Exinda How To Guide:

Assuring Application Quality Based on Host

Exinda ExOS Version 6.4

exinda

Copyright

Document Built on August-15-13 at 10:43 AM

Using this guide

Before using this guide, become familiar with the Exinda documentation system.

- "Exinda documentation conventions" on page 2
- "Notes, Tips, Examples, and Cautions" on page 3

Exinda documentation conventions

The Exinda documentation uses the following conventions in the documentation.

Graphical interface conventions

The following is a summary of the conventions used for graphic interfaces such as those in the Exinda Web UI and the Central Management Technical Preview UI.

Convention	Definition
bold	Interface element such as buttons or menus. For example: Select the **Enable** checkbox.
Italics	Reference to other documents. For example: Refer to the *Exinda Application List*.
>	Separates navigation elements. For example: Select **File > Save**.

Command line conventions

The following is a summary of the syntax used for the CLI commands.

```
(config)# command <user input> keyword {list|of|options|to|select|from} [optional
parameter]
```

Convention	Definition
`monospace text`	Command line text or file names
`<courier italics>`	Arguments for which you use values appropriate to your environment.
courier bold	Commands and keywords that you enter exactly as shown.
`[x]`	Enclose an optional keyword or argument.
`{x}`	Enclose a required element, such as a keyword or argument.
`|`	Separates choices within an optional or required element.
`[x {y | z}]`	Braces and vertical lines (pipes) within square brackets indicate a required choice within an optional element.
`command with many parameters that wrap onto two lines in the documentation`	Underlined CLI commands may wrap on the page, but should be entered as a single line.

Notes, Tips, Examples, and Cautions

Throughout the manual the following text styles are used to highlight important points:

- **Notes** include useful features, important issues. They are identified by a light blue background.

  Note Note text

- **Tips** include hints and shortcuts. They are identified by a light blue box.

  Tip Tip text

- **Examples** are presented throughout the manual for deeper understanding of specific concepts. Examples are identified by a light gray background.

  Example

  Text

- **Cautions** and warnings that can cause damage to the device are included when necessary, and are highlighted in yellow.

  Caution Caution text

Table of Contents

Chapter 1: Specify application quality based on host

Per Host Quality of Service (QoS) allows you to manage traffic congestion by policing bandwidth available to each host in your network. You can allocate a minimum amount of bandwidth for critical applications, such as VoIP and Citrix, for every host in your network. You can also restrict the bandwidth that each host can utilize for recreational purposes. All out-of-path interfaces are included in the QoS calculations.

The Exinda appliance enables greater system throughput, up to 10GB, by using multiple queues to handle the traffic. The multiple queues are based on the licensed bandwidth, but the multiple queues are used when the licensed bandwidth exceeds 1.8GB per second.

Tip	Per Host QoS can be integrated with Active Directory so bandwidth management can be tailored to users or groups.

1. (Optional) Integrate the Exinda appliance with Active Directory. Refer to the Active Directory guide.
2. "Set a per-host limit on bandwidth usage" on page 5
3. "View the number of hosts on a Dynamic Virtual Circuit" on page 8

Set a per-host limit on bandwidth usage

Per Host QoS is applied at the Virtual Circuit level. It is disabled by default. A Virtual Circuit with Per Host QoS enabled is called a Dynamic Virtual Circuit (DVC).

1. Click **Optimizer**.
2. Click **Create New Virtual Circuit**.
3. Type a name for the virtual circuit.
4. Type the amount of bandwidth to be used by the virtual circuit.
5. To enable Per Host QoS, select the **Dynamic Virtual Circuit** checkbox.
6. Set the amount of bandwidth (in KB per second or percentage of the virtual circuit bandwidth) that each host will receive in the **Per Host Bandwidth** field.

   This bandwidth is guaranteed, so it will be available to each host, if required.

   To have the amount of bandwidth each host receives calculated by dividing the Virtual Circuit guaranteed bandwidth by the number of active hosts, select **Automatically Share**.
7. Set the maximum amount of bandwidth (in KB per second or percentage of the virtual circuit

bandwidth) that each host can burst to in the **Per Host Max Bandwidth** field.

If **No Bursting Allowed** is selected, each host only gets the bandwidth that they have been guaranteed.

8. Set the location of the hosts to allocate bandwidth to.

   Internal Hosts are those that are on the LAN side of the appliance. External Hosts are those that are on the WAN side of the appliance.

9. Set the maximum number of hosts that can use the Dynamic Virtual Circuit.

   If **Auto** is selected, the maximum number of hosts is calculated by assuming each host gets its guaranteed bandwidth.

   If **Automatically Share** is selected, the maximum number of hosts is calculated by assuming each host is entitled to minimum bandwidth, which is 10kbps.

   Any host that becomes active after the maximum number of hosts is exceeded do not fall into this Virtual Circuit.

Note

- There is a system limit of 325,00 hosts that can fall into each Dynamic Virtual Circuit. This may occur if the Virtual Circuit has more than 300 Mbps of bandwidth. When this limit is exceeded, hosts fall into the next applicable Virtual Circuit.
- When Per Host QoS is enabled, a further level of traffic shaping is introduced. Traffic is first shaped at the Host level, then at the Policy level. The bandwidth allocated will be the minimum of the two levels.

The following examples describe various Dynamic Virtual Circuit configurations.

Name: Example 1 **Bandwidth:** 1024kbps **Direction:** Both **Network Object:** Internal Users **Dynamic Virtual Circuits Enabled:** Yes **Per Host Bandwidth:** Auto **Per User Max Bandwidth:** 100% **Host Location:** Internal **Max Hosts:** Auto	Internal Users is a Network Object that defines all hosts on the LAN side of the Exinda appliance. If there is 1 user, they get the full 1024kbps. If there are 2 users, they each get 512kbps and can burst up to the full 1024kbps (if the other user is not using their guaranteed 512kbps). If there are 10 users, they each get 102kbps and can burst up to the full 1024kbps (if the other users are not using their guaranteed 102kbps).
Name: Example 2 **Bandwidth:** 1024kbps **Direction:** Both	Internal Users is a Network Object that defines all hosts on the LAN side of the Exinda appliance. If there is 1 user, they get 102kbps and cannot burst.

Network Object: Internal Users **Dynamic Virtual Circuits Enabled:** Yes **Per Host Bandwidth:** 10% **Per User Max Bandwidth:** No **Host Location:** Internal **Max Hosts:** Auto	If there are 10 users, they each get 102kbps and cannot burst. If there are 100 users, the first 10 users each get 102kbps and cannot burst. The remaining 90 users will not match this VC.
Name: Example 3 **Bandwidth:** 1024kbps **Direction:** Both **Network Object:** Internal Users **Dynamic Virtual Circuits Enabled:** Yes **Per Host Bandwidth:** 64kbps **Per User Max Bandwidth:** 50% **Host Location:** Internal **Max Hosts:** 16	Internal Users is a Network Object that defines all hosts on the LAN side of the Exinda appliance. If there is 1 user, they get 64kbps and can burst up to 512kbps. If there are 16 users, they each get 64kbps and can burst up to 512kbps (if the other users are not using their guaranteed 64kbps). If there are 30 users, the first 16 users each get 64kbps and can burst up to 512kbps (if the other users are not using their guaranteed 64kbps). The remaining 14 users will not match this VC.
Name: Example 4 **Bandwidth:** 1024kbps **Direction:** Both **Network Object:** Internal Users **Application:** Citrix **Dynamic Virtual Circuits Enabled:** Yes **Per Host Bandwidth:** 64kbps **Per User Max Bandwidth:** No **Host Location:** Internal **Max Hosts:** 16	Internal Users is a Network Object that defines all hosts on the LAN side of the Exinda appliance. "Citrix" is an Application that defines Citrix traffic. This VC will match all Internal User's Citrix traffic. If there is 1 user, they get 64kbps for their Citrix traffic and cannot burst. If there are 16 users, they each get 64kbps for their Citrix traffic and cannot burst. If there are 30 users, the first 16 users each get 64kbps for their Citrix traffic and cannot burst. The remaining 14 users will not match this VC.

Specify when multi-queue is activated

The Exinda appliance enables greater system throughput, up to 10GB, by using multiple queues to handle the traffic. Configure the appliance to switch from using a single-queue to using multiple queues when the specified bandwidth is reached.

1. Click **Tools > Console**.
2. Type the appliance username and password at the prompts.
3. To enter privileged EXEC (enable) mode, at the prompt type the following command:

   ```
   hostname > enable
   ```

   The `hostname #` prompt is displayed.
4. To enter configuration (config) mode, at the prompt type the following commands:

   ```
   hostname # configure terminal
   ```

   The `hostname (config)#` prompt is displayed.
5. Ensure the bridge and policy-based routing interfaces use `auto-license` mode. Auto-license is the default mode.

