61700544G1-29.2C
May 2014

Configuration Guide

Hardware ACLs in AOS

This guide provides an overview of hardware access control lists (ACLs) and their operation in ADTRAN Operating System (AOS) products. Included in this guide is a description of hardware ACLs, a description of how hardware ACLs and hardware access maps function in AOS products, and instructions regarding configuration of hardware ACLs and access control maps through both the web-based graphical user interface (GUI) and through the AOS command line interface (CLI).

This guide includes the following sections:

Hardware ACLs Overview

Hardware ACLs are access control lists that function by comparing all received frames to specific criteria at the hardware level. These hardware ACLs function in the same way as typical IP ACLs do at the software level. The difference is that hardware ACLs filter incoming traffic through the switch chip at wire speeds, rather than through the software packet filtering processes.

It is beneficial to understand the basic functioning of ACLs in AOS before working with hardware ACLs. All ACLs, whether hardware or software, by themselves do not perform any action. Rather, they are lists of criteria to which all incoming frames are compared. These lists provide the methods for many of the configurable filtering and security features of AOS to logically inspect each frame, compare it to the criteria in the ACL, and behave accordingly.

ACLs list criteria for incoming traffic that begin with either the keyword **permit** or **deny**. **Permit** indicates that incoming frames matching the specific criteria are selected and handled according to the configuration of the AOS feature using the ACL. **Deny** indicates that packets matching the specific criteria are not selected and are handled accordingly. Each ACL's criteria is compared to the frame in the order in which it was entered. This means that the order of criteria for permitting or denying frames is one to one with the order in which the criteria were entered into the ACL's configuration. As frames come into the unit, they are compared to the ACL criteria from top-to-bottom. If a frame does not match the criteria specified in the first entry, then it is compared to the criteria in the next entry. When the incoming frame is found to match an entry's specified criteria, then the frame is either categorized as **permit** or **deny** and the comparison of the ACL entries abruptly stops. At this point, the feature using the ACL takes the appropriate action.

There are many uses for ACLs, and many ways to configure ACLs. If you would like more information about ACL basic configuration and uses in AOS, refer to the configuration guide *Configuring IP Access Control Lists (ACLs) in AOS* available online at https://supportforums.adtran.com.

Hardware ACLs and Hardware Access Maps

Hardware ACLs can filter frames based either on IP information or on media access control (MAC) address information. IP hardware ACLs support filtering traffic on source and destination IP addresses, Transmission Control Protocol (TCP) and User Datagram Protocol (UDP), and TCP or UDP port numbers. MAC hardware ACLs filter traffic based on source and destination MAC addresses. All hardware ACLs filter only the incoming traffic, comparing the traffic to the list of criteria cited in the ACL.

As with all ACLs, the hardware ACL by itself performs no action. In order for the hardware ACL to function, a hardware access map must be created and applied to a virtual local area network (VLAN) interface. Access maps are the feature that uses the ACL and performs the action on the incoming traffic. Each access map can either forward or discard incoming frames acting on a single IP hardware ACL, a single MAC hardware ACL, or both. When both an IP and MAC hardware ACL are used by the access map, the two ACLs can be linked by **and** logic. **And** logic indicates to the access map that *both* ACLs must conclude that the frame be forwarded for the access map to forward it. As with all other ACLs, the information entered into the hardware ACLs is order dependent. The order in which criteria is listed in the ACL configuration is the order in which the frames will be compared to the criteria.

Once the access map has been created and associated with a hardware ACL, it must be applied to a VLAN for the ACL to be fully functional. Access maps can be applied to a single VLAN or a range of VLANs, however, only one access map can be applied to a VLAN at a time.

Hardware and Software Requirements and Limitations

The hardware ACL feature is available on AOS products as outlined in the *AOS Product Feature Matrix* available online at https://supportforums.adtran.com.

Hardware ACL Requirements and Limitations

Each IP hardware ACL supports filtering on TCP/UDP, a network of source and destination IP addresses, and TCP/UDP port numbers or ranges of TCP/UDP port numbers. MAC hardware ACLs support filtering on groups of source and destination MAC addresses.

Hardware ACLs support the tabulation of matches on each rule defined in the ACL, but they do not support filtering on host names or associations with tracks. There is no Simple Network Management Protocol (SNMP) support for hardware ACLs.

Each hardware ACL has an implicit **deny any** as the last criteria if there are other explicit criteria entries within the ACL. Each hardware ACL has an implicit **permit any** when there are no other explicit criteria entries within the ACL.

NOTE *Although hardware ACLs function very similarly to regular standard or extended ACLs, it is important to remember that they are not interchangeable in your unit's configuration.*

Access Map Requirements and Limitations

Each hardware ACL access map can act with the action of **forward** only. This action can be performed based on the criteria outlined in a single IP hardware ACL, a single MAC hardware ACL, or both.

If you configure the access map to reference an ACL other than a hardware ACL (such as the standard or extended IP ACLs or MAC ACLs), an error is displayed.

If you configure the map to reference a nonexistent IP or MAC hardware ACL, the ACL will be created. Note that this newly created ACL will have an implicit **permit any** as the default entry because no other entries are present.

Hardware ACL access maps can only be applied to VLANs, and only one access map can be applied to a VLAN at one time. If you attempt to apply a second access map to a VLAN, an error is displayed.

Hardware Resource Limitations

Because hardware ACLs are tied directly to your hardware, hardware resources can play an important part in their functioning. Each time that criteria in an existing hardware ACL changes, if that ACL is applied to a VLAN through an access map, the hardware will be reinitialized with the new criteria for the VLAN. If an access map is already applied to a list of VLANs, and it is applied to another VLAN, the hardware is reinitialized with the new list of VLANs to which the access map is applied. If the hardware ACL to which an access map refers is changed, the hardware is reinitialized with the new ACLs. It is possible to run out of hardware resources depending on how many resources are needed to apply the desired change. If there are not enough hardware resources to install the new criteria in the hardware, an error message is displayed. For more information on how to free up hardware resources, refer to *Optimizing Hardware Resources on page 26*.

In addition, when routing and route cache are enabled, the number of resources reserved for hardware ACLs drops by 25 percent. The number of hardware ACLs that can be configured can be increased by disabling routing (when possible).

Configuring Hardware ACLs and Hardware Access Maps Using the GUI

There are two basic steps to configuring hardware ACLs on your AOS product.

1. Configure either an IP hardware ACL, a MAC hardware ACL, or both.
2. Configure a hardware access map and apply it to a VLAN.

The following sections guide you through configuring hardware ACLs and access maps via the GUI.

