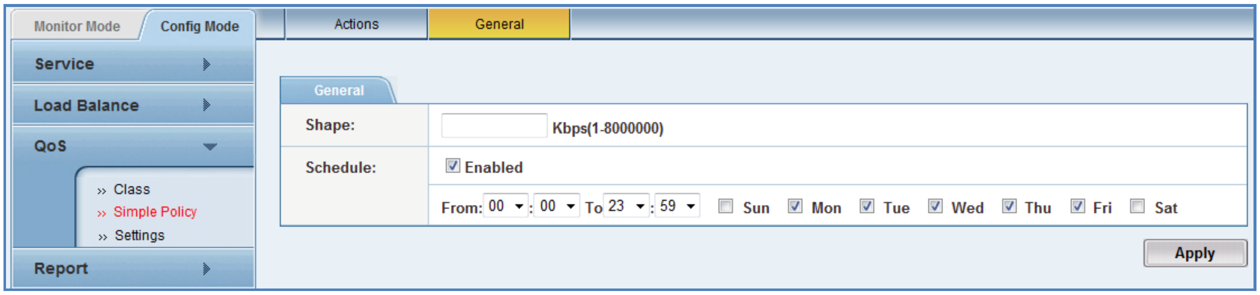
1. Select Config Mode > QoS > Simple Policy.
   The Simple Policy window appears, as shown below:



Class / Category	Precedence	Methods
100bao	10	Drop
default-class	10	

* Click a line to select or unselect it.

2. Select General from the Menu bar. A window similar to the one shown below appears:



Shape: Kbps(1-8000000)

Schedule: ☑ Enabled

From: 00 : 00 To 23 : 59 □ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat

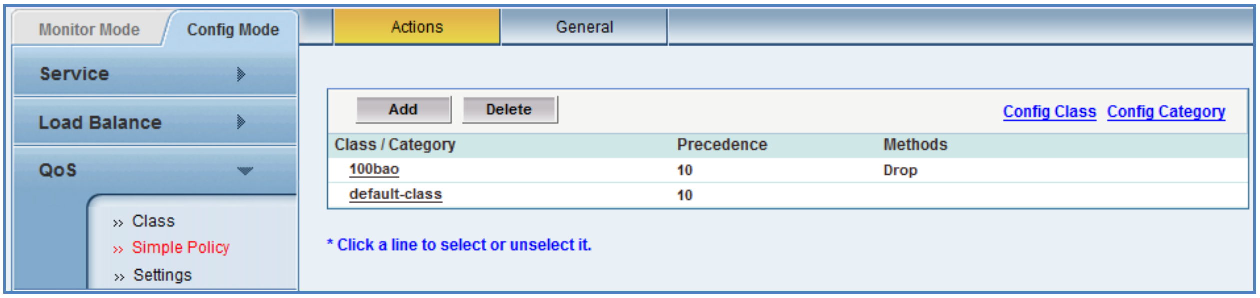
a. Enter the Kbps value in the Shape field. Shaping applies to egress traffic and guarantees a specific amount of bandwidth for forwarding traffic.

b. In the Schedule fields, enter the hours during which the policy will be active (e.g. 9:00 – 17:00), and use the checkboxes to determine which days of the week the policy will be active (e.g. Mon – Fri).

3. Click Apply to save your changes.

Configuring Action Groups

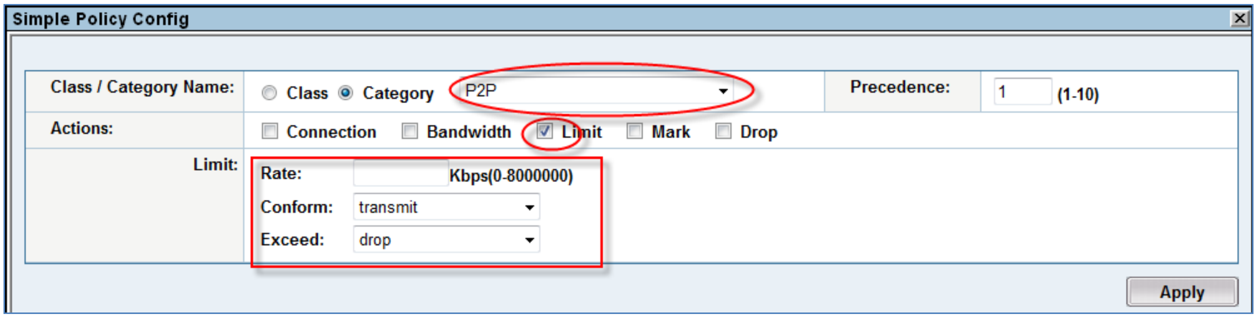
1. Next, select Actions from the Menu bar.
   A window similar to the one shown below appears, listing Action Groups.



Class / Category	Precedence	Methods
100bao	10	Drop
default-class	10	

* Click a line to select or unselect it.

2. Click the Add button to configure a new Action Group. A window similar to the one shown below appears.



Class / Category Name: ○ Class ● Category P2P

Precedence: 1 (1-10)

Actions: □ Connection □ Bandwidth ☑ Limit □ Mark □ Drop

Limit:
Rate: Kbps(0-8000000)
Conform: transmit
Exceed: drop

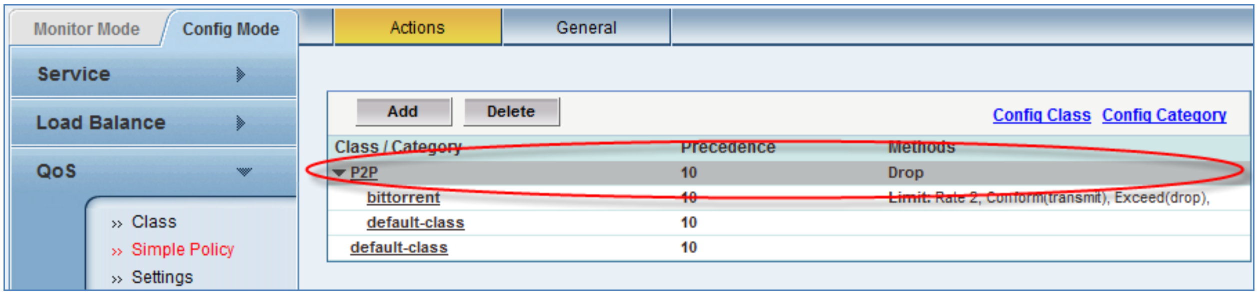
3. Select the Class or Category radio button, and then click the drop-down menu and select the desired class or category for which traffic will be classified.

4. Enter a value (1 – 10) in the Precedence field. The default value is 10. Entering 1 will cause this Action Group to receive the highest (or most preferred) precedence.
   Note: The EX appliance compares traffic against the match criteria within an Action Group, taking action based upon the first positive match. Action Groups that have a lower Precedence will vet traffic before Action Groups that have a higher Precedence. Thus, if the most important goal for your network is to prevent P2P traffic, then you should create an Action Group based on the "P2P" category and assign that Action Group a Precedence value of 1.
5. Next, select the desired Actions checkbox. Options are:
   - Connection – Limit traffic based on connection usage.
   - Bandwidth – Limit traffic based on bandwidth usage.
   - Limit – Apply rate limiting to police the bandwidth used by traffic of a certain QoS class of category by enforcing a specified maximum rate.
   - Mark – Change the DSCP value in the IP packet headers to change their forwarding priority throughout the network or routing through the EX appliance.
   - Drop – Drop traffic that matches the criteria in the Action Group.

Configuring Sub-Policies

If desired, you can create a sub-policy within another policy. This may be helpful if you wanted to create a policy based on an IP address or VLAN, and then define the policies for certain types of traffic for that IP or VLAN. To configure a sub-policy, follow the procedure below:

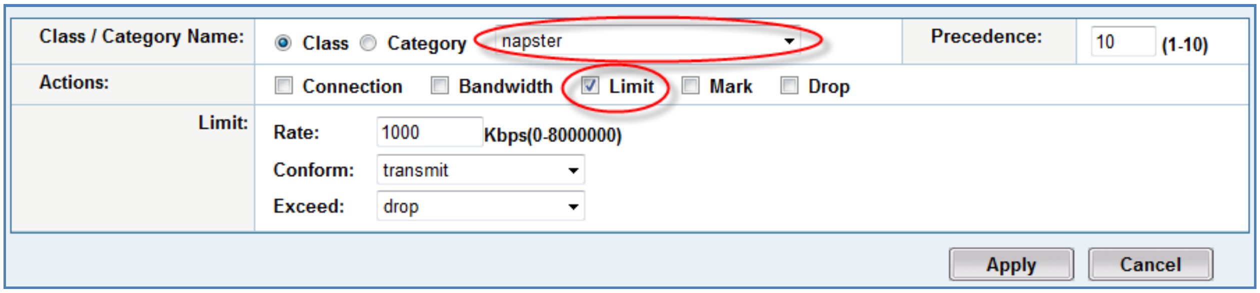
1. Select Config Mode > QoS > Simple Policy. The Simple Policy window appears, with a table listing the configured policies.
2. Click on the row within the table to highlight the class or category for which you would like to create a sub-policy. *Do not click on the hyperlink.*
   In the example below, we select the P2P category to highlight that row in grey.



Class / Category	Precedence	Methods
P2P	10	Drop
bittorrent	10	Limit: Rate 2, Conform(transmit), Exceed(drop),
default-class	10	
default-class	10	

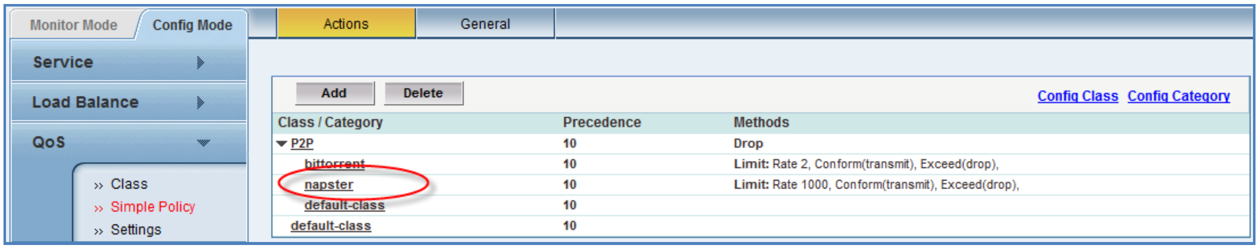
3. Click the Add button to add a traffic policy rule, such as Napster, to the selected category. The Simple Policy Config window appears.

4. Select the Class or Category radio button as desired, and then click the drop-down menu and select the desired application and define the traffic policy.
   In our example, we will select Napster from the drop-down menu, select the Limit checkbox, and configure the rate and associated options.



Class / Category Name:	● Class ○ Category napster	Precedence:	10 (1-10)
Actions:	□ Connection □ Bandwidth ☑ Limit □ Mark □ Drop		
Limit:	Rate: 1000 Kbps(0-8000000) Conform: transmit Exceed: drop		

5. Click Apply to save your changes.
   The new traffic policy rule for the specified class (or category) appears indented in order to convey that it is a nested sub-policy, as shown below:



Class / Category	Precedence	Methods
P2P	10	Drop
bittorrent	10	Limit: Rate 2, Conform(transmit), Exceed(drop),
napster	10	Limit: Rate 1000, Conform(transmit), Exceed(drop),
default-class	10	
default-class	10	

4.11.2 CLI Config

A10 Networks does not recommend using the CLI to modify QoS Policies that have been created using the “Easy QoS GUI”. If the “Easy QoS GUI” feature has been used to configure QoS Policies, then users should continue to use the EX appliance GUI to make any necessary modifications to QoS Policies or to create new QoS policies.

With that said, you can use the following CLI command to verify whether or not “Easy QoS GUI” feature is enabled:

```
EX(config)#show gui
GUI Settings:
                Simple QoS Policy....................Enabled
```

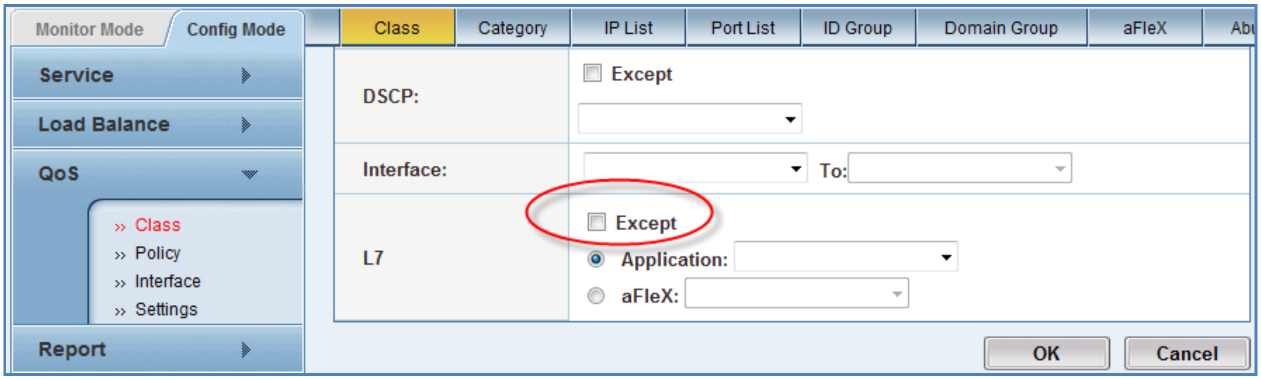
4.12 L7 Based Rule Exception

Prior releases allowed the user to create exceptions for certain rules within a QoS class. This latest release expands this list by allowing exceptions for Layer 7 protocols. Users can now create an exception for Layer 7 protocols. By creating an exception, traffic that would ordinarily create a positive match for the QoS Class will no longer create a positive match, and the designated Layer 7 traffic will continue through the EX appliance without being positively classified. An example of using a Layer 7 exception would be to create a class with TCP port 80 defined, and not HTTP or HTTPS. This would result in the classification of all traffic on port 80 that is not HTTP or HTTPS.