   ```
   (config)# bridge <bridge-name> mq mode auto-license
   (config)# pbr interface <interface-name> mq mode auto-license
   ```
6. Specify at what bandwidth usage the auto-license switches from single-queue to multi-queue.

   ```
   (config)# bridge <bridge-name> mq switch-bandwidth <bandwidth>
   (config)# pbr interface <interface-name> mq switch-bandwidth <bandwidth>
   ```

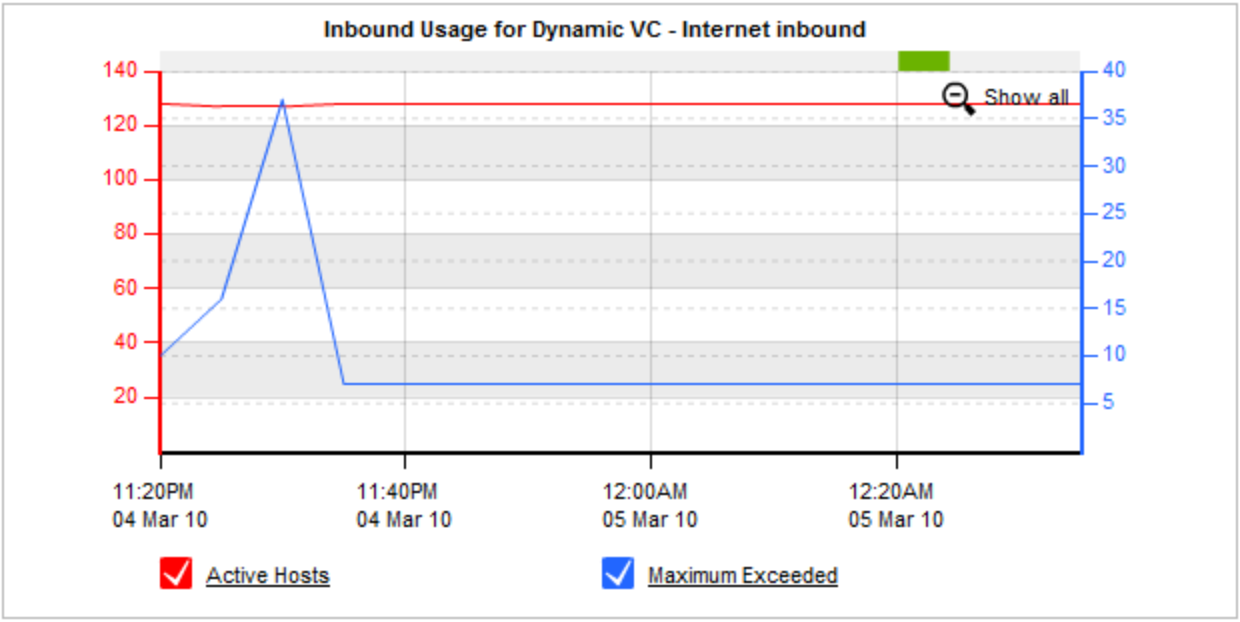
View the number of hosts on a Dynamic Virtual Circuit

The Optimizer Shaping Report shows how each Circuit, Virtual Circuit, Dynamic Virtual Circuit and Policy performs over time. You can see how well your Policies are performing and exactly how much bandwidth each Policy is served. The "Average Rate" is the average policy throughput for the time specified in the time range. The "Current Rate" is the policy throughput averaged over the last 20 seconds.

1. Click **Monitor > Control > Policies**.
2. Filter the charts by selecting the relevant **Circuit**, **Virtual Circuit**, and **Policy**.

   The charts are updated immediately to reflect these choices.

   When the Virtual Circuit selected is a Dynamic Virtual Circuit, the following graph is displayed above the throughput graph.



The number of **Active Hosts** for the selected Dynamic Virtual Circuit is represented by the red line.

The number of hosts that have exceeded maximum allowed hosts for this Dynamic Virtual Circuit is represented by the blue **Maximum Exceeded** line.

View the data throughput on the interfaces

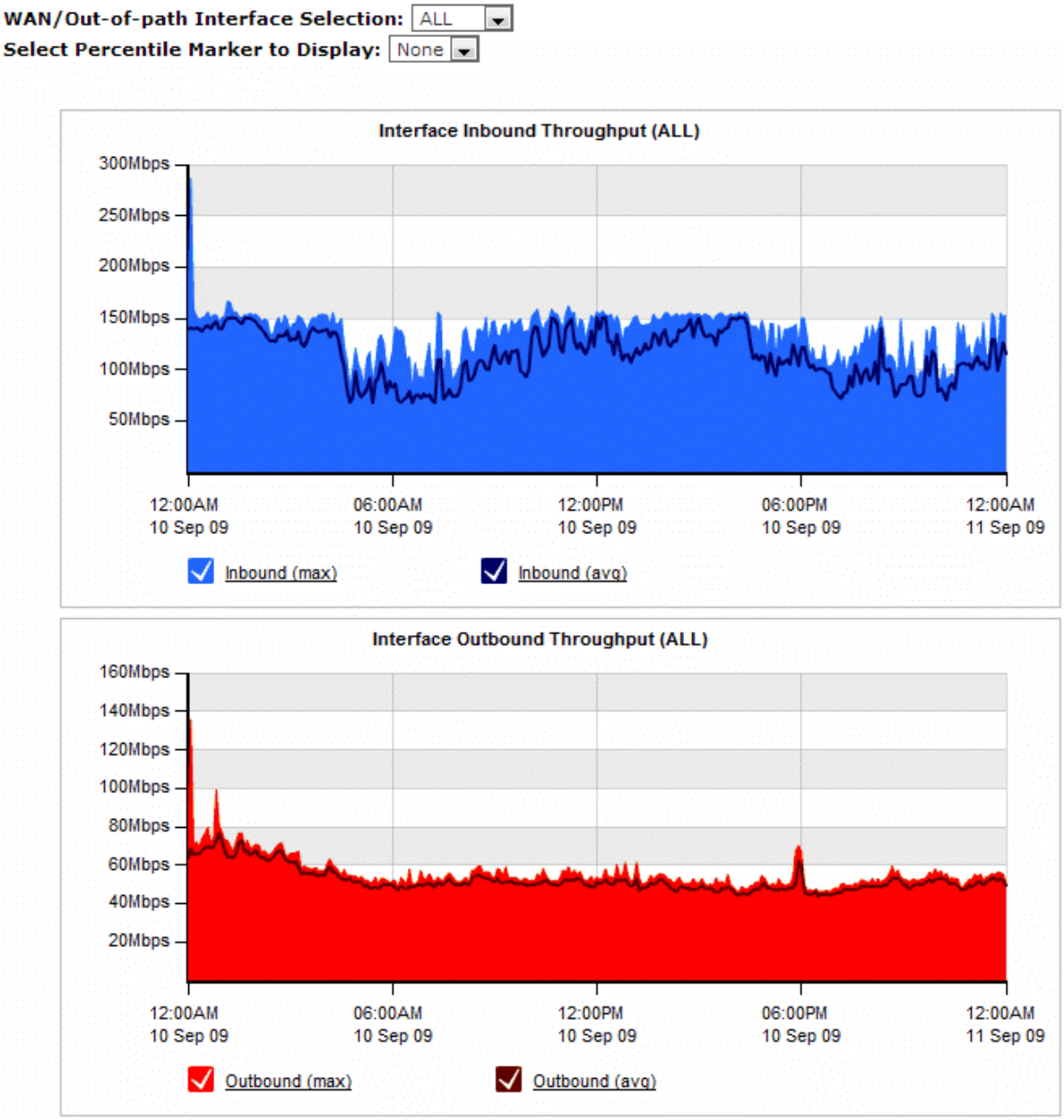
The Interface Throughput Report provides you with statistics of the total data that has passed through each WAN interface on each bridge. This report allows you to see the inbound and outbound throughput for all traffic on the wire, over time.

1. Click **Monitor > Interfaces > Throughput**.
2. To filer the data in the chart, select the WAN or out-of-path interface to display.

   Bridge WAN ports, policy-based routing interfaces, and WCCP interfaces are available. Selecting **All** includes all out-of-path interfaces in the report.
3. To identify how much traffic falls above a specific percentile, select the desired value from the **Select Percentile Marker to Display** list.