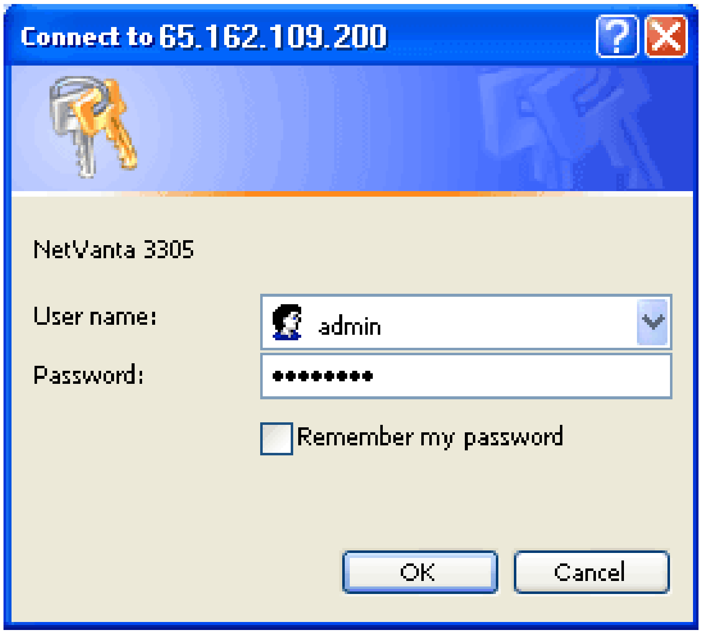
Configuring Hardware ACLs

To configure hardware ACLs via the GUI, follow these steps:

1. Open a new web page in your Internet browser.
2. Type your AOS product’s IP address in the Internet browser’s address field in the following form: **http:**//<*ip address*>, for example:

   http://65.162.109.200

3. At the prompt, enter your user name and password and select **OK**.



Connect to 65.162.109.200

NetVanta 3305

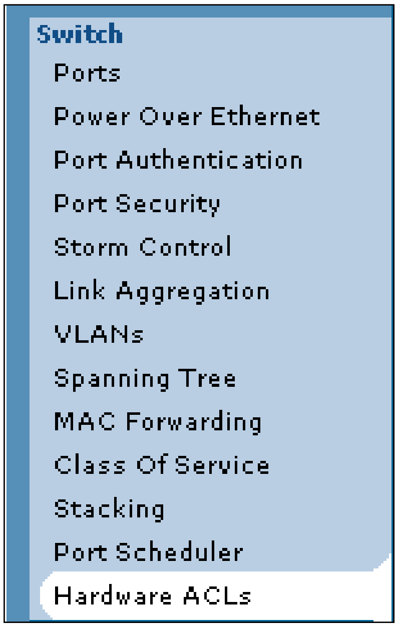
User name: admin

Password: ••••••••

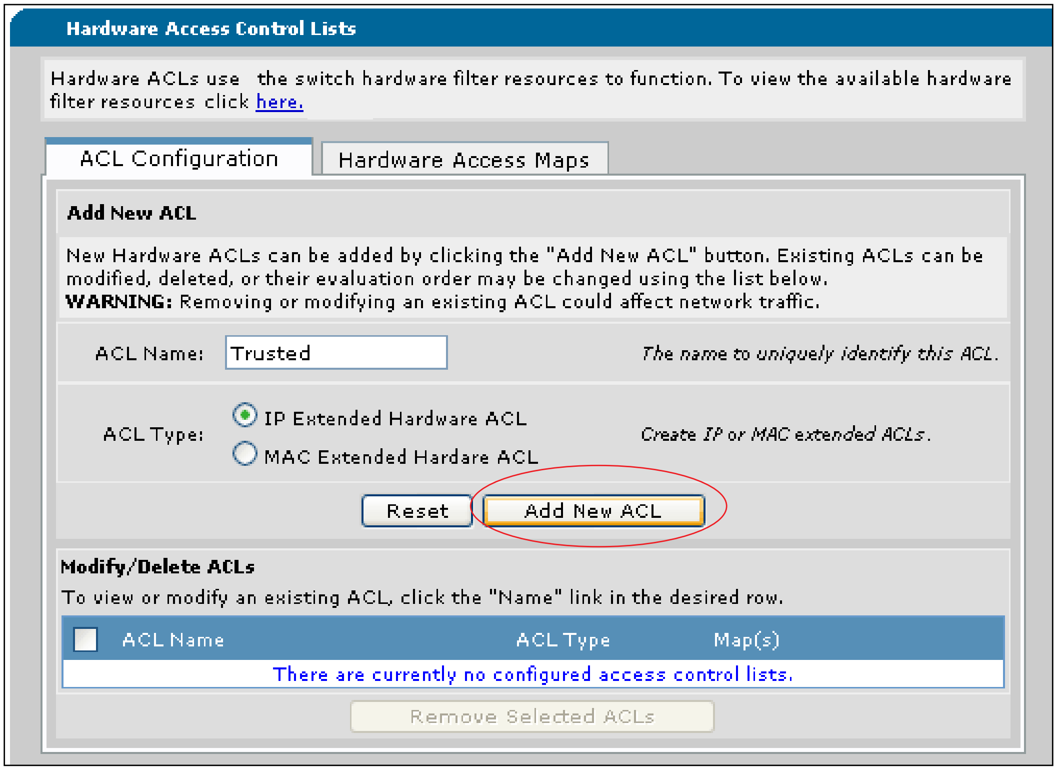
□ Remember my password

NOTE *The default user name is **admin** and the default password is **password**.*

4. Navigate to **Data** > **Switch** > **Hardware ACLs**.



5. Enter the ACL's name in the appropriate field, and select whether this ACL will be an **IP Extended Hardware ACL** or a **MAC Extended Hardware ACL**. Once you have defined the ACL type, select **Add New ACL**.



Hardware Access Control Lists

Hardware ACLs use the switch hardware filter resources to function. To view the available hardware filter resources click here.

Add New ACL

New Hardware ACLs can be added by clicking the "Add New ACL" button. Existing ACLs can be modified, deleted, or their evaluation order may be changed using the list below.
WARNING: Removing or modifying an existing ACL could affect network traffic.

ACL Name: Trusted — *The name to uniquely identify this ACL.*

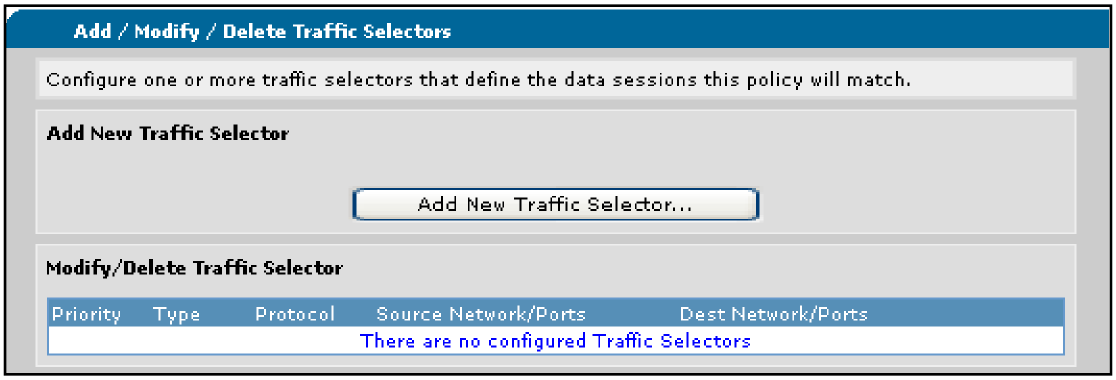
ACL Type: ● IP Extended Hardware ACL ○ MAC Extended Hardare ACL — *Create IP or MAC extended ACLs.*

Modify/Delete ACLs

To view or modify an existing ACL, click the "Name" link in the desired row.