4.12.1 GUI Config

To configure the EX appliance to exclude L7 protocols from QoS classes:

1. Select Config Mode > QoS > Class.
2. Select Class from the menu bar (if not already selected).
3. From the Class column, select one of the predefined classes you wish to modify (or click New to create a new class). The Class tab appears, with a list of associated rules.
4. Click a rule to highlight it and then click the Edit button.
   The Rule tab appears, with a list of rules associated with that predefined Class.
5. Scroll to the bottom of the Rule tab to the L7 section. A window similar to the one shown below appears:



6. Create an exception for L7 traffic within this class by selecting the Except checkbox.
7. Select the appropriate radio button:
   - Application – The drop-down menu will be pre-populated if you are modifying one of the predefined classes.
   - aFleX – Click the drop-down menu and select the desired aFleX configuration.
8. Click OK to save your changes.

4.12.2 CLI Config

To create a Layer 7 exception within a QoS class rule, use the **`match application [except]`** Command, as shown below:

```
EX(config)#qos class test category Misc
EX(config)#match application except ssh
```

4.13 L7 Signature Updates

The EX WAN Bandwidth Manager now offers *L7 Signature Updates*. This feature creates a separate Layer 7 signature library, allowing the L7 classification to be upgraded without interrupting traffic on the box.

In prior releases, the L7 signature updates required an upgrade of the EX software. When new signature rules were added to the library, the user had to perform a full software upgrade, reboot the box, thus interrupting traffic on the network.

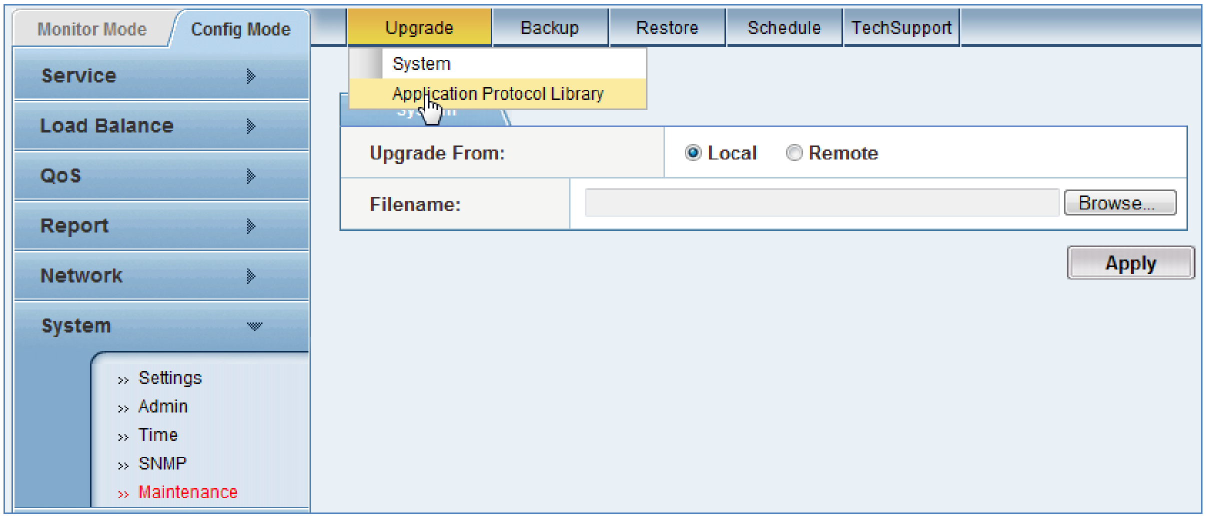
Details:

- The L7 signature library can now be upgraded separately.
- Signature library updates are non-disruptive, so existing traffic is unaffected.
- Flows can be classified using the new signature library, providing a seamless transition.
- A reboot or software reload is no longer required.

4.13.1 GUI Config

You can upgrade the L7 signature library (a.k.a. “Application Protocol Library”) without interrupting traffic on the EX appliance. To do so:

1. Select Config Mode > System > Maintenance.
2. Select Upgrade from the menu bar (if not already selected).
   A window similar to the one shown below appears:



3. Hover the cursor over the Upgrade menu button to display two menus, and then select Application Protocol Library to display the Application Protocol Library tab.
4. Select the Local or Remote radio button, and then click the Browse button to navigate to the file that will be used to upgrade the L7 signature library.
5. Click Apply to save your changes.

4.13.2 CLI Config

The CLI `upgrade` command has been modified to include two options. You can upgrade the entire system (as in prior releases), or you can upgrade just the L7 signature library (i.e. “application protocol”).

```
EX(config)#upgrade ?
  app-protocol  Upgrade application protocol
  system        Upgrade the whole software of system
```

You can use the CLI `upgrade` command to upgrade just the L7 signature library (i.e. “application protocol”), as shown below. You will be prompted to select the desired file transfer protocol, as well as specify the host name and file name.

```
EX(config)#upgrade app-protocol library ?
  tftp:  Remote file path of tftp: file system(Format:
tftp://host[:port]/file)
  ftp:   Remote file path of ftp: file system(Format:
         ftp://[user:pass@]host[:port]/file)
  scp:   Remote file path of scp: file system(Format:
         scp://[user:pass@]host[:port]/file)
  rcp:   Remote file path of rcp: file system(Format:
rcp://[user@]host/file)
```

To verify that the library has been upgraded, use the following command:

```
EX(config)#show version
```

4.14 QoS Classification by DSCP

The EX now offers the ability to classify traffic based on DSCP values. With this feature, an administrator can define a QoS class based upon DiffServ Code Point values that range from 0 to 63, (or based on a commonly-defined PHB name).

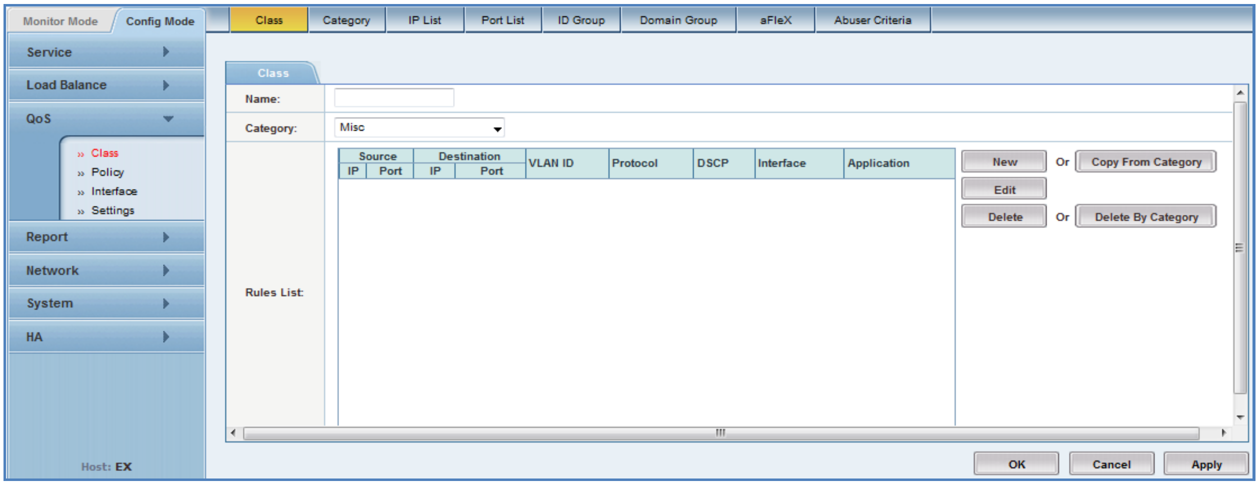
Details:

- If the user-specified DSCP value has a corresponding PHB name, the value (or number) will be converted to a PHB name.
- A QoS class can match multiple DSCP values.
- DSCP conditions (i.e. elements used to define class rules) can be combined with other conditions in QoS class definitions.
- System does not predefine the QoS class, category, or QoS view for DSCP, because the system cannot prejudge how users will want to define and organize DSCP classes. Thus, it depends on how the user wants to create them.
- A10 recommends that the administrator puts DSCP classes in a specially-defined class category and view. In this way, the user can get a DSCP-based statistics report without encountering double-counting issues with L4 or L7 classes.

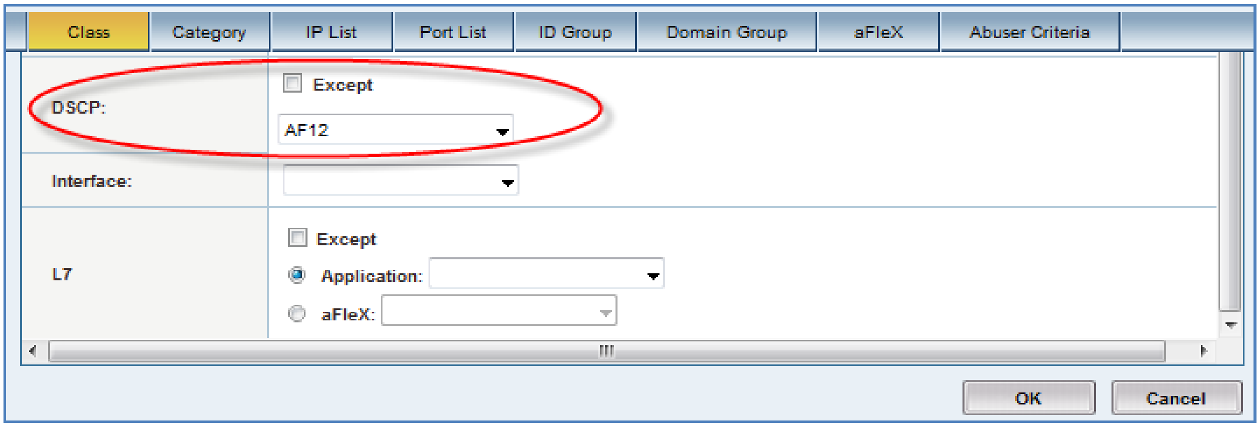
4.14.1 GUI Config

To define a QoS class based upon DSCP values:

1. Select Config Mode > QoS > Class.
2. On the menu bar, select Class, if not already selected.
3. Click the New button, or select a class from the Class column by clicking on the associated hyperlink. A window similar to the one shown below appears:



4. Enter a Name for the QoS Class in the Name field.
   This will be pre-populated if you are modifying one of the existing classes.
5. Select the desired Category from the drop-down menu.
   This will be pre-populated if you are modifying one of the existing classes.
6. To add a Rule, click the New button and scroll down to the DSCP section.