The table at the bottom of the report shows the total amount of data transferred into and out of the WAN interface(s), and also the maximum and average throughput values for the selected time period. The values in the table are automatically updated when the interactive flash graphs are manipulated.

Note	Given that this report shows all data on the wire, the report may also include traffic that is not seen on the WAN, such as local LAN broadcasts, etc.



WAN Interface Throughput Summary (ALL)			
Data Direction	**Total Data (MB)**	**Throughput Avg (Mbps)**	**Throughput Max (Mbps)**
Inbound	1200094.45	113.39	286.88
Outbound	553478.38	52.30	136.31

View the outbound packet rate for all traffic

The Interface PPS Report provides you with the packet rate that has passed through each bridge on the

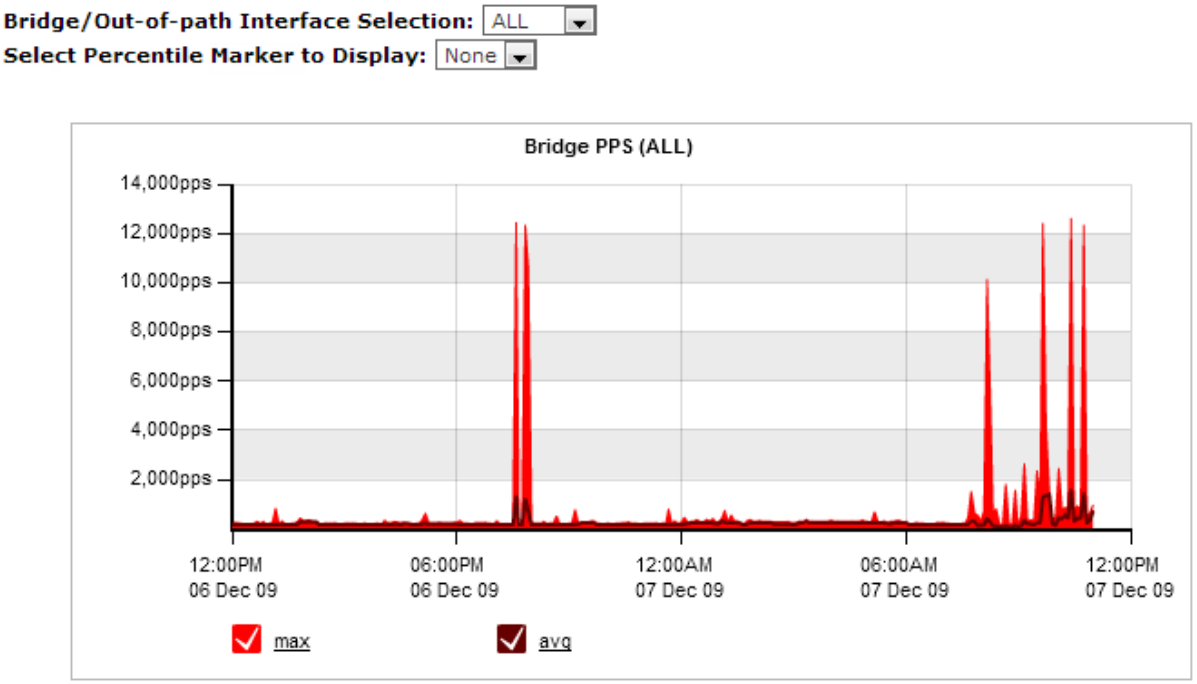
Exinda appliance. This report allows you to see the outbound packet rate for all traffic on the wire, over time.

1. Click **Monitor > Interfaces > Packets Per Second**.
2. To filer the data in the chart, select the Bridge or out-of-path interface to display.

   Bridge WAN ports, policy-based routing interfaces, and WCCP interfaces are available.Selecting **All** includes all out-of-path interfaces in the report.
3. To identify how much traffic falls above a specific percentile, select the desired value from the **Select Percentile Marker to Display** list.

The table at the bottom of the report shows the maximum and average PPS values through the bridge for the selected time period. The values in the table are automatically updated when the interactive flash graphs are manipulated.

> **Note** Given that this report shows all data on the wire, the report may also include traffic that is not seen on the WAN, such as local LAN broadcasts, etc.



Bridge PPS Summary (ALL)		
Data Direction	**Packets Per Second (Avg)**	**Packets Per Second (Max)**
Outbound	215	12,629

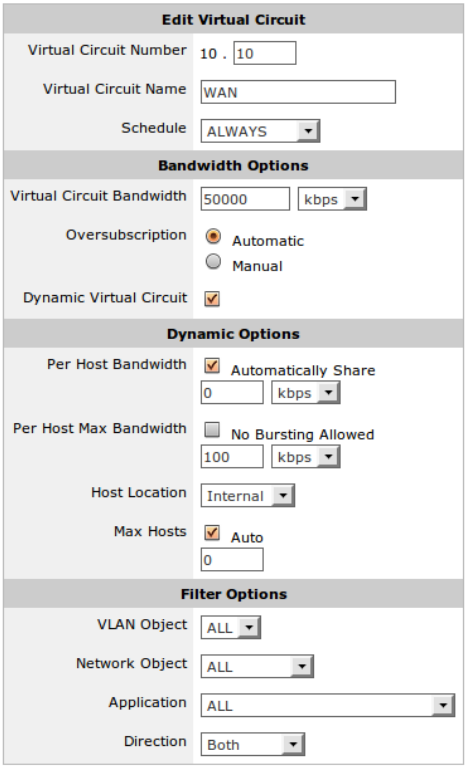
Chapter 2: Per Host QoS Usage Examples

The following examples show how Per Host QoS can be used in a variety of situations.

Limit Bandwidth Per Host

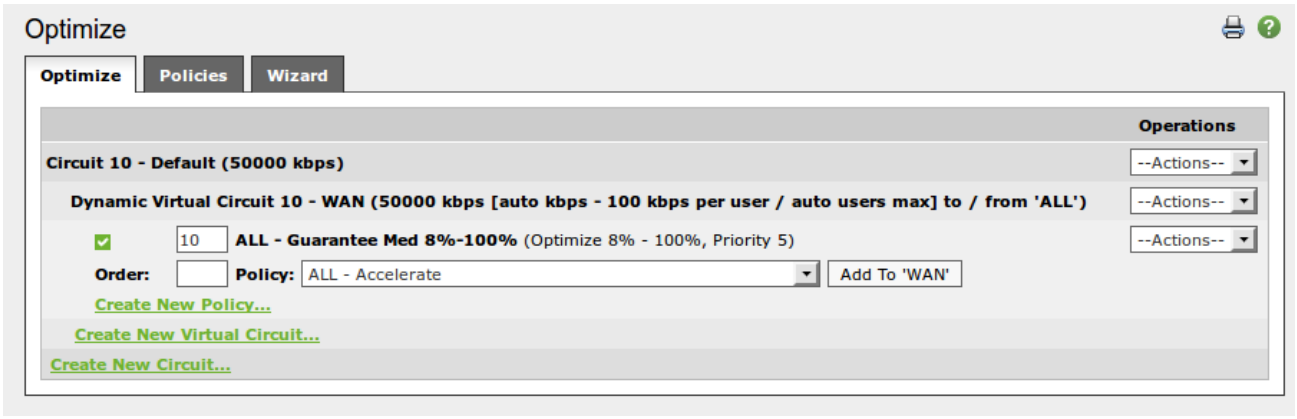
Example #1

Limit bandwidth to 100 kbps for each internal host.



In this Dynamic Virtual Circuit, each host is limited to a maximum bandwidth of 100 kbps.

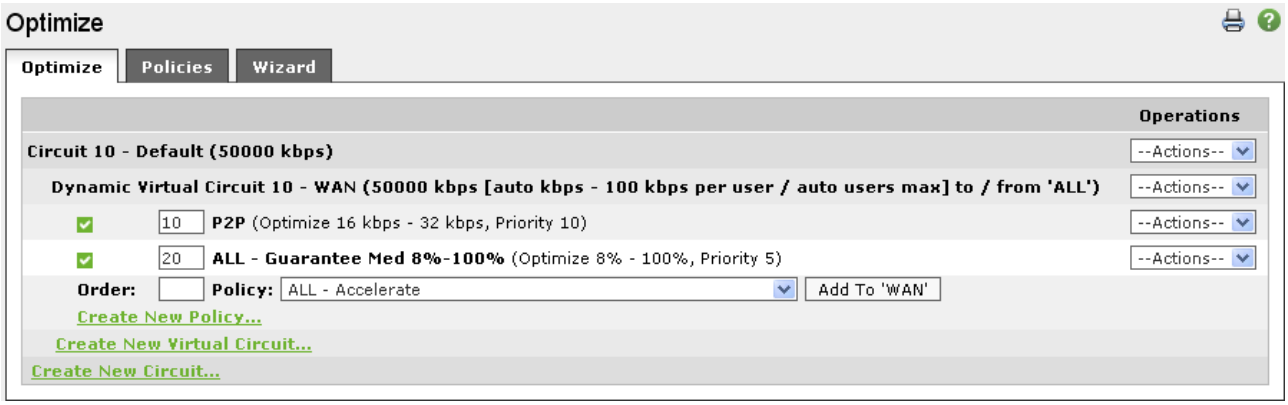
With Max Hosts set to "Auto", a maximum of 5000 hosts can fall into this Dynamic Virtual Circuit. This is calculated by assuming each host is entitled to a minimum bandwidth of 10 kbps as "Automatically Share" is selected.