□	ACL Name	ACL Type	Map(s)
	There are currently no configured access control lists.		

6. You will be automatically directed to a new screen where you will select the criteria for the ACL. Select **Add New Traffic Selector**.



Add / Modify / Delete Traffic Selectors

Configure one or more traffic selectors that define the data sessions this policy will match.

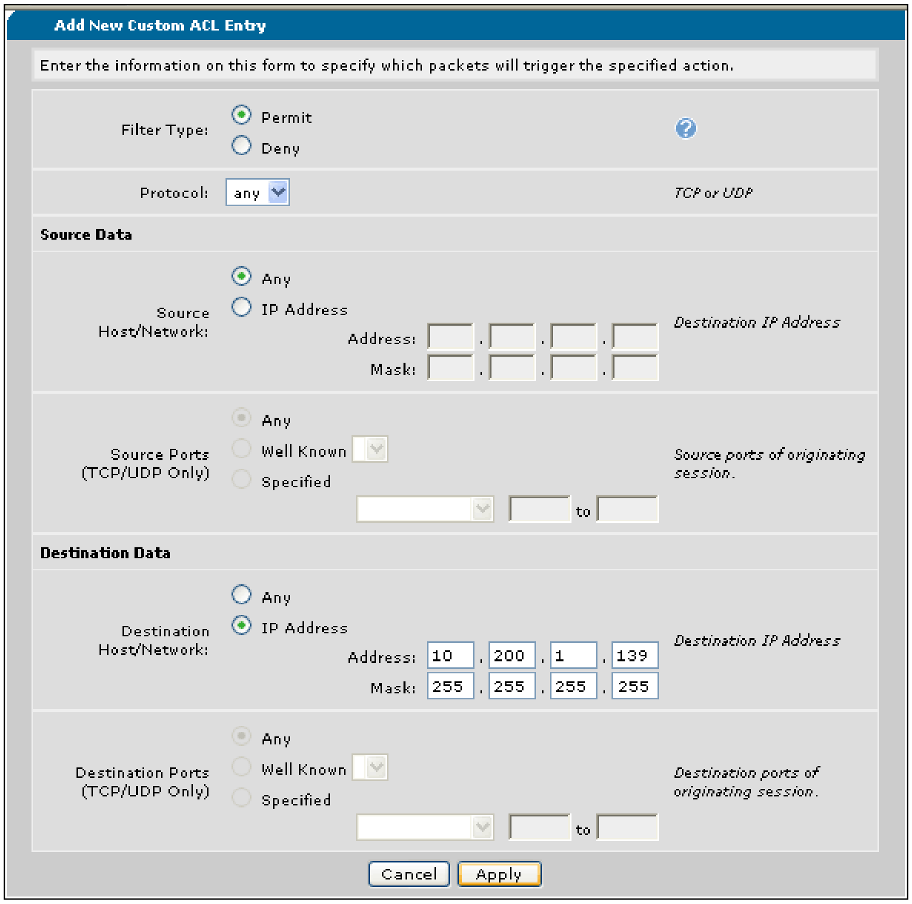
Add New Traffic Selector

Modify/Delete Traffic Selector

Priority	Type	Protocol	Source Network/Ports	Dest Network/Ports
There are no configured Traffic Selectors				

7. At this step, you will enter the specific criteria for this ACL. You will need to decide whether frames that match this criteria will be permitted or denied, keeping in mind that using **Deny** indicates that this policy will not be applied to frames that match this criteria. Because this is an IP ACL, you can select

whether this ACL will match packets on a particular protocol (TCP or UDP), or whether it will match any protocol. Select your protocol from the **Protocol** drop-down menu.



Add New Custom ACL Entry

Enter the information on this form to specify which packets will trigger the specified action.

Filter Type: ● Permit ○ Deny

Protocol: any — *TCP or UDP*

Source Data

Source Host/Network: ● Any ○ IP Address
Address: _ . _ . _ . _
Mask: _ . _ . _ . _
Destination IP Address

Source Ports (TCP/UDP Only): ● Any ○ Well Known ○ Specified
_ to _
Source ports of originating session.

Destination Data

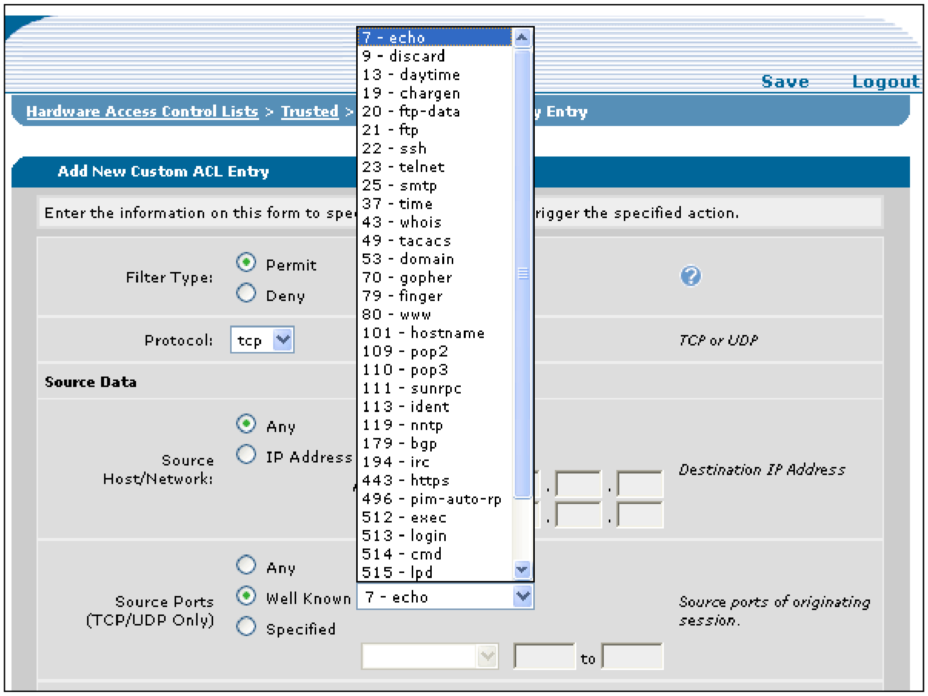
Destination Host/Network: ○ Any ● IP Address
Address: 10 . 200 . 1 . 139
Mask: 255 . 255 . 255 . 255
Destination IP Address

Destination Ports (TCP/UDP Only): ● Any ○ Well Known ○ Specified
_ to _
Destination ports of originating session.

8. You then define how traffic will be matched based on frame source information by entering the parameters for the **Source Host/Network**. You can select from **Any** (indicating any traffic will be matched), or you can enter a specific IP address as your source criteria.

9. If you have specified to match traffic based on either TCP or UDP, you can select the way that source ports for this traffic will be compared. You can select **any**, or you can specify a well-known port or a

range of ports. If you want to specify a well-known port, select the desired port from the **Well Known** drop-down menu.



Add New Custom ACL Entry

Enter the information on this form to spe[…]rigger the specified action.