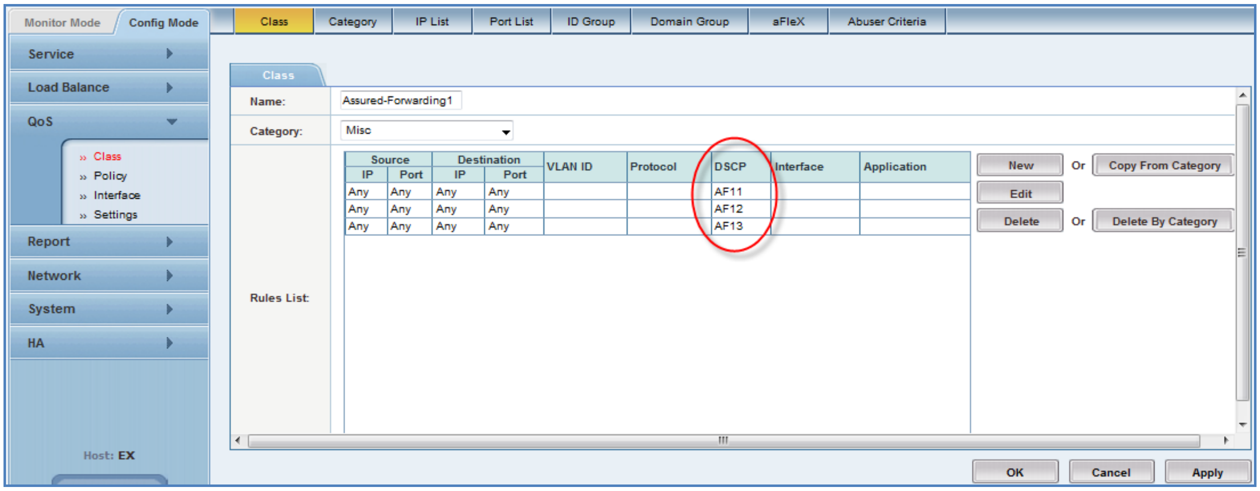


DSCP: ☐ Except
AF12

Interface:

L7 ☐ Except
● Application:
○ aFleX:

7. Click the DSCP drop-down menu and select the desired DSCP value: (e.g. AF11 – AF43, or CS 1 – 7).
8. If desired, select the Except checkbox to exclude traffic with this DSCP value from being classified.
9. Click OK to save your changes.
10. Repeat this process for as many DSCP rules (within the QoS Class) as desired.
11. When finished adding DSCP Rules to the Class, the window should appear similar to the one shown below, with the DSCP column reflecting the newly-configured DSCP values:



Name: Assured-Forwarding1

Category: Misc

Rules List:

Source		Destination		VLAN ID	Protocol	DSCP	Interface	Application
IP	Port	IP	Port					
Any	Any	Any	Any			AF11		
Any	Any	Any	Any			AF12		
Any	Any	Any	Any			AF13		

12. Click OK to save your changes.

4.14.2 CLI Config

To use DSCP to classify traffic, use the CLI commands shown below.

To name the QoS class for which DSCP will be used to classify traffic:

```
EX1100(config)#qos class aim
```

To create the match conditions for traffic within this class:

```
EX1100(config-class)#match ?
  aflex        aFlex name
  application  Application Type
  dip          Destination IP Address
  dmac         Destination MAC address
  dport        Layer 4 Destination Port
  dscp         IP DSCP
  interface    Interface
  prot         Layer 4 protocol
  sip          Source IP Address
  smac         Source MAC address
  sport        Layer 4 Source Port
  vlan         VLAN ID
  <cr>
```

To select the DSCP value upon which traffic will be classified (in our example, AF11):

```
EX1100(config-class)#match dscp ?
  except   Except DSCP value
  <0-63>   Free dscp value (0-63)
  af11     AF11 dscp (001010)
  af12     AF12 dscp (001100)
  af13     AF13 dscp (001110)
  af21     AF21 dscp (010010)
  af22     AF22 dscp (010100)
  af23     AF23 dscp (010110)
  af31     AF31 dscp (011010)
  af32     AF32 dscp (011100)
  af33     AF11 dscp (011110)
  af41     AF41 dscp (100010)
  af42     AF42 dscp (100100)
  af43     AF43 dscp (100110)
  cs1      CS1(precedence 1) dscp (001000)
  cs2      CS2(precedence 2) dscp (010000)
  cs3      CS3(precedence 3) dscp (011000)
  cs4      CS4(precedence 4) dscp (100000)
  cs5      CS5(precedence 5) dscp (101000)
  cs6      CS6(precedence 6) dscp (110000)
  cs7      CS7(precedence 7) dscp (111000)
  default  default dscp (000000)
  ef       EF dscp (101110)

EX1100(config-class)#match dscp af11
```

4.15 QoS Policy Action of Connection Limits

In prior releases, the EX Series was able to limit traffic using the parameters of bandwidth rate (i.e. limiting traffic based on the number of bytes per second going through the device). However, the administrator was not able to limit traffic based on the total number of connections.

With this latest release, the EX appliance now supports the ability to limit traffic based on the maximum number of connections for a particular class or based on the number of connections associated with a particular IP address.

For example, an administrator could create a QoS class to identify HTTP traffic and limit the total number of HTTP connections to no more than 100. In addition, the admin could create a class that would limit each IP address to no more than 10 simultaneous connections. Thus, HTTP could have up to 100 connections, but each new IP address would be limited to no more than 10 connections. Once the connection limit is reached, subsequent connection requests would be dropped or rejected.

Details:

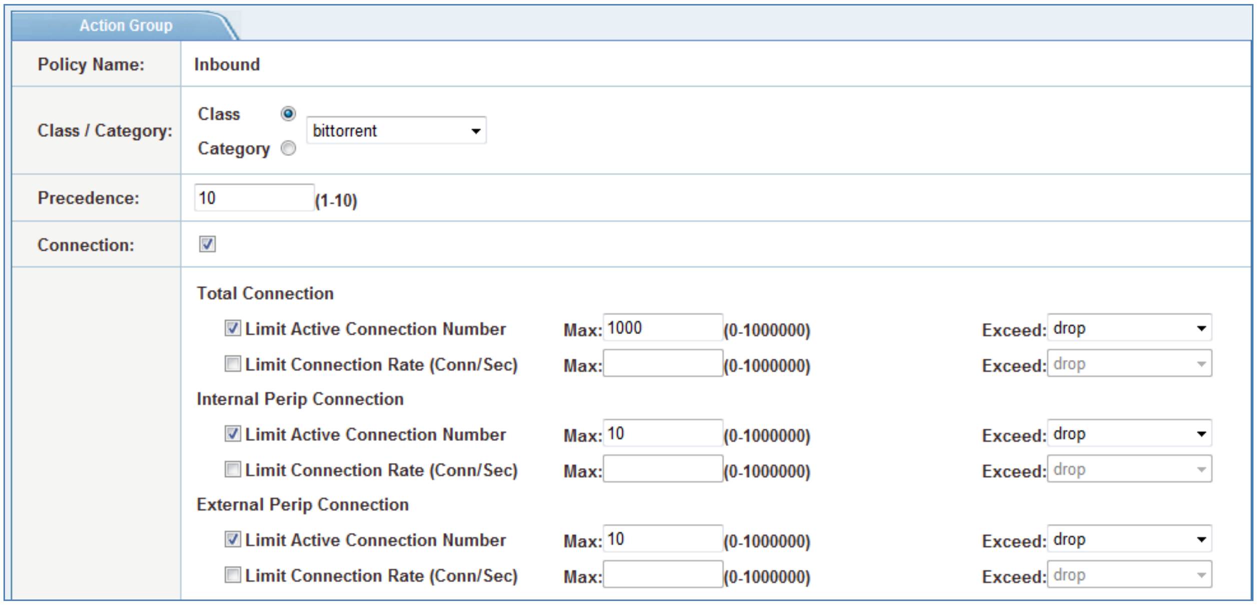
- As with all QoS Policy actions, connection limits must be bound with a QoS class.
- Connection limits can be used to limit the total number of connections for a QoS class.
- Connection limits can limit the number of connections for an IP address within a QoS class.
- The administrator can configure the EX appliance to drop or reject new connection requests once the connection limit has been reached.
    - Dropping means packets from the new connection request are silently dropped.
    - Rejecting means the EX appliance sends a TCP RST (TCP reset flag) to the client.
- Statistics are shown for the counters of the dropped connections under the action.
- The statistics only support real-time counters, which are shown as a part of the QoS interface statistics.

4.15.1 GUI Config

The QoS Policy Action for Connection Limits feature limits the total number of connections or connections per-IP address. This limit on the number of connections is defined within the QoS policy and is bound to a QoS class.

To configure a connection limit, do the following:

1. Select Config Mode > QoS > Policy.
2. On the menu bar, select Policy, if not already selected.
3. Click the New button. In the window that appears, enter a name in the Policy Name field.
4. Click the New button to create a new Action Group.
   A window similar to the one shown below appears:



Policy Name:	Inbound		
Class / Category:	Class ● Category ○	bittorrent	
Precedence:	10 (1-10)		
Connection:	☑		
	Total Connection		
	☑ Limit Active Connection Number	Max: 1000 (0-1000000)	Exceed: drop
	□ Limit Connection Rate (Conn/Sec)	Max: (0-1000000)	Exceed: drop
	Internal Perip Connection		
	☑ Limit Active Connection Number	Max: 10 (0-1000000)	Exceed: drop
	□ Limit Connection Rate (Conn/Sec)	Max: (0-1000000)	Exceed: drop
	External Perip Connection		
	☑ Limit Active Connection Number	Max: 10 (0-1000000)	Exceed: drop
	□ Limit Connection Rate (Conn/Sec)	Max: (0-1000000)	Exceed: drop

5. Select the Class radio button, and then click the drop-down menu and select one of the predefined QoS classes. In the example above, BitTorrent has been selected.
   Note: If desired, you can select a manually-created or auto-created QoS class, but these classes must already exist on the system to appear in the drop-down menu.
6. Click the Connection checkbox to display a number of connection options, as shown in the figure above.
   a. Under Total Connection, select the desired checkbox:
      - Limit Active Connection Number checkbox – Selecting this option will limit the total number of connections for this class.
      - Limit Connection Rate checkbox – Selecting this option will limit the number of connections per second that will be allowed for this class.
      - Max field – Enter the upper threshold for the number of connections.
      - Exceed drop-down menu – Select the action (drop or reject) that should occur when the threshold is exceeded.

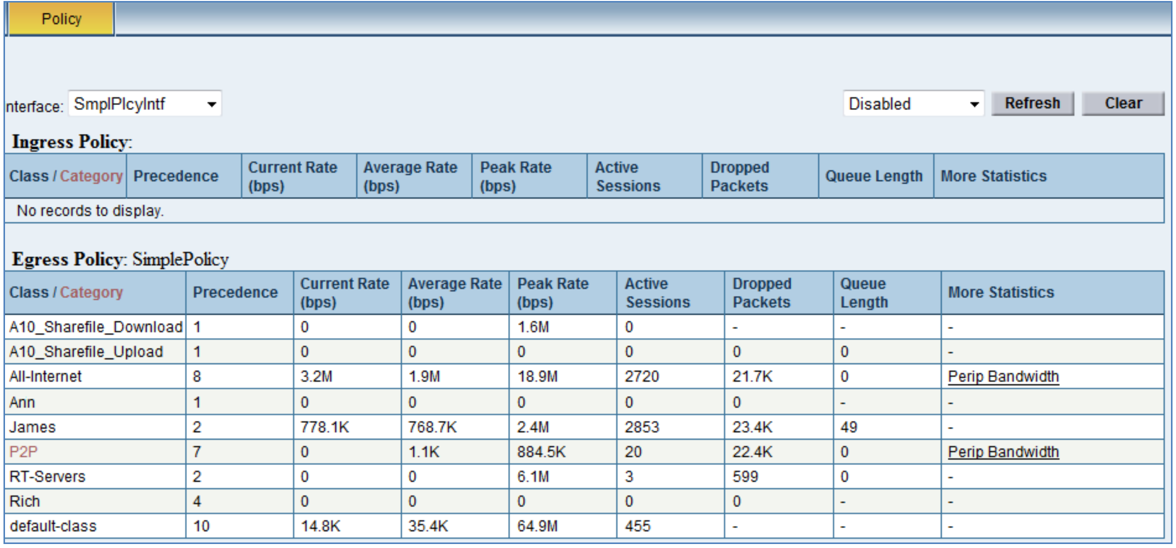
   b. Under Internal Per IP Connection, select the Limit Active Connection Number.
   c. Under External Per IP Connection, select the Limit Active Connection Number.
7. Click OK to save your changes.

Details:

- Entering a Max value of 0 will disallow any connections from occurring.
- In the “Action to overflow connection” field:
  - Drop means all packets in the new connection request will be silently dropped.
  - Reject means the EX appliance will send a TCP RST (reset) to the client.
  - The default action is to drop packets in new connection requests that exceed the configured threshold.