Example #2

> Limit bandwidth to 100 kbps for each internal host. Further limit P2P traffic to a maximum of 32 kbps across ALL hosts.

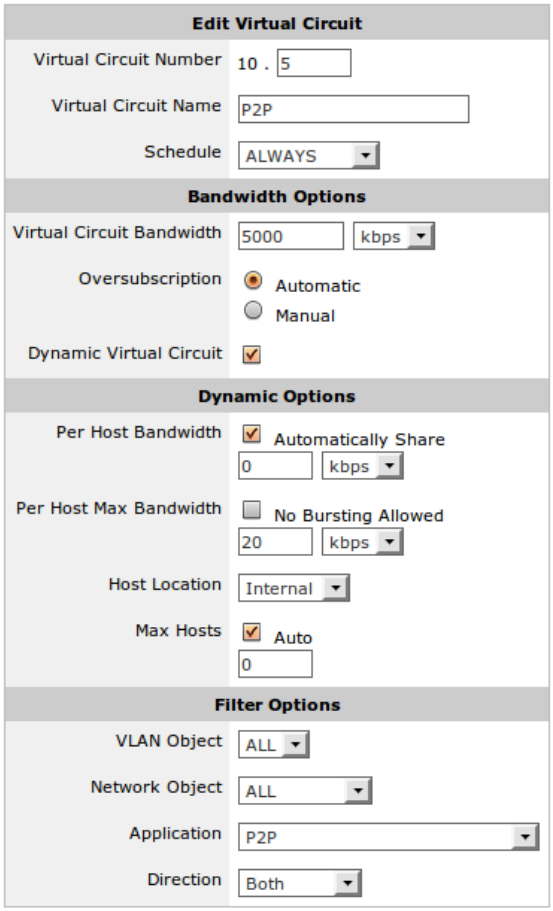
In this example, each host will receive between 10 and 100 kbps. In additional, P2P traffic summed across all hosts is capped at 32 kbps, with a guaranteed rate of 16 kbps. To further illustrate this example, suppose there are 100 active users, all using P2P applications on the WAN. The per host bandwidth is 100 kbps, but the P2P policy caps bandwidth at 32 kbps which will be fairly shared between each user. So we would expect to see P2P traffic per user at approx 320 bps.



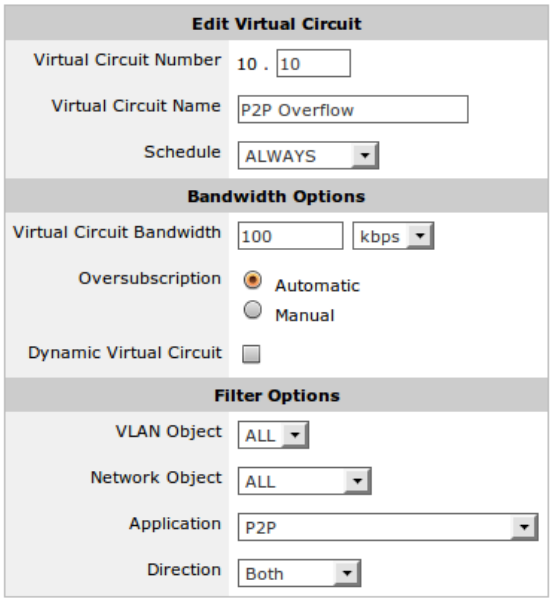
Limit Application Bandwidth

Example

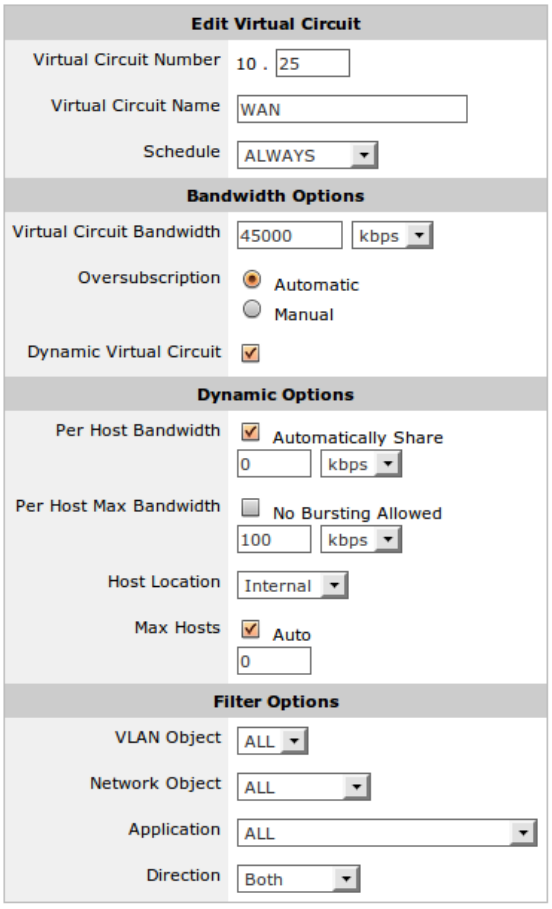
> Limit P2P to 20 kbps.



In the P2P Dynamic Virtual Circuit, each host is limited to 20 kbps of P2P traffic. With **Max Hosts** set to **Auto**, a maximum of 500 hosts can fall into this Dynamic Virtual Circuit. Additional hosts will share bandwidth allocated in the P2P Overflow Virtual Circuit.

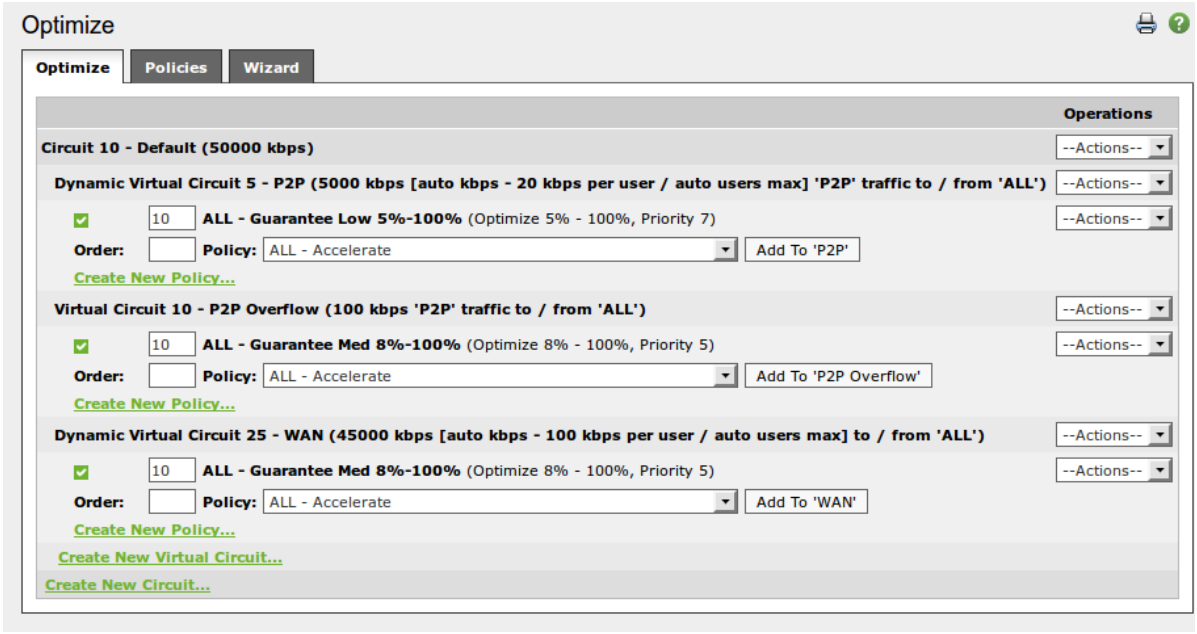


P2P Overflow Virtual Circuit



Dynamic Virtual Circuit To Share Remaining Bandwidth

Create a Dynamic Virtual Circuit using the remaining bandwidth. Each user is limited to a maximum bandwidth of 100 kbps for all other applications.