Filter Type: ● Permit ○ Deny

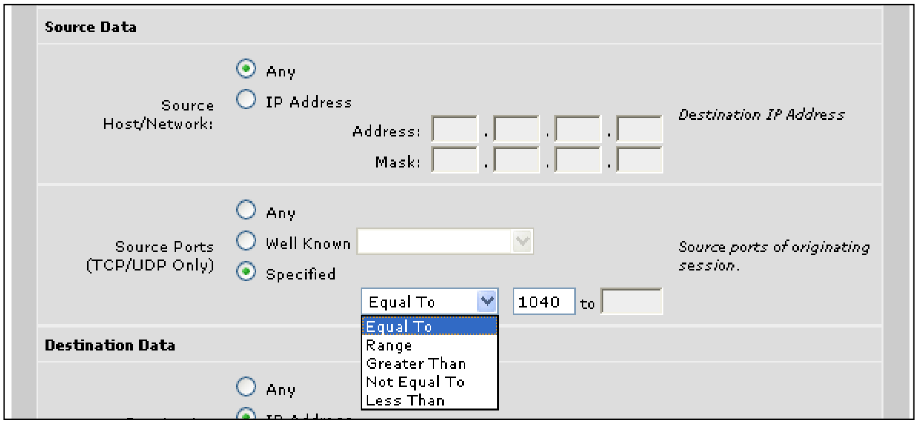
Protocol: tcp — TCP or UDP

Source Data

Source Host/Network: ● Any ○ IP Address — Destination IP Address

Source Ports (TCP/UDP Only): ○ Any ● Well Known 7 - echo ○ Specified — Source ports of originating session.

If you want to specify a range of ports, select the desired parameter from the **Specified** drop-down menu and enter the port number or range.



Source Data

Source Host/Network: ● Any ○ IP Address — Destination IP Address

Address: . . .

Mask: . . .

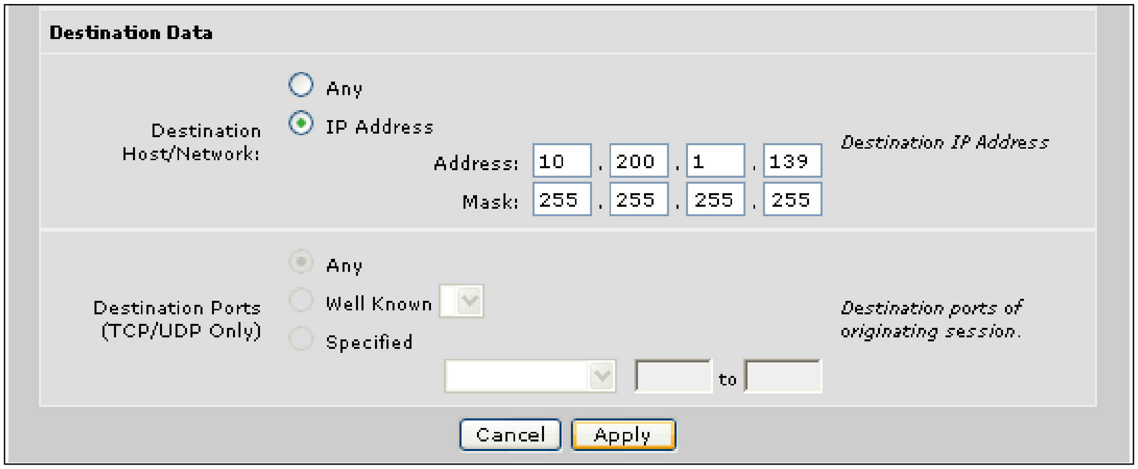
Source Ports (TCP/UDP Only): ○ Any ○ Well Known ● Specified — Source ports of originating session.

Equal To 1040 to

Destination Data

○ Any

10. Once you have specified the source information, you must do the same for the destination information. Enter the **Destination Host/Network** information by either selecting **Any** or entering an IP address and subnet mask. In this example, we are looking at all traffic destined to host **10.200.1.139**. If you have previously selected either TCP or UDP to be matched, enter the port information by selecting **Any**, **Well Known**, or **Specified**.

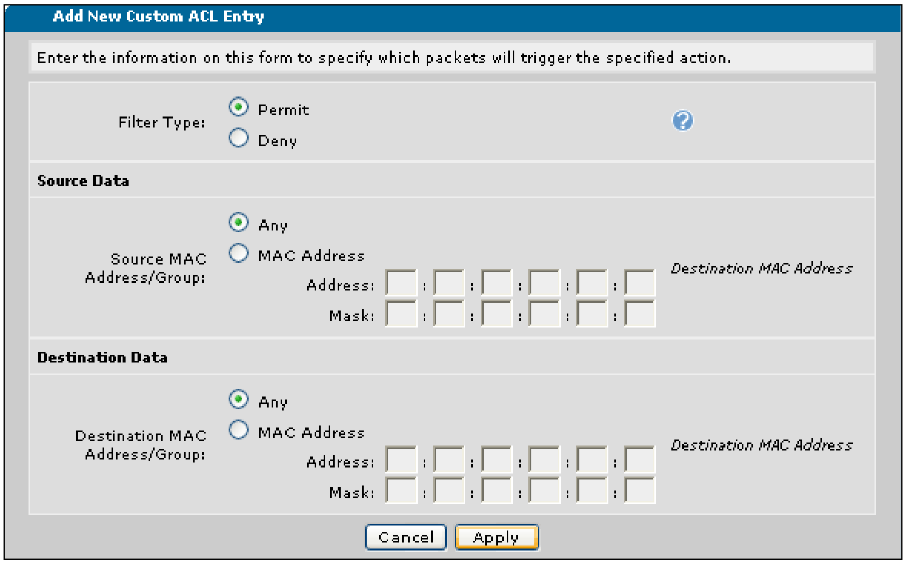


Destination Data

Destination Host/Network:
○ Any
● IP Address
Address: 10 . 200 . 1 . 139
Mask: 255 . 255 . 255 . 255
Destination IP Address

Destination Ports (TCP/UDP Only)
● Any
○ Well Known
○ Specified
to
Destination ports of originating session.

11. If you are working with a MAC hardware ACL, you must define traffic selectors based on source and destination MAC addresses.



Add New Custom ACL Entry

Enter the information on this form to specify which packets will trigger the specified action.