To display policy statistics for a QoS interface:

1. Select Monitor Mode > QoS > Policy.
2. From the Interface drop-down list, select the QoS interface.
   Statistics for the selected interface appear. Statistics are listed separately for the interface's ingress and egress policies.



nterface: SmplPlcyIntf

Disabled

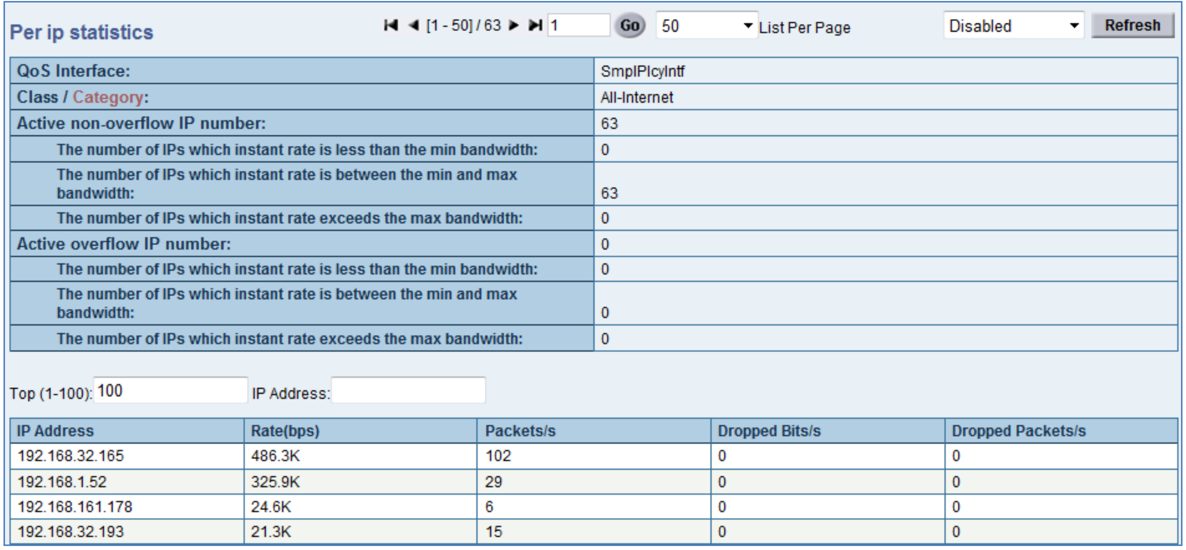
Ingress Policy:

Class / Category	Precedence	Current Rate (bps)	Average Rate (bps)	Peak Rate (bps)	Active Sessions	Dropped Packets	Queue Length	More Statistics
No records to display.								

Egress Policy: SimplePolicy

Class / Category	Precedence	Current Rate (bps)	Average Rate (bps)	Peak Rate (bps)	Active Sessions	Dropped Packets	Queue Length	More Statistics
A10_Sharefile_Download	1	0	0	1.6M	0	-	-	-
A10_Sharefile_Upload	1	0	0	0	0	0	0	-
All-Internet	8	3.2M	1.9M	18.9M	2720	21.7K	0	Perip Bandwidth
Ann	1	0	0	0	0	0	-	-
James	2	778.1K	768.7K	2.4M	2853	23.4K	49	-
P2P	7	0	1.1K	884.5K	20	22.4K	0	Perip Bandwidth
RT-Servers	2	0	0	6.1M	3	599	0	-
Rich	4	0	0	0	0	0	-	-
default-class	10	14.8K	35.4K	64.9M	455	-	-	-

3. The right-most column "More Statistics" includes a link that displays information about the Connection Limits associated with a particular policy. Click this link to display information on a per-IP basis, as shown below:



Per ip statistics

1 · 50 · Disabled

QoS Interface:	SmplPlcyIntf
Class / Category:	All-Internet
Active non-overflow IP number:	63
The number of IPs which instant rate is less than the min bandwidth:	0
The number of IPs which instant rate is between the min and max bandwidth:	63
The number of IPs which instant rate exceeds the max bandwidth:	0
Active overflow IP number:	0
The number of IPs which instant rate is less than the min bandwidth:	0
The number of IPs which instant rate is between the min and max bandwidth:	0
The number of IPs which instant rate exceeds the max bandwidth:	0

Top (1-100): 100 IP Address:

IP Address	Rate(bps)	Packets/s	Dropped Bits/s	Dropped Packets/s
192.168.32.165	486.3K	102	0	0
192.168.1.52	325.9K	29	0	0
192.168.161.178	24.6K	6	0	0
192.168.32.193	21.3K	15	0	0

4. If desired, you can display the QoS policy class detail page by navigating as follows: Monitor Mode > QoS > IP Limit. Then, enter the desired IP address in the IP Address field for which you wish to view the number of Dropped or Rejected connection requests.

4.15.2 CLI Config

To configure QoS Policy Total and Per-IP Connection Limits via the CLI, use the following commands:

To name the QoS policy:

```
EX1100(config)#qos policy Inbound
```

Set the precedence for the QoS class associated with the QoS Policy you are configuring:

```
EX1100(config-policy)#class mail-server-ip-list precedence 10 ?
  <cr>
```

To set the total number of connections for the QoS Class:

```
EX1100(config-policy-class)#connection ?
  total  Total connection limits
  perip  Per ip connection limits
```

To set the maximum number of active connections (as opposed to conn/sec) for the QoS Class:

```
EX1100(config-policy-class)#connection total max-?
  max-active  To set max active connection permitted
  max-rate    To set max connections/sec permitted
EX1100(config-policy-class)#connection total max-active ?
  <0-1000000>  The number of max active connection
EX1100(config-policy-class)#connection total max-active 10000
```

To set the connection limit for an IP address within a QoS Class:

```
EX1100(config-policy-class)#connection perip ?
  internal  Connection limiting for internal ip
  external  Connection limiting for external ip
EX1100(config-policy-class)#connection perip internal ?
  max-active  To set max active connection permitted
  max-rate    To set max connections/sec permitted
EX1100(config-policy-class)#connection perip internal max-active ?
  <0-1000000>  The number of max active connection
EX1100(config-policy-class)#connection perip internal max-active 10
```

To drop connection requests that exceed the maximum configured threshold:

```
EX1100(config-policy-class)#connection total max-active 10 action ?
  drop    Drop the packets
  reject  Drop the packets, and send RST packet for tcp connection
EX1100(config-policy-class)#connection total max-active 10 action drop
```

4.16 Report CSV Format

In prior releases, report formats included HTTP, PDF, and XML. With this latest release, users can now add CSV to the list of supported formats for generating reports from the EX appliance. This new format allows customers to more easily import data into other third-party databases.

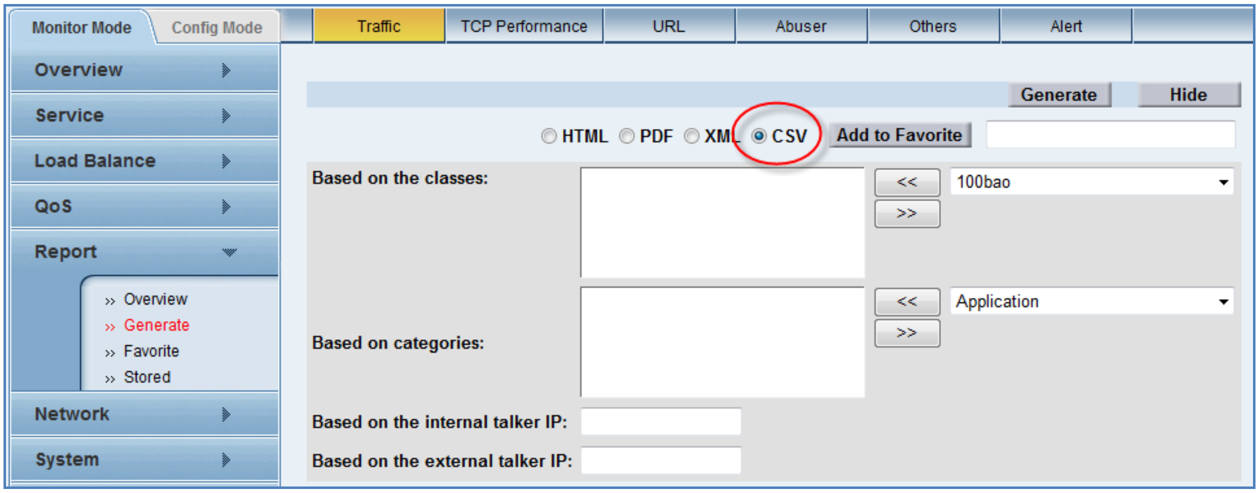
Details:

- Each report type is generated as a separate CSV file.
- When several reports are generated, the multiple CSV files will be bundled into a single .tar archive file.
- The exported CSV file will include the report title, time, and column headers, with data following.
- The extension of the CSV file will be .csv.

4.16.1 GUI Config

To generate a report from the EX appliance in CSV format:

1. Select Monitor Mode > Report > Generate.
2. On the menu bar, select the desired module (e.g. Traffic, URL, etc.).
   A window similar to the one shown below appears:



○ HTML ○ PDF ○ XML ● CSV

Based on the classes: 100bao

Based on categories: Application

Based on the internal talker IP:

Based on the external talker IP:

3. Select the CSV radio button, as shown in the figure above.
4. Select the desired classes using the << button and drop-down menu.
5. Click the Generate button to create the CSV file.
6. If desired, you can save the file on the EX or on a remote server by clicking the Export button.
   Note: For additional details on generating reports, please refer to the *EX GUI User Manual* or *EX CLI User Manual*.

4.16.2 CLI Config

You can generate a favorite report file in CSV format by executing the following CLI commands:

```
EX(config)#report favorite ?
  traffic  Report for general traffic statistics
  tcp      Report for tcp statistics
  url      Report for url statistics
  abuser   Report for abuser statistics
  others   Report for others ip port statistics
```

Specify the desired type of report (e.g. traffic, tcp, url, etc.), and enter the name of the template:

```
EX(config)#report favorite url ?
  LINE  Template name
```

Next, specify the preferred format for the output:

```
EX(config-report-favorite)#format ?
  html  HTML format
  pdf   PDf format
  xml   XML format
  csv   CSV format

EX(config-report-favorite)#format pdf ?
 <cr>
```

4.17 SIP Application Layer Gateway Support for NAT

For this latest release, the EX appliance has been enhanced to make Network Address Translation (NAT) work with applications that use the SIP protocol, such as VoIP.

Session Initiation Protocol (SIP) is a text-based protocol that allows network nodes to discover one another and establish multimedia sessions. The SIP protocol can establish or tear down sessions, and it works independently of the underlying transport protocols.

This enhancement is transparent to the user and requires no configuration of the EX appliance.

4.17.1 GUI Config

There is no user configuration required.

4.17.2 CLI Config

There is no user configuration required.

4.18 TCP Optimization

The EX is capable of optimizing the TCP protocol to help manage the traffic bandwidth. This is a global configuration that is available via the CLI.

4.18.1 GUI Config

This feature can only be enabled and disabled via the EX CLI.

4.18.2 CLI Config

The TCP Optimization feature is disabled by default. You can enable the feature by executing the following command:

```
EX(config)#qos tcp-optimization enable
```

To disabled the TCP Optimization feature, use the following command:

```
EX(config)#no qos tcp-optimization enable
```

4.19 Transparent Health Methods

A new health monitoring option allows a TCP (Layer 4) health method to be used to check the health of a multilink path.

4.19.1 CLI Config

To configure a TCP health method for use across a multi-link path, use the following command at the global configuration level of the CLI:

```
[no] health method method-name tcp port port-num halfopen transparent
ipaddr
```

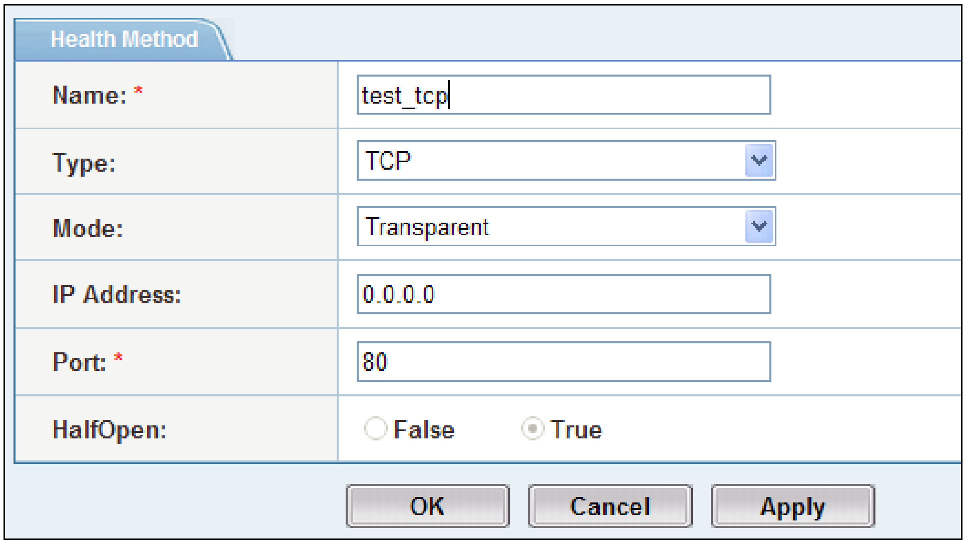
The following example configures a health method named "tcp_method" that checks the health of device 192.168.3.1 across a multi-link path by sending a health check to TCP port 80 on the device.

```
EX(config)#health method tcp_method tcp port 80 halfopen transparent
192.168.3.1
```

4.19.2 GUI Config

To configure a TCP health method for use across a multi-link path:

1. Select Config Mode > Load Balance > Health Monitor.
2. On the menu bar, select Health Method.
3. Click the New button. The Health Method tab appears.



Name: *	test_tcp
Type:	TCP
Mode:	Transparent
IP Address:	0.0.0.0
Port: *	80
HalfOpen:	○ False ● True

4. From the Type drop-down list, select TCP.
5. From the Mode drop-down list, select Transparent.

6. In the IP address field, enter the IP address of the device to which to send the health check. (The example above shows 0.0.0.0. Make sure to enter the IP address of the device at the other end of the link.)
7. In the Port field, enter the TCP port number to which to send the health check.
8. Select the True radio button (next to HalfOpen).
9. Click OK.