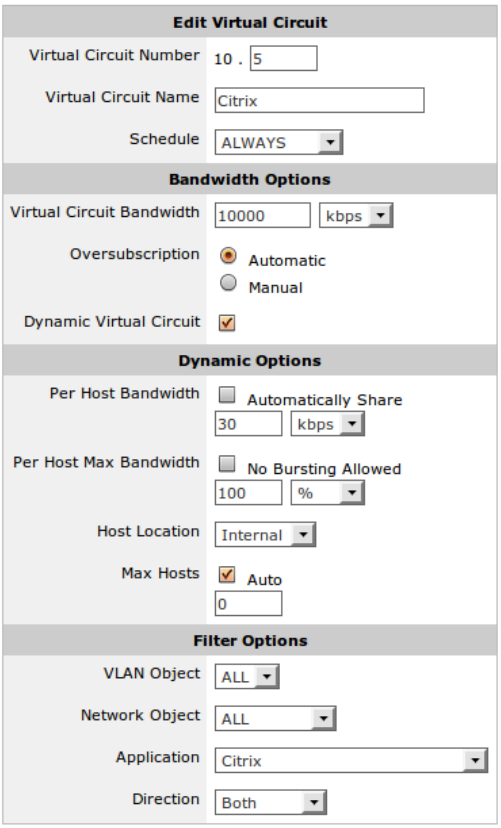


Guarantee Application Bandwidth

Example

> Guarantee 30 kbps per host, for the Citrix application.

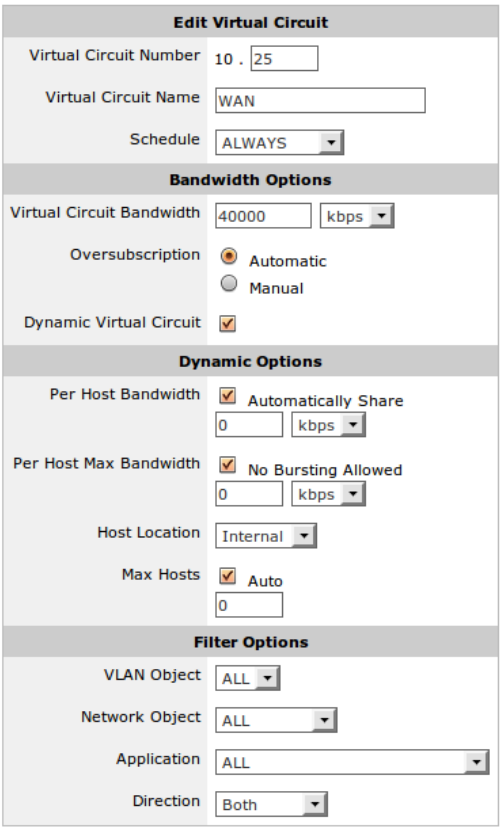
Citrix typically requires 20 to 30 kbps of bandwidth to work effectively.



Citrix Dynamic Virtual Circuit

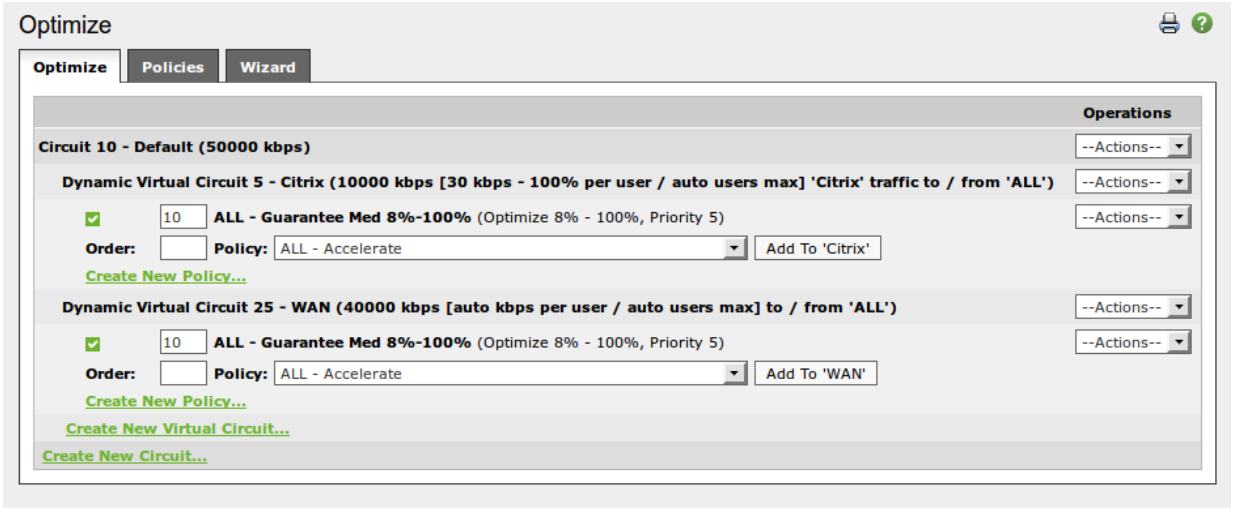
In this example, each user is guaranteed 30 kbps for Citrix. Furthermore, each user can burst up to 100% of the Dynamic Virtual Circuit bandwidth.

With **Max Hosts** set to **Auto**, a maximum of 333 hosts can fall into this Dynamic Virtual Circuit. Additional hosts will share bandwidth allocated in the second Dynamic Virtual Circuit.



Dynamic Virtual Circuit For Remaining Bandwidth

The **WAN** Dynamic Virtual Circuit has **Per Host Bandwidth** set to **Automatically Share**. Each user will be allocated a percentage of the Dynamic Virtual Circuit bandwidth. This is calculated by dividing the Dynamic Virtual Circuit bandwidth by the number of active hosts.