Filter Type:
● Permit
○ Deny

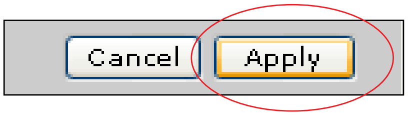
Source Data

Source MAC Address/Group:
● Any
○ MAC Address
Address: : : : : :
Mask: : : : : :
Destination MAC Address

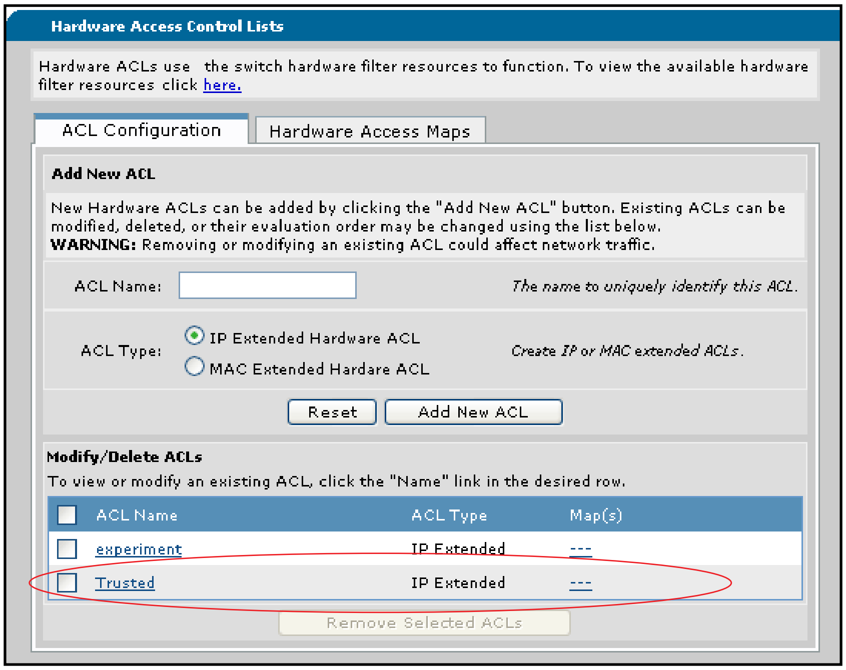
Destination Data

Destination MAC Address/Group:
● Any
○ MAC Address
Address: : : : : :
Mask: : : : : :
Destination MAC Address

12. Once you have entered the criteria for the ACL (**permit** or **deny**, source information, and destination information), select **Apply** to create the IP hardware ACL.



13. The newly created hardware ACL appears in the list of ACLs.



Hardware Access Control Lists

Hardware ACLs use the switch hardware filter resources to function. To view the available hardware filter resources click here.

Add New ACL

New Hardware ACLs can be added by clicking the "Add New ACL" button. Existing ACLs can be modified, deleted, or their evaluation order may be changed using the list below.
WARNING: Removing or modifying an existing ACL could affect network traffic.

ACL Name: *The name to uniquely identify this ACL.*

ACL Type: ● IP Extended Hardware ACL ○ MAC Extended Hardare ACL *Create IP or MAC extended ACLs.*

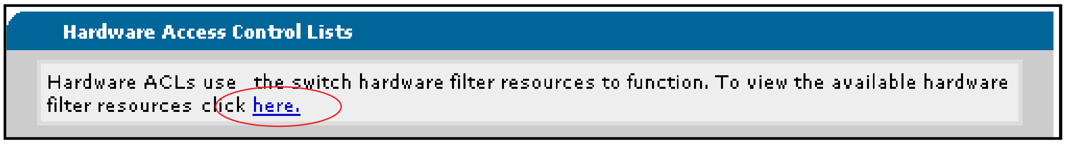
Modify/Delete ACLs

To view or modify an existing ACL, click the "Name" link in the desired row.

□	ACL Name	ACL Type	Map(s)
□	experiment	IP Extended	---
□	Trusted	IP Extended	---

Editing Hardware ACLs

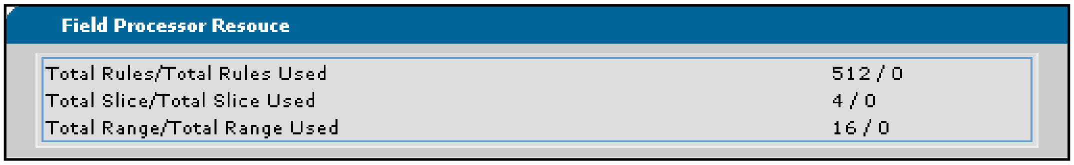
If you need to edit or delete an existing ACL, you can do so by selecting the ACL's name in the **Hardware Access Control Lists** menu. Before you change an ACL, you should check the availability of your hardware resources. To do so, select the hyperlink at the top of the **Hardware Access Control Lists** menu.



Hardware Access Control Lists

Hardware ACLs use the switch hardware filter resources to function. To view the available hardware filter resources click here.

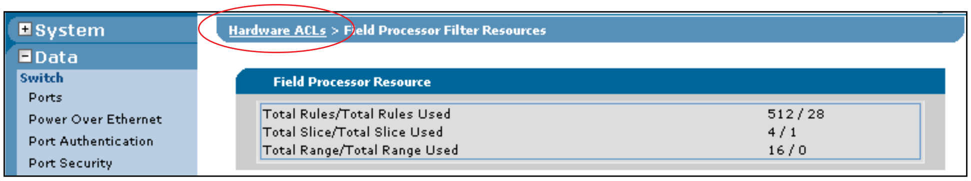
The available hardware resources and how many are being used is displayed. For more information about what these figures mean and how to use them, refer to *Hardware Resource Statistics on page 26*.



Field Processor Resouce

Total Rules/Total Rules Used	512 / 0
Total Slice/Total Slice Used	4 / 0
Total Range/Total Range Used	16 / 0

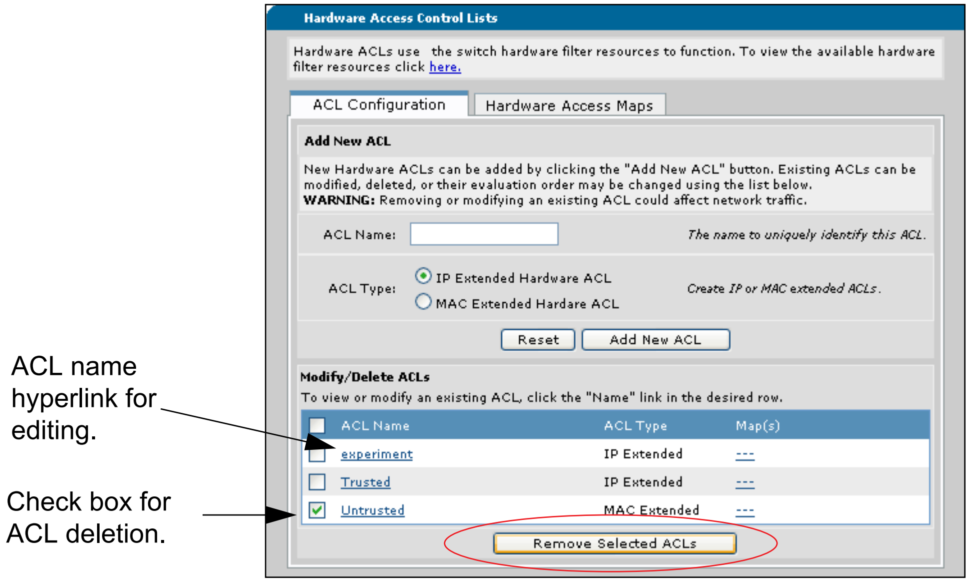
Once you have verified your hardware resources, select the **Hardware ACLs** hyperlink at the top of the menu to return to the main hardware ACL menu.