Note: With "HalfOpen" configured, the EX will try to establish a TCP session and will expect to see the proper ACK packet back from the IP address. With "HalfOpen" not configured, the EX will simply make sure that the path to the IP address is not blocked.

4.20 Multiple Health Methods per Health Monitor

A health monitor can now include multiple health methods, rather than being limited to only one method per monitor. By default, all methods must pass for the health check to pass. You can specify the minimum number of successful health methods required to declare a healthy status.

4.20.1 CLI Config

To configure a health monitor that contains multiple health methods, configure the individual health methods, and then configure a monitor that uses the methods. Optionally, specify the minimum number of methods that must pass in order for the device to pass the health check. By default, all methods must pass.

Create the health methods:

```
EX(config)#health method method1 tcp port 80
EX(config)#health method method2 ftp
EX(config)#health method method3 icmp
```

Create the health monitor:

```
EX(config)#health monitor health-monitor
EX(config-health-monitor)# ?
  interval              Specify the healthcheck interval
  method                Specify the used checking method
  min_active_cnt        Specify the min count of successful method
  retry                 Specify the healthcheck retries
  timeout               Specify the healthcheck timeout
```

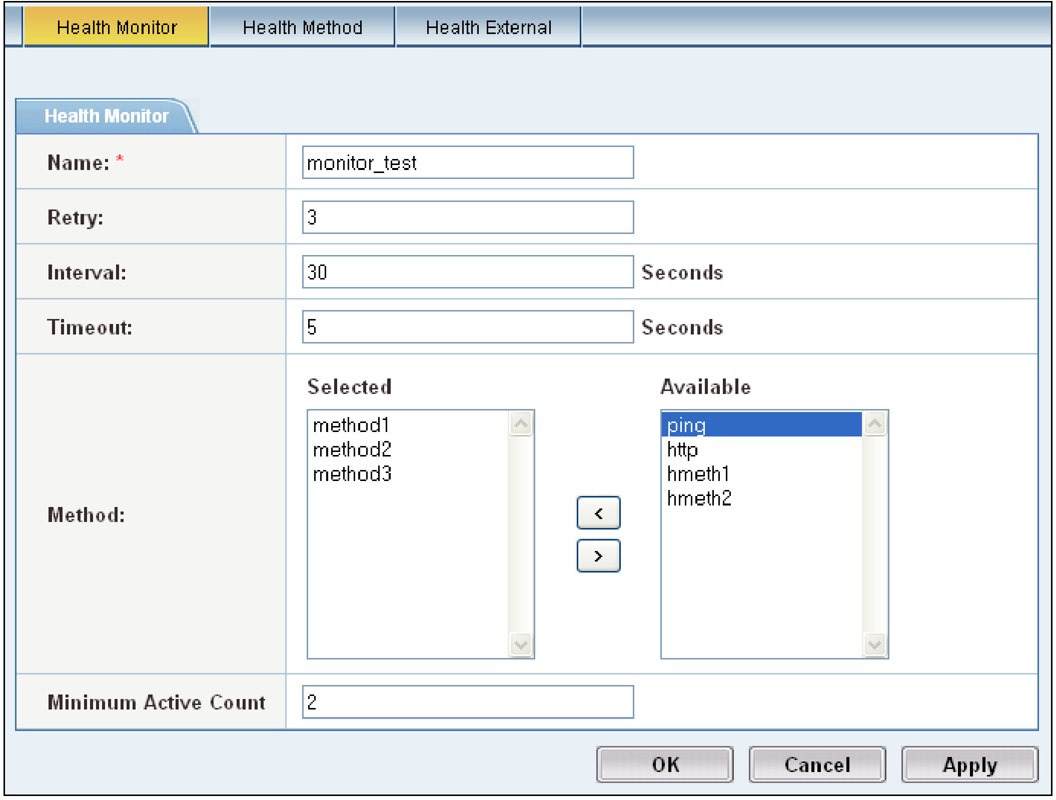
Add the health methods to the health monitor:

```
EX(config)#health monitor monitor_test
EX(config-health-monitor)#method method1
EX(config-health-monitor)#method method2
EX(config-health-monitor)#method method3
EX(config-health-monitor)#min-active-cnt 2
```

4.20.2 GUI Config

To configure a health monitor that has multiple health methods:

1. Select Config Mode > Load Balance > Health Monitor.
2. On the menu bar, select Health Monitor.
3. Click the New button. The Health Monitor tab appears.



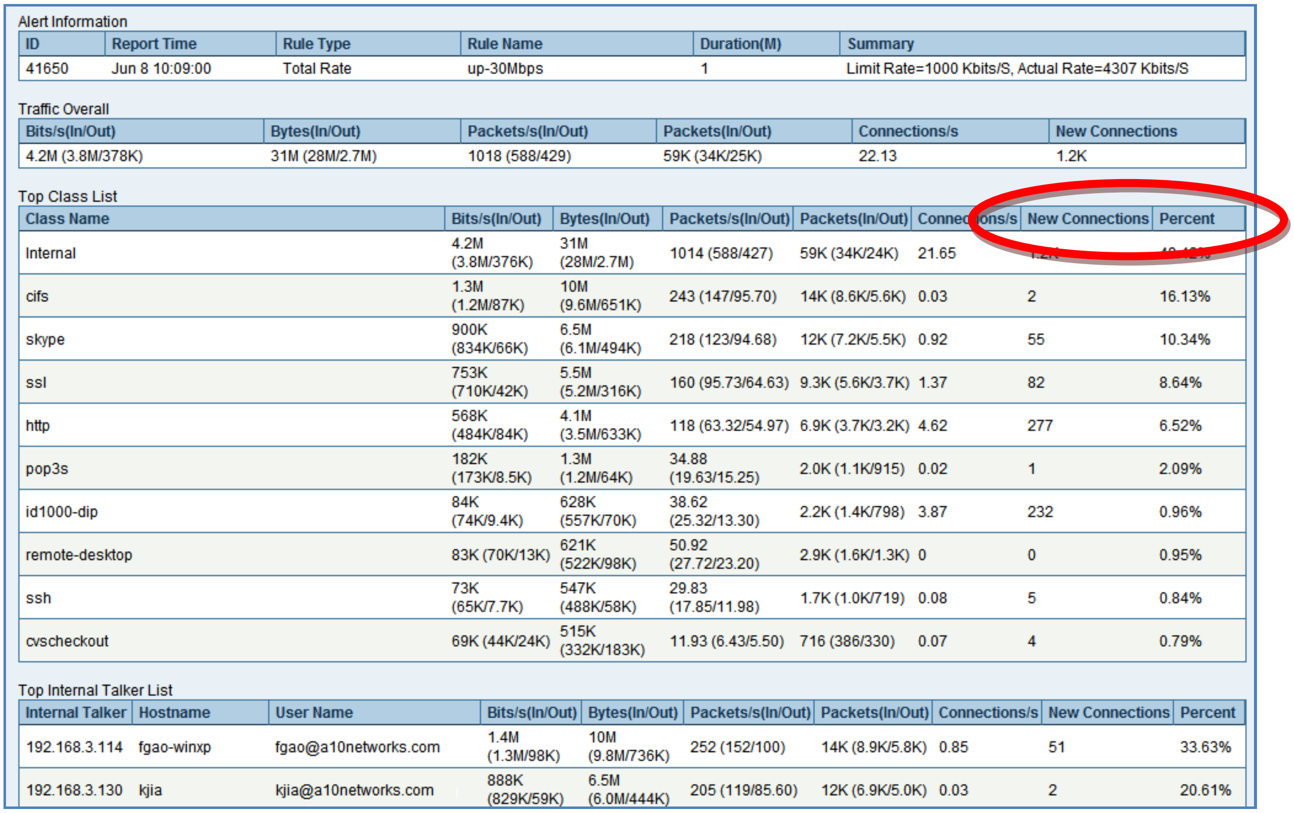
Name: *	monitor_test
Retry:	3
Interval:	30 Seconds
Timeout:	5 Seconds
Method:	Selected: method1 method2 method3 Available: ping http hmeth1 hmeth2
Minimum Active Count	2

4. Enter the Health Monitor Name in the Name field.
5. (Optional) Edit the defaults for Retry, Interval, and Timeout, if desired.
6. Select the desired Health Method from the “Available” list on the right, and click << to move it to the “Selected” field on the left.
   Note: A Health Monitor can contain a maximum of 10 Health Methods.
7. Enter a value in the Minimum Active Count field to determine how many of the Selected Health Methods must pass in order for the overall Health Monitor to pass.
   Note: If 3 health methods are selected and you want the check to pass if any 2 out of 3 methods pass, then you would enter 2 in the Minimum Active Count field. Alternatively (and counter intuitively), you could enter 0 as a shorthand way to indicate that the health monitor will only pass if ***all*** Selected methods pass.
8. Click OK to save your changes.

4.21 Enhanced Alert Content

4.21.1 Total Rate Alert Report

Columns for New Connections and Percent have been added to Total Rate Alert Reports.



Alert Information

ID	Report Time	Rule Type	Rule Name	Duration(M)	Summary
41650	Jun 8 10:09:00	Total Rate	up-30Mbps	1	Limit Rate=1000 Kbits/S, Actual Rate=4307 Kbits/S

Traffic Overall

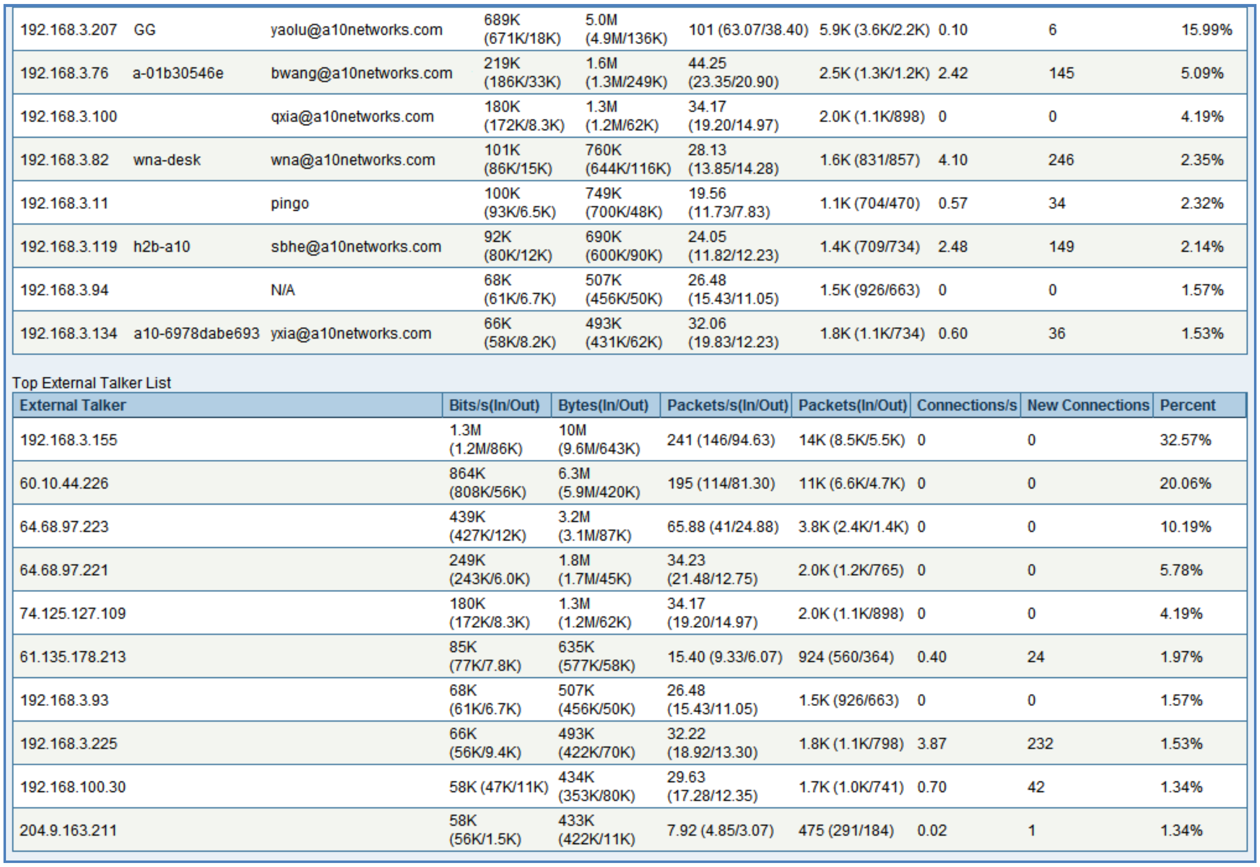
Bits/s(In/Out)	Bytes(In/Out)	Packets/s(In/Out)	Packets(In/Out)	Connections/s	New Connections
4.2M (3.8M/378K)	31M (28M/2.7M)	1018 (588/429)	59K (34K/25K)	22.13	1.2K