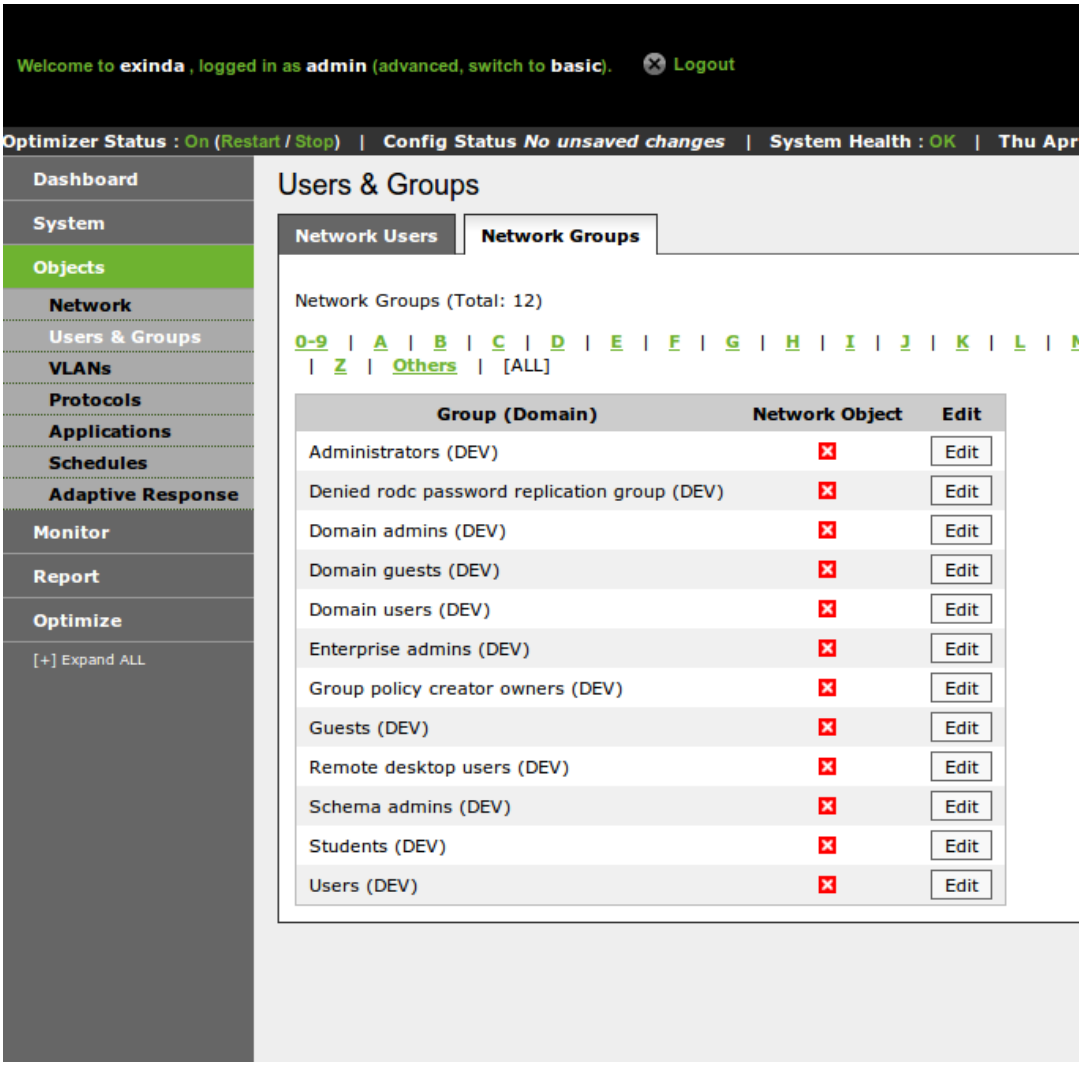


Per Host QoS with Active Directory

Example

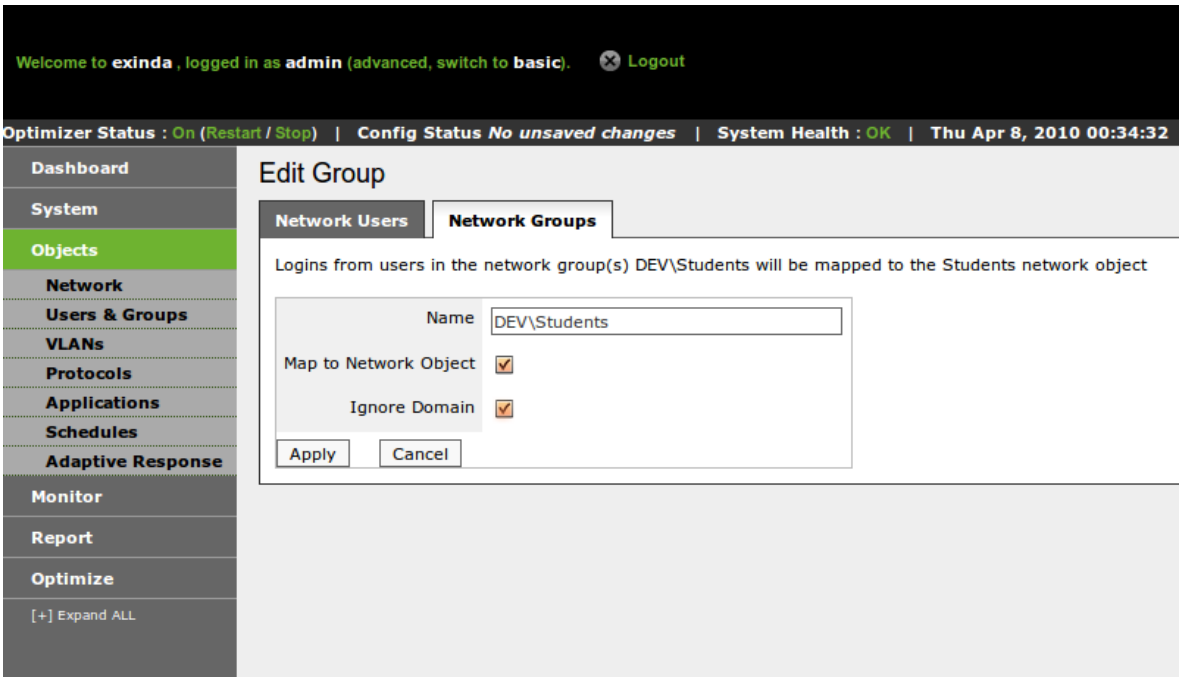
Restrict users in the Active Directory 'Students' group to 100 kbps.

Using the Web UI - Advanced Mode, navigate to Objects | Users & Groups. Edit the "Students (DEV)" group.



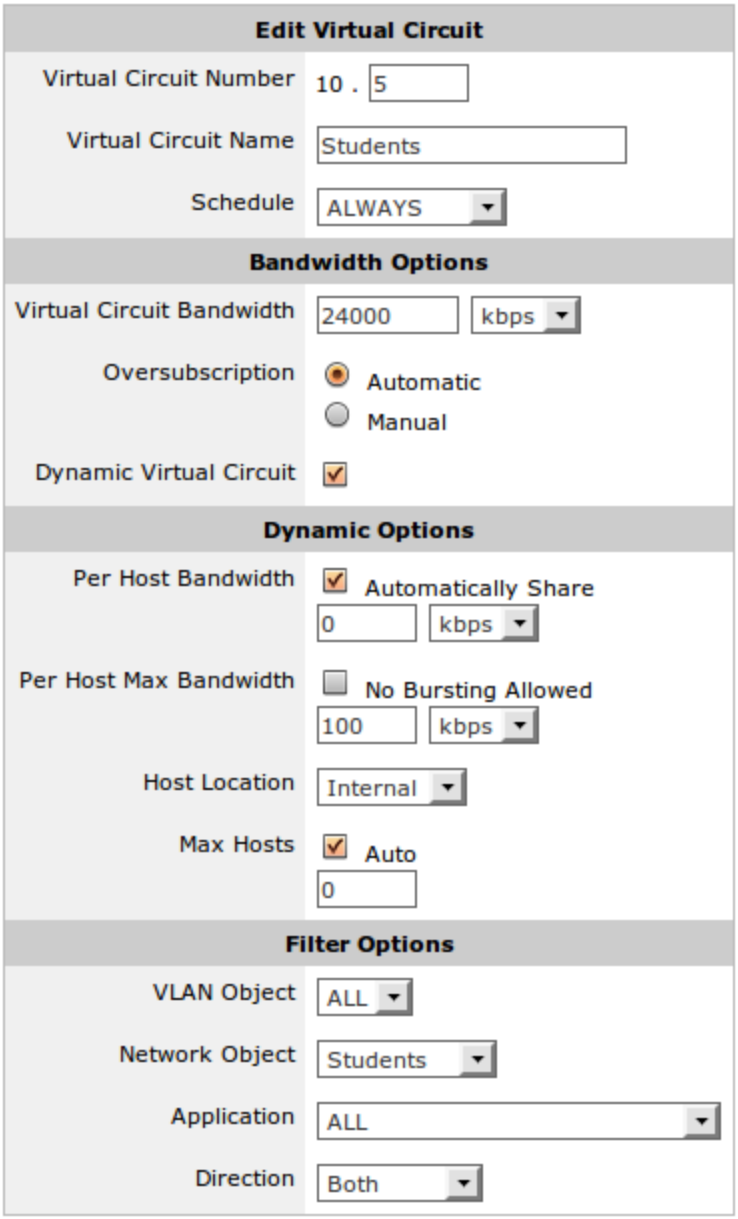
Active Directory Groups

Create a Network Object from the Active Directory group.



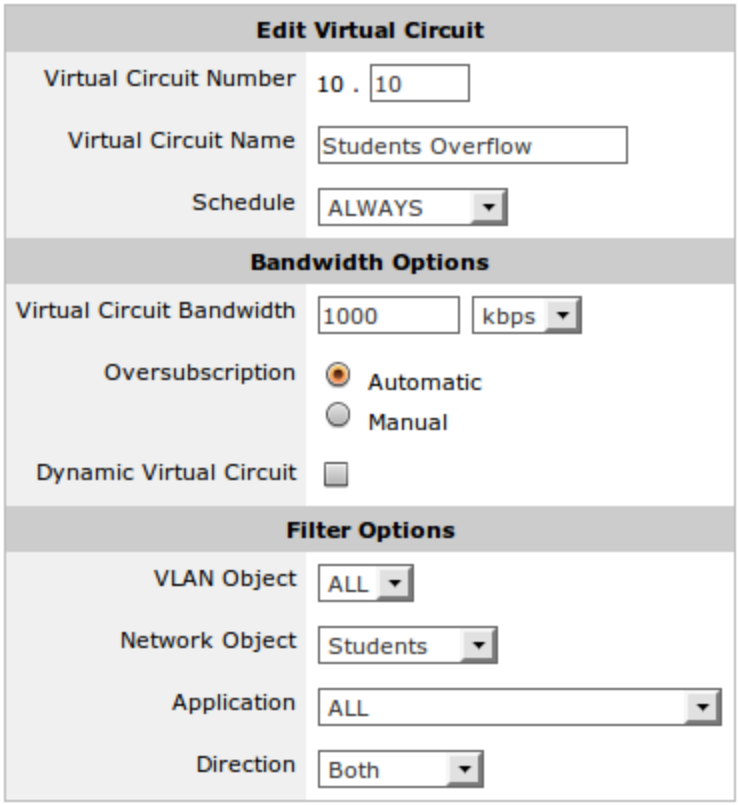
Map AD Group 'Students' To Network Object 'Students'

The Network Object "Students" can now be used in a Dynamic Virtual Circuit.