Field Processor Resource

Total Rules/Total Rules Used	512 / 28
Total Slice/Total Slice Used	4 / 1
Total Range/Total Range Used	16 / 0

Back at the main menu, you can delete or edit any of your currently configured ACLs by selecting the ACL from the list. If you want to edit the ACL, select the hyperlink of the ACL name. If you want to delete an ACL, check the box next to the appropriate ACL and select **Remove Selected ACLs**.



Hardware Access Control Lists

Hardware ACLs use the switch hardware filter resources to function. To view the available hardware filter resources click here.

Add New ACL

New Hardware ACLs can be added by clicking the "Add New ACL" button. Existing ACLs can be modified, deleted, or their evaluation order may be changed using the list below.
WARNING: Removing or modifying an existing ACL could affect network traffic.

ACL Name: *The name to uniquely identify this ACL.*

ACL Type: ● IP Extended Hardware ACL ○ MAC Extended Hardare ACL *Create IP or MAC extended ACLs.*

Modify/Delete ACLs

To view or modify an existing ACL, click the "Name" link in the desired row.

□	ACL Name	ACL Type	Map(s)
□	experiment	IP Extended	---
□	Trusted	IP Extended	---
☑	Untrusted	MAC Extended	---

ACL name hyperlink for editing.

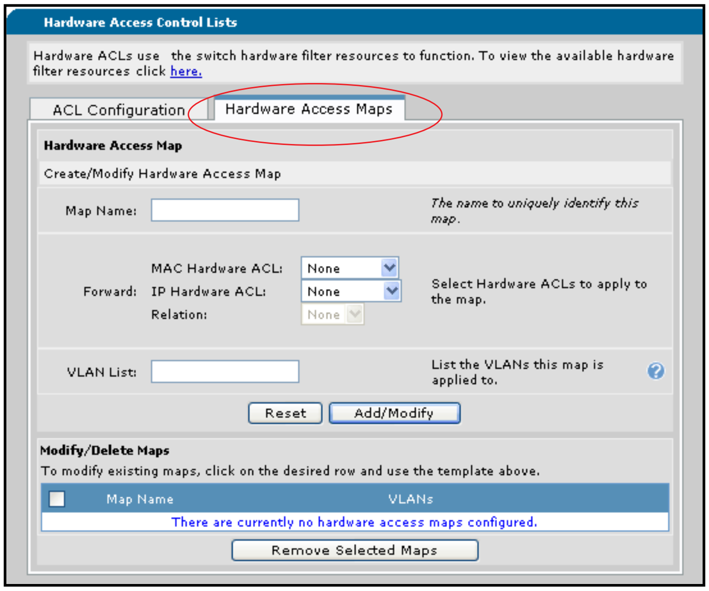
Check box for ACL deletion.

When you select an ACL to be edited, you will be routed back through the traffic selector definition process. Select **Add New Traffic Selector**, enter the desired parameters, and select **Apply**. The ACL has been edited and the criteria will be reinitialized where the ACL is in use.

When you select an ACL to be deleted, it will be removed from the list of configured ACLs.

Configuring Hardware Access Maps

To begin configuring hardware access maps, select the **Hardware Access Maps** tab from the main hardware ACL menu.



Hardware Access Control Lists

Hardware ACLs use the switch hardware filter resources to function. To view the available hardware filter resources click here.

Hardware Access Map

Create/Modify Hardware Access Map

Map Name: *The name to uniquely identify this map.*

Forward: MAC Hardware ACL: None
IP Hardware ACL: None
Relation: None

Select Hardware ACLs to apply to the map.

VLAN List: List the VLANs this map is applied to.

Modify/Delete Maps

To modify existing maps, click on the desired row and use the template above.

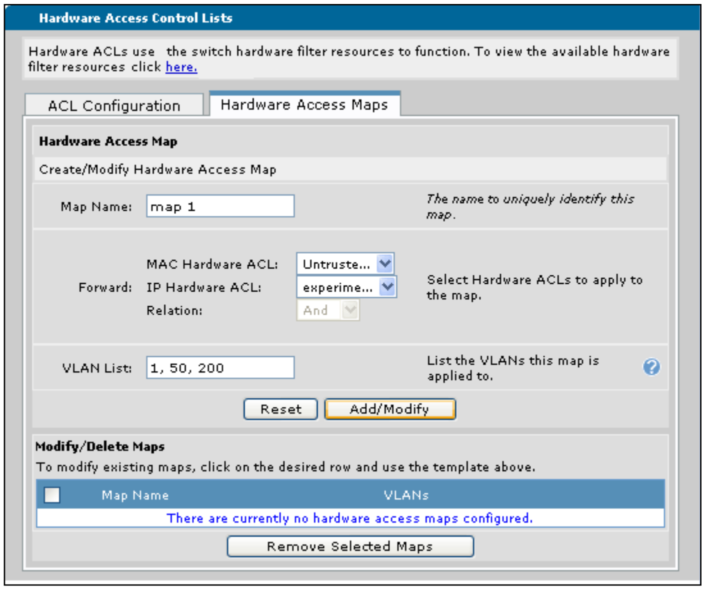
□	Map Name	VLANs
There are currently no hardware access maps configured.		

Next, you will enter the following information about the access map:

1. Enter the access map name in the **Map Name** field.
2. Select the hardware ACLs that will be used by this map. You can select either an IP hardware ACL or a MAC hardware ACL, or both. Select the name of the ACL you would like to use from the drop-down menus.

> NOTE
>
> *If you select both an IP hardware ACL and a MAC hardware ACL for this access map, the relationship between the two is based on* ***and*** *logic, indicating that the access map will forward frames that pass both ACLs.*

3. Specify the VLAN(s) that will use this access map. You can enter one VLAN by entering the VLAN ID in the field, or you can enter multiple VLANs by entering either a range of VLAN IDs or VLAN IDs separated by commas.



Hardware Access Control Lists

Hardware ACLs use the switch hardware filter resources to function. To view the available hardware filter resources click here.

Hardware Access Map

Create/Modify Hardware Access Map

Map Name: map 1 — *The name to uniquely identify this map.*

Forward: MAC Hardware ACL: Untruste... IP Hardware ACL: experime... Relation: And — Select Hardware ACLs to apply to the map.

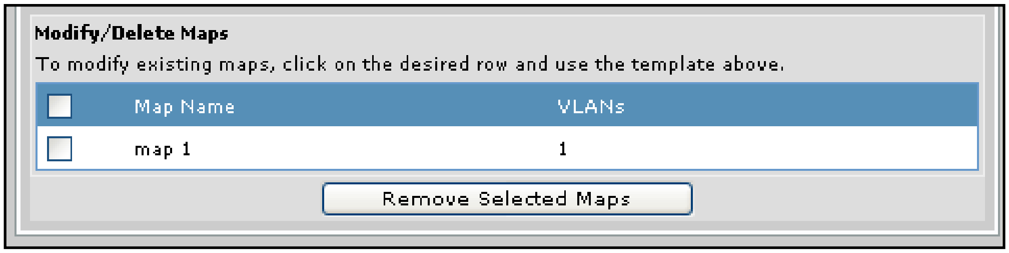
VLAN List: 1, 50, 200 — List the VLANs this map is applied to.

Modify/Delete Maps

To modify existing maps, click on the desired row and use the template above.