Top Class List

Class Name	Bits/s(In/Out)	Bytes(In/Out)	Packets/s(In/Out)	Packets(In/Out)	Connections/s	New Connections	Percent
Internal	4.2M (3.8M/376K)	31M (28M/2.7M)	1014 (588/427)	59K (34K/24K)	21.65	1.2K	40.42%
cifs	1.3M (1.2M/87K)	10M (9.6M/651K)	243 (147/95.70)	14K (8.6K/5.6K)	0.03	2	16.13%
skype	900K (834K/66K)	6.5M (6.1M/494K)	218 (123/94.68)	12K (7.2K/5.5K)	0.92	55	10.34%
ssl	753K (710K/42K)	5.5M (5.2M/316K)	160 (95.73/64.63)	9.3K (5.6K/3.7K)	1.37	82	8.64%
http	568K (484K/84K)	4.1M (3.5M/633K)	118 (63.32/54.97)	6.9K (3.7K/3.2K)	4.62	277	6.52%
pop3s	182K (173K/8.5K)	1.3M (1.2M/64K)	34.88 (19.63/15.25)	2.0K (1.1K/915)	0.02	1	2.09%
id1000-dip	84K (74K/9.4K)	628K (557K/70K)	38.62 (25.32/13.30)	2.2K (1.4K/798)	3.87	232	0.96%
remote-desktop	83K (70K/13K)	621K (522K/98K)	50.92 (27.72/23.20)	2.9K (1.6K/1.3K)	0	0	0.95%
ssh	73K (65K/7.7K)	547K (488K/58K)	29.83 (17.85/11.98)	1.7K (1.0K/719)	0.08	5	0.84%
cvscheckout	69K (44K/24K)	515K (332K/183K)	11.93 (6.43/5.50)	716 (386/330)	0.07	4	0.79%

Top Internal Talker List

Internal Talker	Hostname	User Name	Bits/s(In/Out)	Bytes(In/Out)	Packets/s(In/Out)	Packets(In/Out)	Connections/s	New Connections	Percent
192.168.3.114	fgao-winxp	fgao@a10networks.com	1.4M (1.3M/98K)	10M (9.8M/736K)	252 (152/100)	14K (8.9K/5.8K)	0.85	51	33.63%
192.168.3.130	kjia	kjia@a10networks.com	888K (829K/59K)	6.5M (6.0M/444K)	205 (119/85.60)	12K (6.9K/5.0K)	0.03	2	20.61%



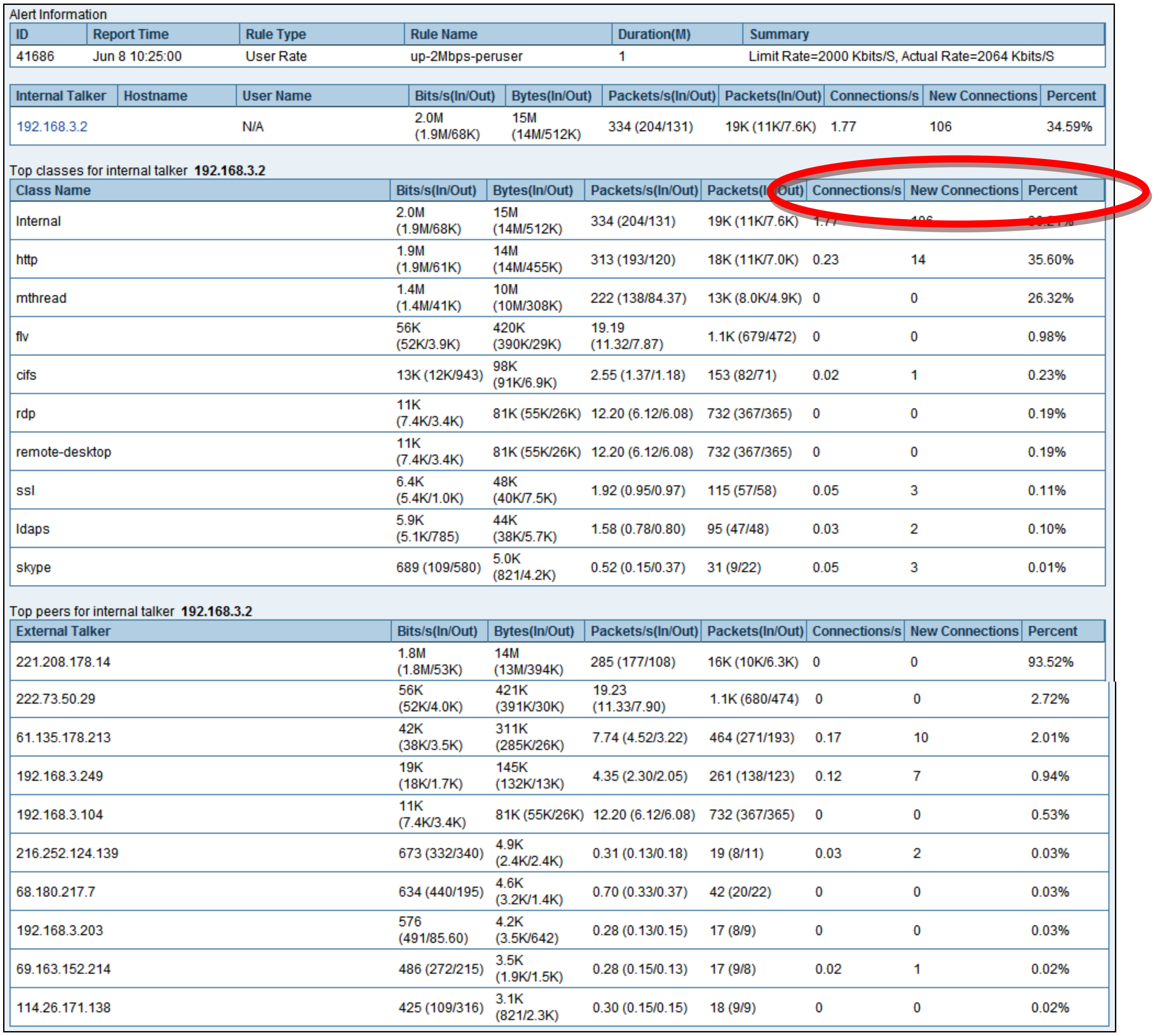
192.168.3.207	GG	yaolu@a10networks.com	689K (671K/18K)	5.0M (4.9M/136K)	101 (63.07/38.40)	5.9K (3.6K/2.2K)	0.10	6	15.99%
192.168.3.76	a-01b30546e	bwang@a10networks.com	219K (186K/33K)	1.6M (1.3M/249K)	44.25 (23.35/20.90)	2.5K (1.3K/1.2K)	2.42	145	5.09%
192.168.3.100		qxia@a10networks.com	180K (172K/8.3K)	1.3M (1.2M/62K)	34.17 (19.20/14.97)	2.0K (1.1K/898)	0	0	4.19%
192.168.3.82	wna-desk	wna@a10networks.com	101K (86K/15K)	760K (644K/116K)	28.13 (13.85/14.28)	1.6K (831/857)	4.10	246	2.35%
192.168.3.11		pingo	100K (93K/6.5K)	749K (700K/48K)	19.56 (11.73/7.83)	1.1K (704/470)	0.57	34	2.32%
192.168.3.119	h2b-a10	sbhe@a10networks.com	92K (80K/12K)	690K (600K/90K)	24.05 (11.82/12.23)	1.4K (709/734)	2.48	149	2.14%
192.168.3.94		N/A	68K (61K/6.7K)	507K (456K/50K)	26.48 (15.43/11.05)	1.5K (926/663)	0	0	1.57%
192.168.3.134	a10-6978dabe693	yxia@a10networks.com	66K (58K/8.2K)	493K (431K/62K)	32.06 (19.83/12.23)	1.8K (1.1K/734)	0.60	36	1.53%

Top External Talker List

External Talker	Bits/s(In/Out)	Bytes(In/Out)	Packets/s(In/Out)	Packets(In/Out)	Connections/s	New Connections	Percent
192.168.3.155	1.3M (1.2M/86K)	10M (9.6M/643K)	241 (146/94.63)	14K (8.5K/5.5K)	0	0	32.57%
60.10.44.226	864K (808K/56K)	6.3M (5.9M/420K)	195 (114/81.30)	11K (6.6K/4.7K)	0	0	20.06%
64.68.97.223	439K (427K/12K)	3.2M (3.1M/87K)	65.88 (41/24.88)	3.8K (2.4K/1.4K)	0	0	10.19%
64.68.97.221	249K (243K/6.0K)	1.8M (1.7M/45K)	34.23 (21.48/12.75)	2.0K (1.2K/765)	0	0	5.78%
74.125.127.109	180K (172K/8.3K)	1.3M (1.2M/62K)	34.17 (19.20/14.97)	2.0K (1.1K/898)	0	0	4.19%
61.135.178.213	85K (77K/7.8K)	635K (577K/58K)	15.40 (9.33/6.07)	924 (560/364)	0.40	24	1.97%
192.168.3.93	68K (61K/6.7K)	507K (456K/50K)	26.48 (15.43/11.05)	1.5K (926/663)	0	0	1.57%
192.168.3.225	66K (56K/9.4K)	493K (422K/70K)	32.22 (18.92/13.30)	1.8K (1.1K/798)	3.87	232	1.53%
192.168.100.30	58K (47K/11K)	434K (353K/80K)	29.63 (17.28/12.35)	1.7K (1.0K/741)	0.70	42	1.34%
204.9.163.211	58K (56K/1.5K)	433K (422K/11K)	7.92 (4.85/3.07)	475 (291/184)	0.02	1	1.34%

4.21.2 User Rate Alert Report

Columns for Connections, New Connections, and Percent have been added to the User Rate Alert Reports.



Alert Information

ID	Report Time	Rule Type	Rule Name	Duration(M)	Summary
41686	Jun 8 10:25:00	User Rate	up-2Mbps-peruser	1	Limit Rate=2000 Kbits/S, Actual Rate=2064 Kbits/S

Internal Talker	Hostname	User Name	Bits/s(In/Out)	Bytes(In/Out)	Packets/s(In/Out)	Packets(In/Out)	Connections/s	New Connections	Percent
192.168.3.2		N/A	2.0M (1.9M/68K)	15M (14M/512K)	334 (204/131)	19K (11K/7.6K)	1.77	106	34.59%