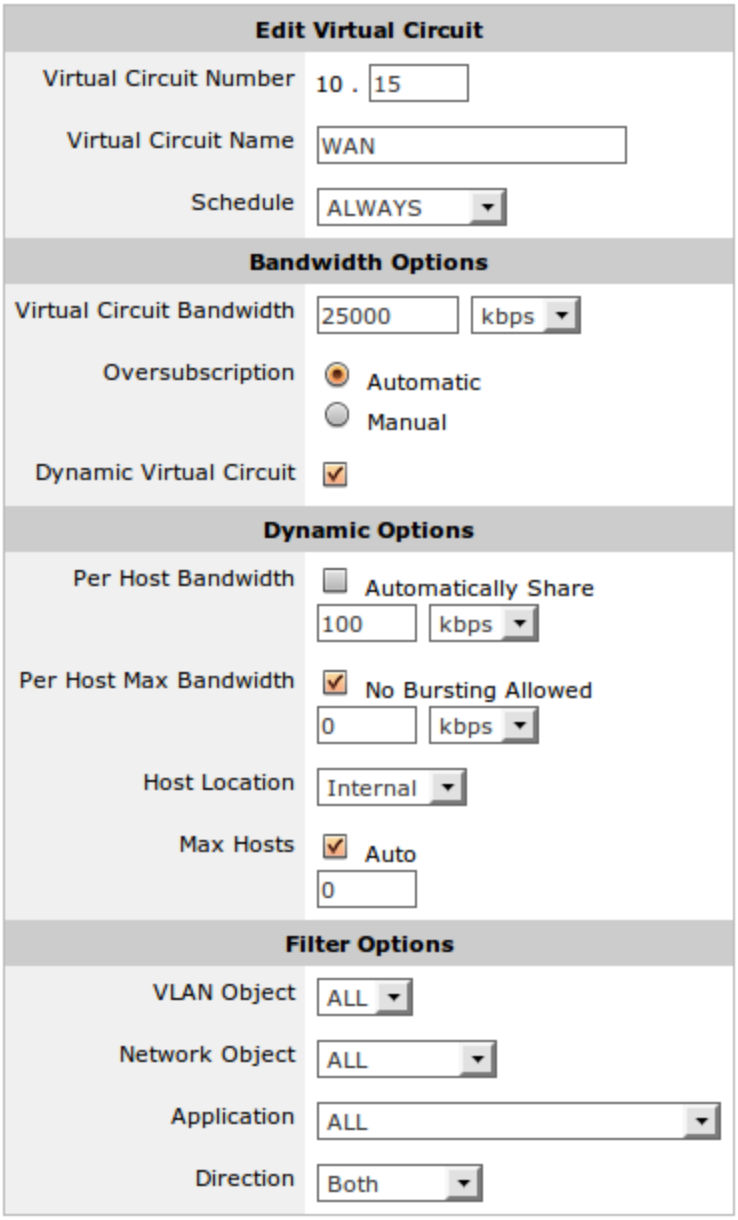


Students Dynamic Virtual Circuit

Each host in the "Students" Network Object is limited to 100 kbps. With Max Hosts set to "Auto", a maximum of 2400 hosts can fall into this Dynamic Virtual Circuit. Additional hosts will share bandwidth allocated in the "Students Overflow" Virtual Circuit.

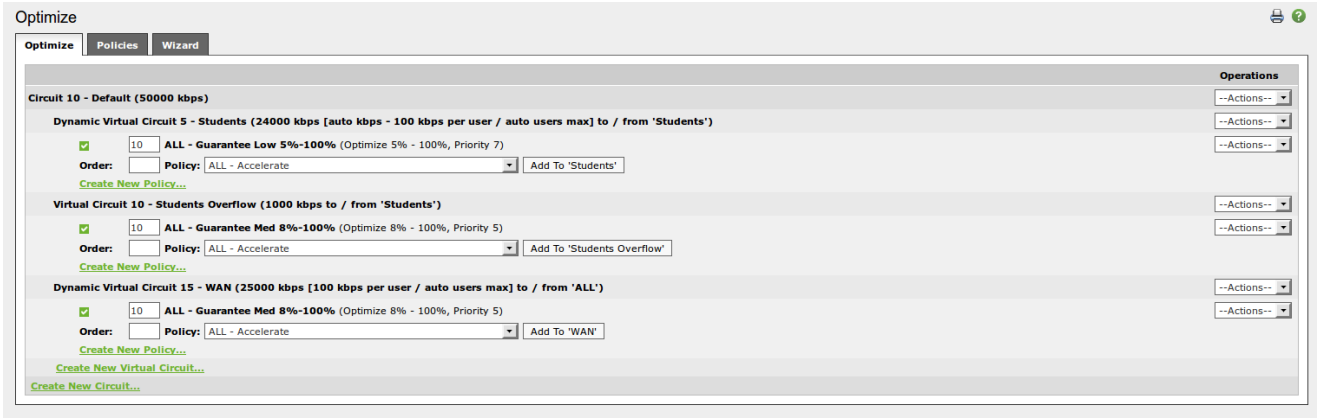


Students Overflow Virtual Circuit



Dynamic Virtual Circuit For Remaining Bandwidth

Another Dynamic Virtual Circuit can be created to share the remaining bandwidth for other hosts. In this example, each host is guaranteed 100 kbps with **No Bursting Allowed**.



Per Host QoS for Adaptive Response

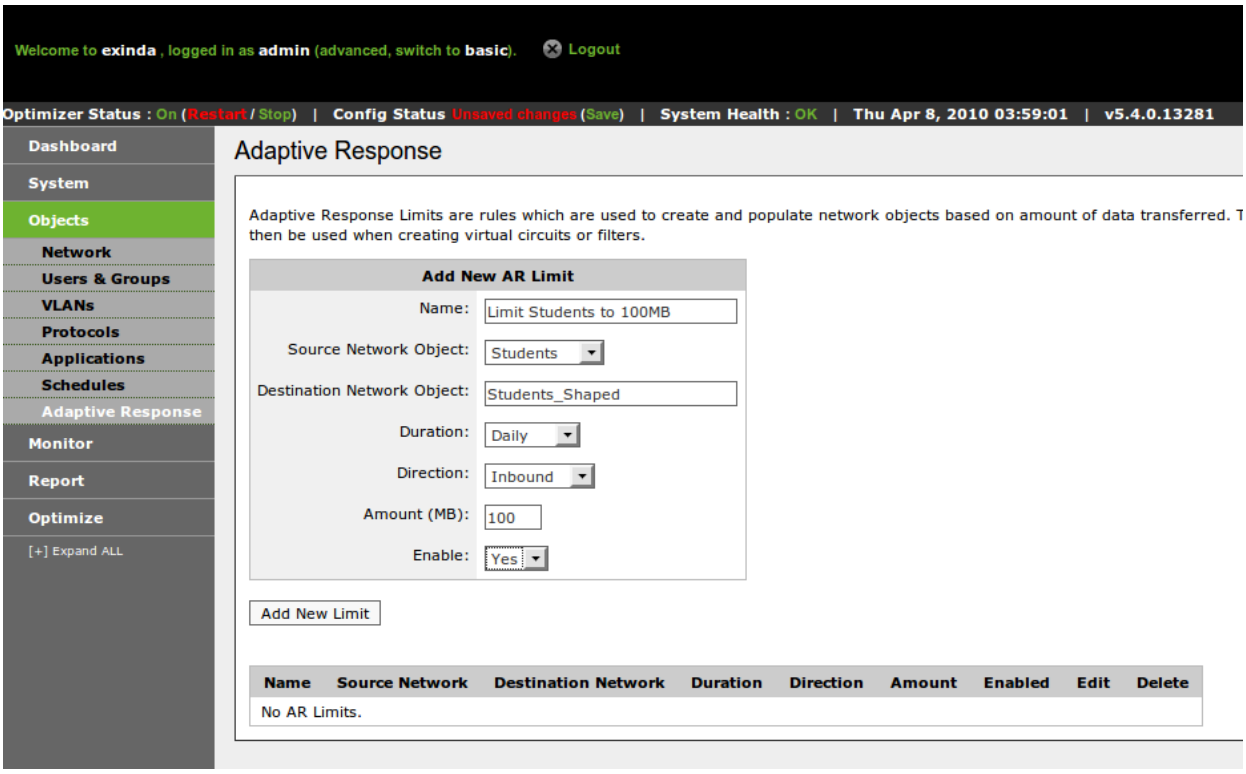
Example

> Restrict users in the Active Directory 'Students' group to 100 kbps, once the user has downloaded 100 MB per day.