□	Map Name	VLANs
There are currently no hardware access maps configured.		

4. When you have completed entering the access map parameters, select **Add/Modify**. The newly created access map will appear in the list at the bottom of the menu.



Modify/Delete Maps

To modify existing maps, click on the desired row and use the template above.

□	Map Name	VLANs
□	map 1	1

5. If you need to edit or delete an access map, you can easily do that from the same menu. Mouse over to highlight the map in the list you wish to edit, and enter the new configuration information in the dialogue box. Select **Add/Modify** when your changes are complete, and the access map will be updated. To delete an access map, check the box next to the map name and select **Remove Selected Maps**.

Configuring Hardware ACLs and Hardware Access Maps Using the CLI

There are two basic steps to configuring hardware ACLs on your AOS product.

1. Configure either an IP hardware ACL, a MAC hardware ACL, or both.
2. Configure a hardware access map and apply it to a VLAN.

The following sections guide you through configuring hardware ACLs and access maps via the CLI.

Configuring an IP Hardware ACL

To configure an IP hardware ACL using the CLI, follow these steps:

1. Create and name an extended IP hardware ACL using the **ip hw-access-list extended** <*name*> command from the Global Configuration mode prompt. This command will also enter the configuration for the ACL. Enter the command as follows:

   ```
   (config)#ip hw-access-list extended Trusted
   Configuring New IP Hardware Extended ACL “Trusted”
   (config-ext-ip-hw-nacl)#
   ```

   Using the **no** form of this command removes the ACL from the unit’s configuration.

2. Specify an ACL comment using the **remark** <*text*> command. The ACL comments make it easier for another user to identify the purpose of the ACL. Enter the command from the IP hardware ACL configuration mode as follows:

   ```
   (config-ext-ip-hw-nacl)#remark permits Smith workstation
   (config-ext-ip-hw-nacl)#
   ```

   Using the **no** form of this command removes the remark from the ACL.

3. Decide whether this ACL will filter IP packets, TCP packets, or UDP packets. Depending on the protocol, you will use one of the following commands:

   [permit | deny] ip [any | host <*ip address*> **|** <*ip address*> <*wildcard*>**] [any | host** <*ip address*> **|** <*ip address*> <*wildcard*>**] [log]**

   [permit | deny] tcp [any [eq <*port*> **| range** <*min*> <*max*>**] | host** <*ip address*> **[eq** <*port*> **| range** <*min*> <*max*>**] |** <*ip address*> <*wildcard*> **[eq** <*port*> **| range** <*min*> <*max*>**]] [any [eq** <*port*> **| range** <*min*> <*max*>**] | host** <*ip address*> **[eq** <*port*> **| range** <*min*> <*max*>**] |** <*ip address*> <*wildcard*> **[eq** <*port*> **| range** <*min*> <*max*>**]] [log]**

   [permit | deny] udp [any [eq <*port*> **| range** <*min*> <*max*>**] | host** <*ip address*> **[eq** <*port*> **| range** <*min*> <*max*>**] |** <*ip address*> <*wildcard*> **[eq** <*port*> **| range** <*min*> <*max*>**]] [any [eq** <*port*> **| range** <*min*> <*max*>**] | host** <*ip address*> **[eq** <*port*> **| range** <*min*> <*max*>**] |** <*ip address*> <*wildcard*> **[eq** <*port*> **| range** <*min*> <*max*>**]] [log]**

Filtering IP Packets

If you are filtering IP packets, use the **[permit | deny] ip** command and its keywords. There are a variety of ways that you can configure IP traffic filtering, but all filtering depends on specifying whether traffic that matches the criteria will be permitted or denied and on packet source and destination information. The command can be broken down into these three groups:

```
[permit | deny] ip [source information] [destination information] [log]
```

The source information can be determined in three ways: by specifying **any**, by specifying a **host** IP address, or by specifying an IP address and a wildcard mask. Using **any** indicates that any IP address is considered a match. Specifying a **host** IP address indicates that traffic from a specific source/address is matched. Specifying an IP address and a wildcard mask indicates that a range of IP addresses are used for matching.

The destination information is also determined in the same three ways. Using the **any** keyword indicates that any IP address is considered a match, specifying a **host** IP address indicates that traffic to a specific destination address is matched, and specifying an IP address and wildcard mask indicates a range of destination IP addresses are matched.

There are a number of ways to combine these criteria. The following example specifies that IP packets from any source are permitted, but that only packets destined for a specific IP address are permitted. This essentially means that any incoming IP packets are verified against the **any** keyword, and then verified against the specific destination IP address.

```
(config-ext-ip-hw-nacl)#permit ip any host 192.168.20.0
```

When using IP addresses or wildcard masks, they should be entered in dotted decimal notation, for example, **X.X.X.X**. In the wildcard mask for source or destination IP addresses, **0** is used for matching and **1** is used for “don’t care bits.”

When specifying an IP ACL, the optional **log** parameter specifies that any entries that match the ACL criteria will be logged. Logging is beneficial when used in conjunction with the **debug hw-access-list** command, which will display the number of times in the last five seconds that an inspected IP packet has matched the entry.

Using the **no** form of this command removes the matching criteria from the hardware ACL.

Filtering TCP or UDP Packets

In addition to filtering IP packets, you can also filter TCP or UDP packets using an ACL. The filtering process works the same as with IP packets, but with additional source and destination information. You will use the **[permit | deny] [tcp | udp]** command and its keywords. There are a variety of ways that you can configure TCP or UDP traffic filtering, but all filtering depends on specifying whether traffic that matches the criteria will be permitted or denied and on packet source and destination information. The command can be broken down into these four groups:

```
[permit | deny] [tcp | udp] [source information] [destination information]
```

The source information can be defined in a number of ways. You can still use the **any** keyword, the **host** <*ip address*> parameter, or the <*ip address*> <*wildcard*> parameter, but you also have additional options for narrowing those parameters. Each of these choices for defining source information can be optionally narrowed by either defining a specific TCP or UDP port number, or you can define a range of port numbers. If you want to specify a TCP or UDP port for source packets, enter the **eq** <*port*> parameter. The command (only partially completed because it only contains source information) would appear as follows:

```
(config-ext-ip-hw-nacl)#permit tcp any eq 1080
```

If you want to define a range of port numbers for source TCP or UDP ports, enter the **range** <*min*> <*max*> parameter as follows:

```
(config-ext-ip-hw-nacl)#permit tcp any range 1080 1150
```

Port range is **0** to **65535**.

Specifying the destination for a TCP or UDP hardware ACL works the same way as setting the source information. Again, you can specify the destination by using **any**, **host** <*ip address*>, or <*ip address*> <*wildcard*>.

NOTE *IP addresses and wildcard masks must be entered in dotted decimal notation, for example,* ***X.X.X.X****. All wildcard masks for TCP or UDP hardware ACLs use* ***0*** *for matching and* ***1*** *for "don't care bits."*

You can also narrow the destination criteria by using the **eq** <*port*> or **range** <*min*> <*max*> parameters.