Top classes for internal talker **192.168.3.2**

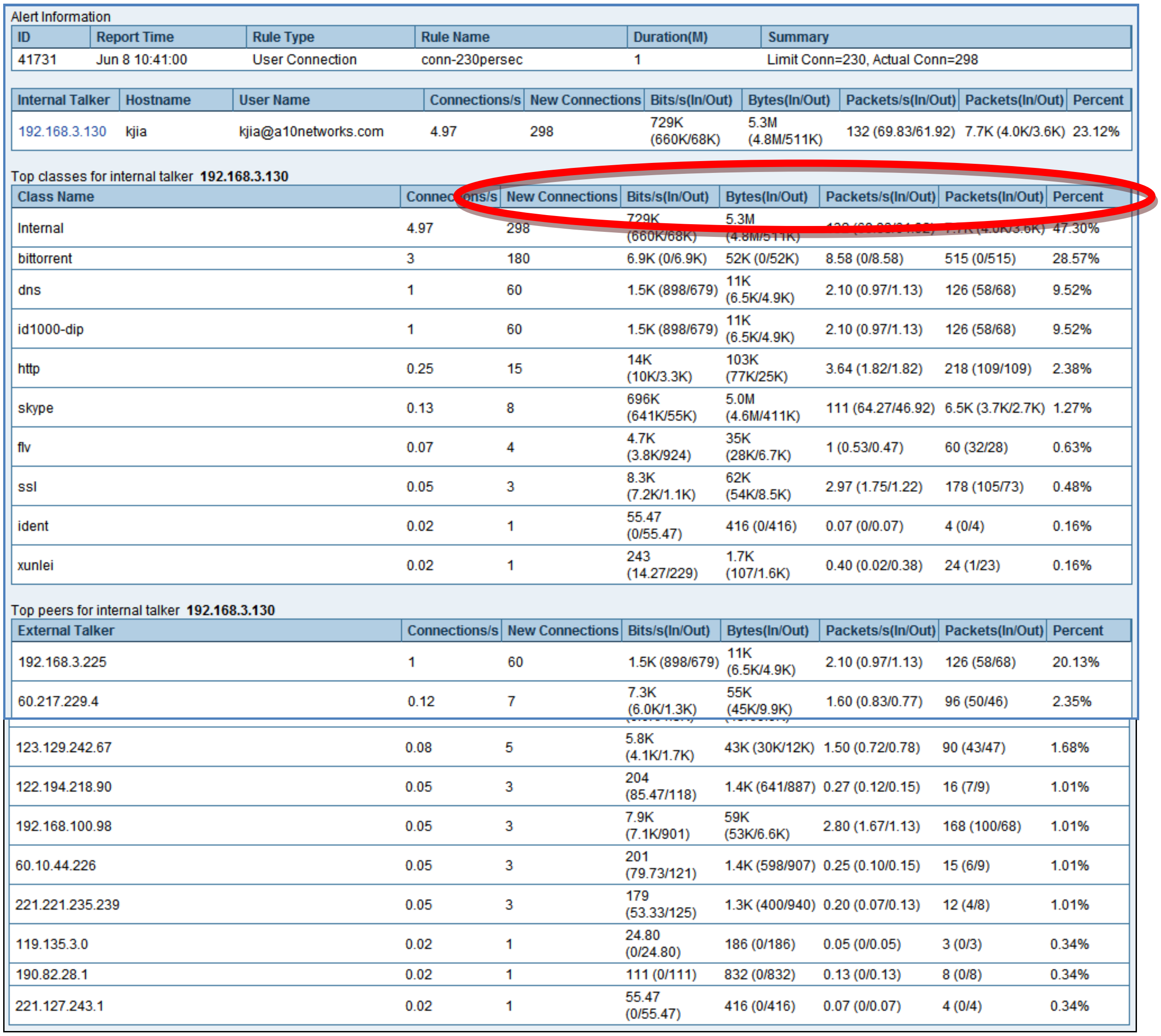
Class Name	Bits/s(In/Out)	Bytes(In/Out)	Packets/s(In/Out)	Packets(In/Out)	Connections/s	New Connections	Percent
Internal	2.0M (1.9M/68K)	15M (14M/512K)	334 (204/131)	19K (11K/7.6K)	1.77	106	99.21%
http	1.9M (1.9M/61K)	14M (14M/455K)	313 (193/120)	18K (11K/7.0K)	0.23	14	35.60%
mthread	1.4M (1.4M/41K)	10M (10M/308K)	222 (138/84.37)	13K (8.0K/4.9K)	0	0	26.32%
flv	56K (52K/3.9K)	420K (390K/29K)	19.19 (11.32/7.87)	1.1K (679/472)	0	0	0.98%
cifs	13K (12K/943)	98K (91K/6.9K)	2.55 (1.37/1.18)	153 (82/71)	0.02	1	0.23%
rdp	11K (7.4K/3.4K)	81K (55K/26K)	12.20 (6.12/6.08)	732 (367/365)	0	0	0.19%
remote-desktop	11K (7.4K/3.4K)	81K (55K/26K)	12.20 (6.12/6.08)	732 (367/365)	0	0	0.19%
ssl	6.4K (5.4K/1.0K)	48K (40K/7.5K)	1.92 (0.95/0.97)	115 (57/58)	0.05	3	0.11%
ldaps	5.9K (5.1K/785)	44K (38K/5.7K)	1.58 (0.78/0.80)	95 (47/48)	0.03	2	0.10%
skype	689 (109/580)	5.0K (821/4.2K)	0.52 (0.15/0.37)	31 (9/22)	0.05	3	0.01%

Top peers for internal talker **192.168.3.2**

External Talker	Bits/s(In/Out)	Bytes(In/Out)	Packets/s(In/Out)	Packets(In/Out)	Connections/s	New Connections	Percent
221.208.178.14	1.8M (1.8M/53K)	14M (13M/394K)	285 (177/108)	16K (10K/6.3K)	0	0	93.52%
222.73.50.29	56K (52K/4.0K)	421K (391K/30K)	19.23 (11.33/7.90)	1.1K (680/474)	0	0	2.72%
61.135.178.213	42K (38K/3.5K)	311K (285K/26K)	7.74 (4.52/3.22)	464 (271/193)	0.17	10	2.01%
192.168.3.249	19K (18K/1.7K)	145K (132K/13K)	4.35 (2.30/2.05)	261 (138/123)	0.12	7	0.94%
192.168.3.104	11K (7.4K/3.4K)	81K (55K/26K)	12.20 (6.12/6.08)	732 (367/365)	0	0	0.53%
216.252.124.139	673 (332/340)	4.9K (2.4K/2.4K)	0.31 (0.13/0.18)	19 (8/11)	0.03	2	0.03%
68.180.217.7	634 (440/195)	4.6K (3.2K/1.4K)	0.70 (0.33/0.37)	42 (20/22)	0	0	0.03%
192.168.3.203	576 (491/85.60)	4.2K (3.5K/642)	0.28 (0.13/0.15)	17 (8/9)	0	0	0.03%
69.163.152.214	486 (272/215)	3.5K (1.9K/1.5K)	0.28 (0.15/0.13)	17 (9/8)	0.02	1	0.02%
114.26.171.138	425 (109/316)	3.1K (821/2.3K)	0.30 (0.15/0.15)	18 (9/9)	0	0	0.02%

4.21.3 User Connection Alert Report

Columns for New Connections, Bits/s(In/Out), Bytes(In/Out), Packets/s(In/Out), Packets(In/Out), and Percent have been added to the User Connection Alert Reports.



Alert Information

ID	Report Time	Rule Type	Rule Name	Duration(M)	Summary
41731	Jun 8 10:41:00	User Connection	conn-230persec	1	Limit Conn=230, Actual Conn=298

Internal Talker	Hostname	User Name	Connections/s	New Connections	Bits/s(In/Out)	Bytes(In/Out)	Packets/s(In/Out)	Packets(In/Out)	Percent
192.168.3.130	kjia	kjia@a10networks.com	4.97	298	729K (660K/68K)	5.3M (4.8M/511K)	132 (69.83/61.92)	7.7K (4.0K/3.6K)	23.12%

Top classes for internal talker **192.168.3.130**

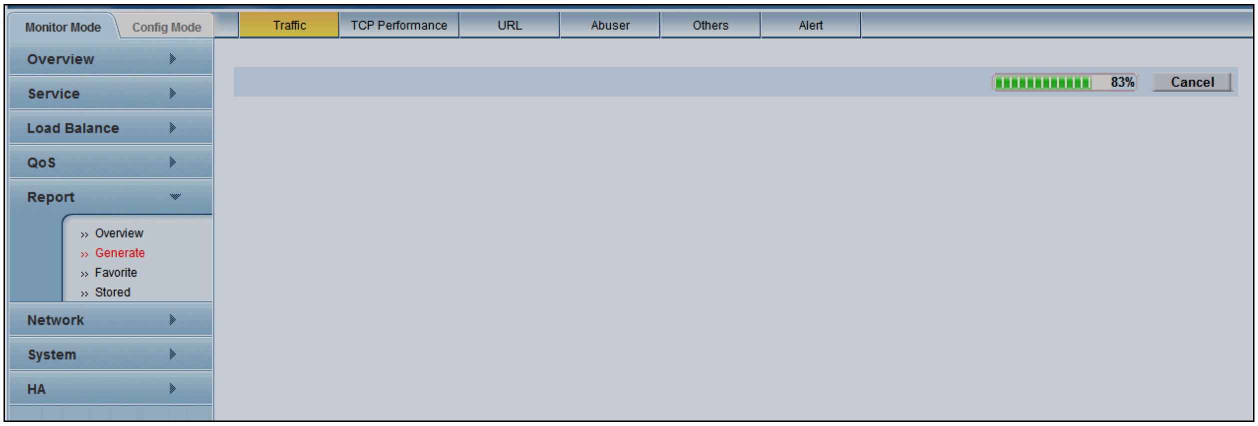
Class Name	Connections/s	New Connections	Bits/s(In/Out)	Bytes(In/Out)	Packets/s(In/Out)	Packets(In/Out)	Percent
Internal	4.97	298	729K (660K/68K)	5.3M (4.8M/511K)	132 (69.83/61.92)	7.7K (4.0K/3.6K)	47.30%
bittorrent	3	180	6.9K (0/6.9K)	52K (0/52K)	8.58 (0/8.58)	515 (0/515)	28.57%
dns	1	60	1.5K (898/679)	11K (6.5K/4.9K)	2.10 (0.97/1.13)	126 (58/68)	9.52%
id1000-dip	1	60	1.5K (898/679)	11K (6.5K/4.9K)	2.10 (0.97/1.13)	126 (58/68)	9.52%
http	0.25	15	14K (10K/3.3K)	103K (77K/25K)	3.64 (1.82/1.82)	218 (109/109)	2.38%
skype	0.13	8	696K (641K/55K)	5.0M (4.6M/411K)	111 (64.27/46.92)	6.5K (3.7K/2.7K)	1.27%
flv	0.07	4	4.7K (3.8K/924)	35K (28K/6.7K)	1 (0.53/0.47)	60 (32/28)	0.63%
ssl	0.05	3	8.3K (7.2K/1.1K)	62K (54K/8.5K)	2.97 (1.75/1.22)	178 (105/73)	0.48%
ident	0.02	1	55.47 (0/55.47)	416 (0/416)	0.07 (0/0.07)	4 (0/4)	0.16%
xunlei	0.02	1	243 (14.27/229)	1.7K (107/1.6K)	0.40 (0.02/0.38)	24 (1/23)	0.16%

Top peers for internal talker **192.168.3.130**

External Talker	Connections/s	New Connections	Bits/s(In/Out)	Bytes(In/Out)	Packets/s(In/Out)	Packets(In/Out)	Percent
192.168.3.225	1	60	1.5K (898/679)	11K (6.5K/4.9K)	2.10 (0.97/1.13)	126 (58/68)	20.13%
60.217.229.4	0.12	7	7.3K (6.0K/1.3K)	55K (45K/9.9K)	1.60 (0.83/0.77)	96 (50/46)	2.35%
123.129.242.67	0.08	5	5.8K (4.1K/1.7K)	43K (30K/12K)	1.50 (0.72/0.78)	90 (43/47)	1.68%
122.194.218.90	0.05	3	204 (85.47/118)	1.4K (641/887)	0.27 (0.12/0.15)	16 (7/9)	1.01%
192.168.100.98	0.05	3	7.9K (7.1K/901)	59K (53K/6.6K)	2.80 (1.67/1.13)	168 (100/68)	1.01%
60.10.44.226	0.05	3	201 (79.73/121)	1.4K (598/907)	0.25 (0.10/0.15)	15 (6/9)	1.01%
221.221.235.239	0.05	3	179 (53.33/125)	1.3K (400/940)	0.20 (0.07/0.13)	12 (4/8)	1.01%
119.135.3.0	0.02	1	24.80 (0/24.80)	186 (0/186)	0.05 (0/0.05)	3 (0/3)	0.34%
190.82.28.1	0.02	1	111 (0/111)	832 (0/832)	0.13 (0/0.13)	8 (0/8)	0.34%
221.127.243.1	0.02	1	55.47 (0/55.47)	416 (0/416)	0.07 (0/0.07)	4 (0/4)	0.34%

4.22 Report Generation Progress Bar

A progress bar now displays the percentage complete of reports being generated.



4.23 Configure Report Templates and Schedules via CLI

The EX now supports new CLI commands for configuring report templates. Before this release, report template configuration is supported only in the GUI.

You can configure templates for the same types of reports configurable in the GUI:

- Traffic
- TCP Performance
- URL
- Abuser
- Others

To begin configuring a report template, use the following command at the global configuration level of the CLI:

`report favorite` *`report-type template-name`*

The *report-type* can be one of the following:

- **`traffic`**
- **`tcp`**
- **`url`**
- **`abuser`**
- **`others`**

This command changes the CLI to the configuration level for the template, where the following commands are available.

4.23.1 Commands for Report Templates Parameters for All Types

The following commands apply to all report template types:

```
period {minutes | hours | days | weeks | months} num
[before {now | mm/dd/yyyy hh:mm}]
```

This command defines the statistics time period for report content.

```
format {html | pdf | xml}
```

This command defines the format for the generated report.

```
schedule [start-time mm/dd/yyyy] [end-time mm/dd/yyyy]
{per-day | per-week | per-month}…
```

This command defines when to generate the report. The **start-time** and **end-time** options define the time period for the schedule. The schedule can be per-day, per-week, or per-month:

```
  schedule per-day num time hh:mm [hh:mm …]

  schedule per-weeks num
  at {Monday | Tuesday | Wednesday … […]} [time hh:mm …]

  schedule per-month num at {day | last-day-of-month}
  {time hh:mm [hh:mm …] | day | last-day-of-month}
```

To enable the schedule, use the following command:

```
  schedule enable
```

```
email [email-address1, email-address2 …]
```

This command specifies the email addresses to which to send the reports that are generated using the template.

4.23.2 Commands Applicable to Traffic Report Templates

Traffic reports show graphs and statistics for the following:

- Traffic rate
- Number of connections
- Packet size distribution

For each type of statistic, you can enable the following:

- Overall
- Top 10 Classes
- Top 10 Talkers

The **overall** option is enabled by default. The **top-class**, **top-internal-talker**, and **top-external-talker** options are disabled by default. The **top-num** option specifies how many classes or talkers to include. The default is 10.