Create the Network Object **Students** based on the Active Directory **Students** group as shown in the previous chapter.

Using the Web UI - Advanced Mode, navigate to **Objects > Adaptive Response**.

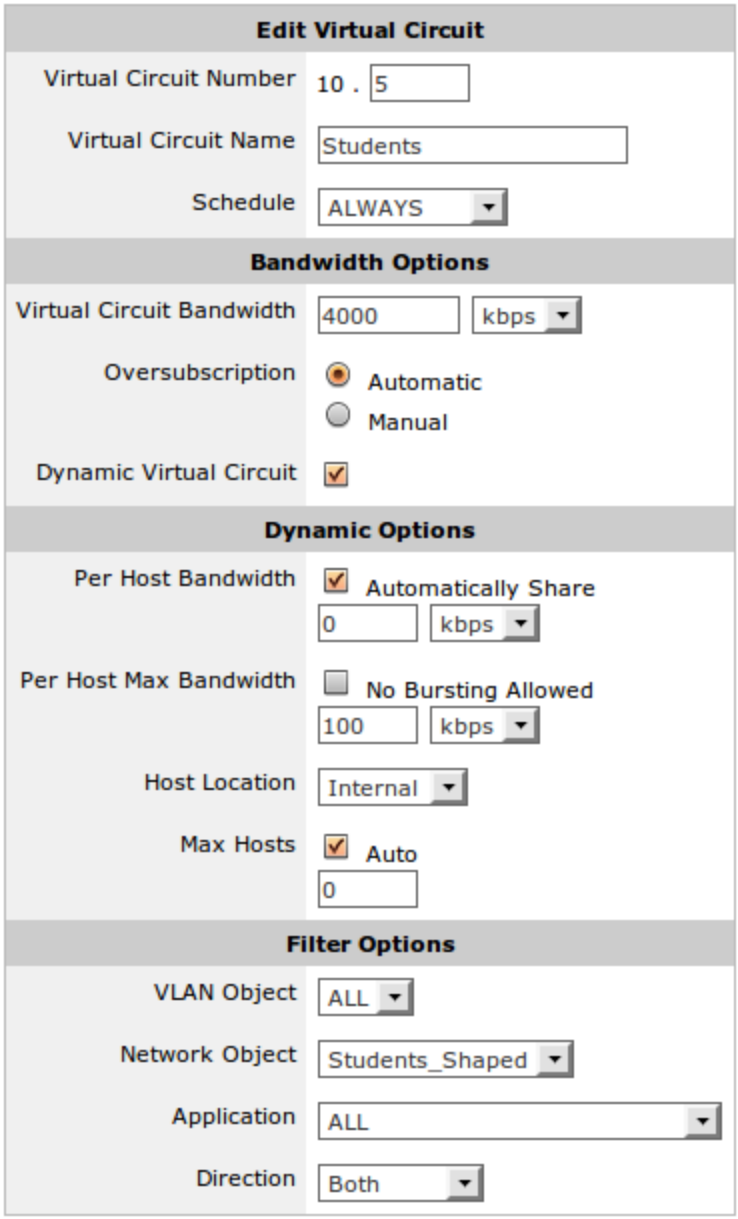
Create a new Adaptive Response rule based on the **Students** Network Object. Each host is allowed to download 100 MB per day before being placed into the **Students_Shaped** Network Object.



Create Adaptive Response Object

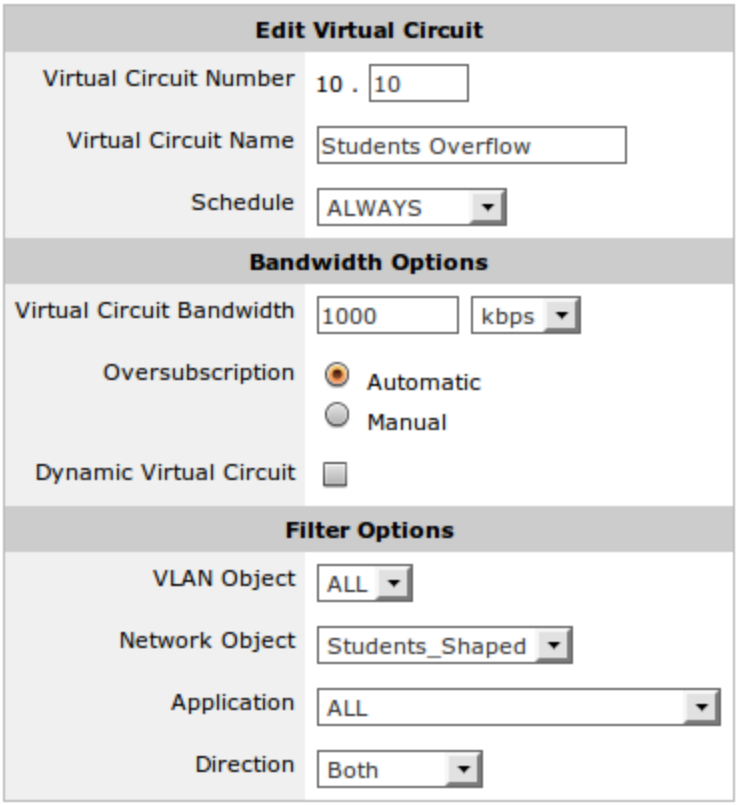
Create a Dynamic Virtual Circuit, with **Network Object** set to "**Students_Shaped**". Hosts matching this Network Object will fall into this Dynamic Virtual Circuit.

Each host is limited to a maximum bandwidth of 100 kbps. With **Per Host Bandwidth** set to **Automatically Share**, a maximum of 400 hosts can fall into this Dynamic Virtual Circuit.

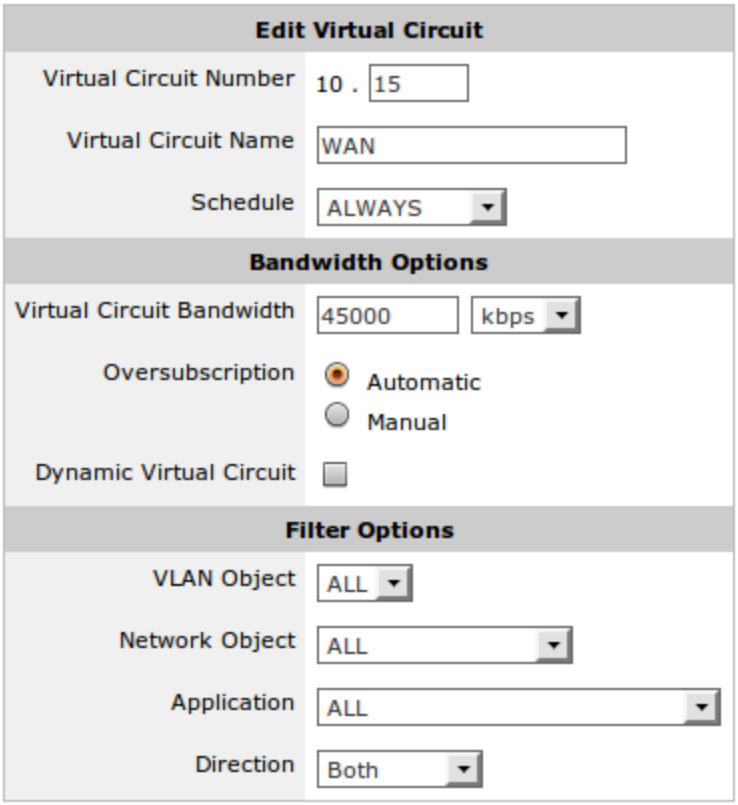


Students Dynamic Virtual Circuit

Additional hosts will share bandwidth allocated in the Students Overflow Virtual Circuit.



Students Overflow Virtual Circuit



Virtual Circuit To Share Remaining Bandwidth

Other users and students who have not used their 100MB daily quota will share 45 Mbps of bandwidth in the WAN Virtual Circuit.