By default, statistics are shown for all classes, internal talker IPs, and external talker IPs. You can narrow the scope of the report by specifying any of the following:

- Specific classes
- Specific internal talker IP
- Specific external talker IP

Statistics for all (both) inbound and outbound connection and packet directions are shown. For traffic rate, you can change the direction to inbound or outbound connections only. For packet distribution, you can change the connection direction and packet direction individually, to inbound or outbound.

The following commands apply specifically to traffic report templates:

```
scope class class-name [class-name …] [internal-talker ipaddr]
[external-talker ipaddr]

scope class internal-talker ipaddr [external-talker ipaddr]
[class-name [class-name …]]

scope class external-talker ipaddr [internal-talker ipaddr]
[class-name [class-name …]]

content rate overall conn-dir {inbound | outbound}

content rate top-class [view view-name]
[conn-dir {inbound | outbound}] [top-num num]

content rate top-internal-talker [conn-dir {inbound | outbound}]
[top-num num]
```

```
content rate top-external-talker [conn-dir {inbound | outbound}]
[top-num num]
```

```
content connection overall
```

```
content connection top-class [view view-name] [top-num num]
```

```
content connection top-internal-talker [top-num num]
```

```
content connection top-external-talker [top-num num]
```

```
content packet-distribution overall
[conn-dir {inbound | outbound}] [packet-dir {inbound | outbound}]
```

```
content packet-distribution top-class [view view-name]
[large-packet-size size] [conn-dir {inbound | outbound}]
[packet-dir {inbound | outbound}] [top-num num]
```

```
content packet-distribution top-internal-talker
[large-packet-size size] [conn-dir {inbound | outbound}]
[packet-dir {inbound | outbound}] [top-num num]
```

4.23.3 Commands Applicable to TCP Report Templates

TCP performance reports shows graphs and statistics for the following:

- Efficiency
- Round-trip-time (RTT)
- Connection health (Conn-Health)

By default, statistics are shown for all classes and for both packet and connection directions. You can narrow the scope of the report by selecting individual classes, and by selecting inbound or outbound for the packet or connection direction.

The following commands apply specifically to TCP report templates:

```
scope class class-name
```

```
content tcp efficiency [packet-dir {inbound | outbound}]
```

```
content tcp conn-health [conn-dir {inbound | outbound}]
```

```
content tcp rtt
```

4.23.4 Commands Applicable to URL Report Templates

URL reports show the URLs accessed by internal talkers during the report period and list the most active internal talker IP addresses.

By default, overall statistics are displayed, as well as the 10 most active URLs and the 10 most active internal talkers.

You can narrow the scope of the report by entering a specific URL string, internal talker IP, or both. You also can change the number of URLs or talker IPs listed in the report output.

The following commands apply specifically to URL report templates:

```
scope url url-path [talker ipaddr]

scope talker ipaddr [url url-path]

content url overall

content url top-url [top-num num]

content url top-talker [top-num num]
```

4.23.5 Commands Applicable to Abuser Report Templates

Abuser reports show statistics for users who were in the abuser class during the report period. Users are placed in the abuser class when their network activity exceeds the thresholds specified by the configured abuser criteria.

By default, the 10 most active abusers are listed, by username. You can change the number of abusers listed. You also can select to list them by IP address instead of username.

The following command applies specifically to network abuser report templates:

```
content abuser top base-on {ip | user} [top-num num]
```

4.23.6 Commands Applicable to Others Report Templates

Others reports show activity for the Others traffic class. By default, overall statistics are shown for all IP addresses and Layer 4 protocol ports by source address.

You can narrow the scope of the report by entering a specific IP address or protocol port. You also can enable statistics for the following:

- Top services (listed by IP address and protocol port)
- Top IP addresses
- Top protocol ports

The following commands apply specifically to report templates for report type “others”:

```
scope ip ipaddr [port port-num]

scope port port-num [ip ipaddr]

content others-class {overall | ip-port | ip | port}
range {destination | source} [conn-dir {inbound | outbound}]
[top-num num]
```

4.24 New EX 1100 Hardware Model

The EX 1100 offers 4 Ethernet copper ports, hardware bypass, and 1 dedicated management port. It provides a total throughput of 1 Gbps and offers 512 QoS classes.

4.25 L7 New and Enhanced Signatures

New L7 Classes

Class	**Category**
Kkbox	Multimedia
Sharetastic	P2P
Shareaza	P2P
Foxy	P2P
Vagaa	P2P
Gogobox	P2P
Clubbox	P2P
Myth	Games*
Need_4_speed	Games*
Msn_game	Games*
Operation_flashpoint	Games*
Outlaws	Games*
Quake	Games*
Swat3	Games*
Ultima	Games*

*Not enabled by default

Enhanced L7 Classes

Class	**Category**
DNS	Directory Service
NTP	Miscellaneous
YouTube	Multimedia
ISAKMP	Security
RDP (renamed to remote-desktop)	Session
Kazaa Lite	P2P
iMesh	P2P
Winny	P2P
Share (merged into shareaza and sharetastic)	P2P
Xunlei	P2P
Ares	P2P
eMule	P2P
BitTorrent	P2P
Skype	VoIP

5 Resolved Issues

The following table lists the issues that are fixed in this release, starting from the 3.0 General Availability release. Issues are listed by A10 Networks tracking ID. Lower ID numbers correspond to older issues.

TRACKING ID	**DESCRIPTION**
25755	Restart while processing MicroSoft MMS with NAT
34356	TCP efficiency total drop packets incorrect
38132	Missing route configuration after software restart
39892	UDP broadcast and GRE fragments dropped
40897	IPsec fragments dropped
41684	Support clear local session by filter condition but without support for function that clears local session
25755	System reload occurred while processing NAT, Application Layer Gateway (ALG) for Microsoft Media Server.
37440	IP-to-ID test button did not work when the password included the pound sign (#).
38132	Static routes were missing after process restarted.
39198	Failed to apply QoS class precedence via Web GUI.
39266	Configuration was incorrectly detected as having changed when health monitor process restarted.
39892	Generic Routing Encapsulation fragment was dropped.

TRACKING ID	DESCRIPTION
40324	Reload occurred while processing aFleX script.
40658	System reload occurred when deleting an interface from a VLAN while Foundry proprietary Layer 2 traffic was received on the VE.
40897	IPsec Encapsulating Security Payload (ESP) fragments were not being handled properly.

6 Known Issues

The following table lists knows issues in this release.

ISSUE	DESCRIPTION
40092	DHCP process is not included in the overall health status of the EX device. This could affect HA operations.

7 Known Limitations

The following table lists knows issues in this release.

ISSUE	DESCRIPTION
1	Spanning Tree Protocol is not supported.
2	Some encrypted P2P protocols may not be detected.
3	HA may flap when a process is restarted.
4	Traffic from new application software releases may not be properly classified.
5	No packet statistics are collected for locally sent or received traffic.
6	Inbound LLB statistics are not collected on a link group but are collected on the link on which it arrives.
7	HA will switch over if the time zone is changed.
8	HA configuration sync does not synchronize static ARP entries, external heath monitor scripts, or system time. Use NTP to synchronize the system time.
9	ARP learns IP address 0.0.0.0.
10	Fiber ports support auto-negotiation only. Peer devices need to use auto-negotiation; otherwise, fiber links may not come up.
11	Health monitor external scripts can not be exported.
12	NAT ALG supports the following protocols only: H323, RAS, SIP, PPTP, FTP, DNS, NBT, ICMP, HWCC, ILS, and MSN.
13	IP bandwidth and connection limits are applied before QoS bandwidth and may affect the application of bandwidth on flowing packets.
14	An IP address with an IP Pool is considered by the EX device to be a local IP address, and thus can not be a gateway address of a link.
15	Link statistics do not count traffic that is not destined to the link gateway. For example, local interface traffic sent on the same port destined to machines on the same network is not counted.

ISSUE	DESCRIPTION
16	Health monitor packets can be affected by the DNAT feature if the source IP of the initiating health check packet matches the EX appliance's local DNAT IP that is configured for packet forwarding. This issue can be resolved by enabling the reply-same-interface feature using the following command: `ip route reply-same-interface <force|prefer>`
17	Configuration of NAT will not invalidate existing sessions. If NAT processing is not working as expected, use the **clear flow sessions** command to flush existing sessions.
18	Time of HA failover in transparent mode depends on the MAC-to-port entry aging time of any intermediary third party switches connected to the EX device.
19	Link aggregation or trunk interface can not be used with LLB currently.
20	The **bypass** CLI command exists on EX 1000, 2100, 2200 platforms but does not work on these models.
21	TCP dump does not accept a Virtual Ethernet interface, but it can accept a dump from a VLAN ID.
22	Clear application log by wildcard string may take a long time if the stored application logs are very large.
23	FTP transfer will stop after HA failover with session synchronization.
24	Reports, dynamic logs, domain group, and IP-to-ID cache are not synchronized to HA standby.
25	Aggregated links also in a VLAN may create a loop in a special topology.

8 Related Documentation

EX Series products are shipped with a printed Installation and Setup Guide, as well as a Documentation CD. The Installation and Setup Guide provides sufficient information for you to install and initially configure your product. The CD contains additional product documentation (CLI manual, GUI manual, Warranty Information and License Agreement, and Release Notes), which you can access and print out.

9 System Information

9.1 Hardware

System Component	EX 1000	EX 1100	EX2110	EX 2100/2200	
CPU	Single	Single Quad Core	Single Quad Core	Dual	
Memory	1 GB	1 GB	2 GB	2 GB	
Hard Disk	160 GB	250 GB	250 GB	Two 160 GB (RAID 1)	
Compact Flash	128 MB	1 GB	1 GB	1 GB	
Power Supply	Single	Single	Single	Dual (Hot swappable)	
Max Power Consumption	123 W	123 W	158 W	265 W	
Fan	Single	Single	Single	Dual (Field replaceable)	
Rack Units	1U	1U	1U	2U	
Weight	17 lbs	17 lbs	16 lbs	34 lbs	
Serial Port	RS-232	RS-232	RS-232	RS-232	
Power Off Eth Bypass	No	Yes	Yes	Yes	
Power On Eth Bypass	No	Yes	Yes	No	
Ethernet				2100	2200
Gigabit Copper	4	4	6	8	12
Gigabit Fiber (SFP)	0	0	2	2	0
Dedicated Mgmt port	0	1	1	0	0

9.2 Resource Limits

Resource Limits (maximum values)	EX 1000/1100	EX 2100/2110/2200
LLB Links	128	128
LLB Group	64	64
LLB Domain	64	64
SLB, FWLB, CLB nodes	256	256
SLB, FWLB, CLB groups	128	128
SLB Real Ports	512	512
SLB Virtual Server	128	128
SLB Virtual Ports	512	512
IP Lists	256	256
IP Address in IP List	No Limit	No Limit
IP Pools	64	64
IP Range within IP Pool	32	32
IPS Groups	30	30
IPS Hold IPs	128 subnets	128 subnets
QoS Rules	1024	1024

Resource Limits (maximum values)	EX 1000/1100	EX 2100/2110/2200
QoS Classes	1,024 - 2,048*	2,048 - 5,120*
QoS Rules per Class	32	32
QoS Policies	4096	4096
QoS Policy Schedules	No Limit	No Limit
Application Log Filter	63	63
Application Log Filter Includes	128	128
Virtual Group Per Interface	32	32
Virtual IPs Per Virtual Group	8	8
Connections	500,000-1,000,000	1,000,000-2,000,000

* 2048 classes, 1M connections for EX1100-002 model
5120 classes, 2M connections for EX2110-004 model

9.3 Maximum Performance

Performance (maximums)	EX 1000	EX 1100	EX 2110	EX 2100/2200
Connections per second	15,000	40,000	80,000	40,000
Throughput	500 Mbps	1 Gbps	4 Gbps	2 Gbps

Connections per second based on HTTP GET test of 64 byte HTTP payload and maximum port utilization.
Throughput based on bidirectional HTTP GET test of 512 KB HTTP payload and maximum port utilization.

10 Contact and Support Information

10.1 A10Networks.com

You can access the most current documentation on the World Wide Web at this URL: *http://www.A10networks.com using your customer support login.*

10.2 Documentation Feedback

You can send your comments in e-mail to support@A10Networks.com or you can submit comments by using the response card (if present) or using the comment forms that are at the end of the configuration documents by writing to the following address:

Attn: Customer Document Feedback
A10 Networks
2309 Bering Drive
San Jose, CA 95131

We appreciate your comments.

10.3 Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid A10 Networks Regular and Technical Support service contracts, the A10 Networks Technical Assistance Center (ATAC) provides support services online and over the phone (refer to the support phone number below).

A10 Networks, Inc.
2309 Bering Drive
San Jose, CA 95131
(408) 325-8676 (Support)
(408) 325-8666 (Fax)

This document is for informational purposes only. A10 Networks MAKES NO WARRANTIES, EXPRESSED OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.