The following example permits any TCP packets that come from **any** IP address sending packets from port **1080**, and that are destined for IP address **192.168.20.0**.

```
(config-ext-ip-hw-nacl)#permit any tcp eq 1080 host 192.168.20.0
```

Both TCP and UDP hardware ACLs also allow you to optionally log each packet match. Enter the **log** keyword at the end of the command to turn on the logging feature. The command appears as follows:

```
(config-ext-ip-hw-nacl)#permit any tcp eq 1080 host 192.168.20.0 log
```

Using the **no** form of this command removes the matching criteria from the hardware ACL. If no other criteria are specified, the ACL will contain an implicit **permit any**.

Once you have configured either an IP, TCP, or UDP hardware ACL, you can either configure a MAC ACL, or begin configuring the hardware access map.

Configuring a MAC Hardware ACL

To configure a MAC hardware ACL using the CLI, follow these steps:

1. Create and name an extended MAC hardware ACL using the **mac hw-access-list extended** <*name*> command from the Global Configuration mode prompt. This command will also enter the configuration for the ACL. Enter the command as follows:

   ```
   (config)#mac hw-access-list extended Untrusted
   Configuring New MAC Hardware Extended ACL "Untrusted"
   (config-ext-mac-hw-nacl)#
   ```

   Using the **no** form of this command removes the ACL from the unit's configuration.

> NOTE *You cannot create an ACL with the same name as any other ACL. All ACL names must be unique.*

2. Specify an ACL comment using the **remark** <*text*> command. The ACL comments make it easier for another user to identify the purpose of the ACL. Enter the command from the MAC hardware ACL configuration mode as follows:

   ```
   (config-ext-mac-hw-nacl)#remark denies traffic to reception desk
   (config-ext-mac-hw-nacl)#
   ```

   Using the **no** form of this command removes the remark from the ACL.

3. Specify the matching criteria for the MAC hardware ACL using the **[permit | deny] mac [any | address** <*mac address*> | <*mac address*> <*wildcard*>**] [any | address** <*mac address*> | <*mac address*> <*wildcard*>**] [log]** command. As with IP hardware ACLs, this command is specifying both source and destination information for the ACL matching criteria. The command in its basic form looks like this:

   ```
   [permit | deny] mac [source information] [destination information] [log]
   ```

   Source information is defined by specifying that any MAC address will match the criteria (using the **any** keyword), that a specific MAC address will match the criteria (using the **address** <*mac address*> parameter), or that a range of MAC addresses will match the criteria (using the <*mac address*> <*wildcard*> parameter).

   Destination information is also defined using the same parameters. **Any** specifies that any destination MAC address will match the criteria, **address** <*mac address*> specifies that a specific destination MAC address will match the criteria, and using <*mac address*> <*wildcard*> specifies that a range of destination MAC addresses will match the criteria.

> NOTE *MAC addresses should be specified in 6-byte hexadecimal notation, for example, **XX:XX:XX:XX:XX:XX** (where X=0-f). Wildcards are also specified in **XX:XX:XX:XX:XX:XX** format with **0** used for matching and **f** used for wildcard bits.*

The **log** keyword is optionally used to configure the MAC ACL to log any entries that match the ACL criteria. Logging is beneficial when used in conjunction with the **debug hw-access-list** command, which will display the number of times in the last five seconds that an inspected frame has matched the entry.

Using the **no** form of this command removes the criteria from the MAC hardware ACL. If no other criteria is specified, the ACL will contain an implicit **permit any**.

In the following example, the MAC hardware ACL is configured to deny traffic from MAC address **08:00:69:02:01:FC** heading to MAC address **08:00:69:02:06:CB**. The **log** feature is also enabled.

```
(config-ext-mac-hw-nacl)#deny address 08:00:69:02:01:FC address 08:00:69:02:06:CB log
```

4. The MAC hardware ACL is now configured, and you can either configure an IP hardware ACL or move on to configuring the hardware access map.

Configuring a Hardware Access Map

To configure a hardware access map, follow these steps:

1. Create and name the hardware access map using the **hw-access-map** <*name*> command from the Global Configuration mode prompt. This command also enters the hardware access map configuration mode. Enter the command as follows:

   ```
   (config)#hw-access-map Map1
   (config-hw-access-map)#
   ```

   Using the **no** form of this command removes the hardware access map from the unit's configuration.

2. Specify which ACL(s) the access map will use, and the **and** logical relationship between the ACLs. You will only have to define the relationship if you are using more than one ACL in the access map. To specify the ACLs and their **and** relationship, enter the **forward mac** <*acl name*> **[[and] ip** <*acl name*>**]** or the **forward ip** <*acl name*> **[[and] mac** <*acl name*>**]** command from the access map configuration mode prompt.
   If you are using a MAC hardware ACL in the access map, use the **forward mac** <*acl name*> command. If you want to use an IP hardware ACL in conjunction with the MAC hardware ACL on this access map, remember that they will have an **and** logical relationship, and specify the IP hardware ACL by entering **ip** <*acl name*>.

   > NOTE *The* ***and*** *logical relationship between ACLs indicates to the access map that both ACLs must conclude the frame should be forwarded for the access map to forward it.*

   If you are using an IP hardware ACL in the access map, use the **forward ip** <*acl name*> command. If you want to use a MAC hardware ACL in conjunction with the IP hardware ACL on this access map, remember that they will have an **and** logical relationship, and specify the MAC hardware ACL by entering **mac** <*acl name*>.

   > NOTE *The* ***and*** *logical relationship between ACLs indicates to the access map that both ACLs must conclude the frame should be forwarded for the access map to forward it.*

Using the **no** form of either of these commands removes the ACL from the access map.

In the following example, the access map is configured to operate on both an IP hardware ACL (**Trusted**) and a MAC hardware ACL (**Untrusted**) specifying that both must agree on forwarding the frame before the access map will forward the frame.

```
(config-hw-access-map)#forward ip Trusted and mac Untrusted
```

3. Apply the hardware access map to a VLAN interface. The access map can be applied to a single VLAN, a list of VLANs, or a range of VLANs. Access maps are applied using the **vlans** <*vlan id*> command. To specify a single VLAN, enter the command as follows:

   ```
   (config-hw-access-map)#vlans 200
   ```

   To specify a list or range of VLANs, enter the command in the following way:

   ```
   (config-hw-access-map)#vlans 1-2,4
   ```

   Using the **no** form of this command removes the hardware access list from the specified VLAN(s).

4. The hardware access map is now configured and applied to the specified VLAN(s).

Hardware ACL Configuration Examples

The following sections describe typical hardware ACL applications in real-world settings. All of the following configurations are done using the CLI, though hardware ACL configurations can be achieved using the GUI as described in *Configuring Hardware ACLs and Hardware Access Maps Using the GUI on page 4*. The configuration parameters entered in these examples are sample configurations only. You should configure these applications in a manner consistent with the needs of your particular network. CLI prompts have been removed from the configuration examples to provide you with a method of copying and pasting configurations directly from this guide into the CLI. You should make the necessary adjustments to these configurations before adding them to your configuration to ensure they will function properly in your network.

Configuration Example 1

In this example, a hardware ACL is used on **VLAN 10** to permit only traffic from a device with an ADTRAN source MAC address. The configuration for this example includes creating a MAC hardware ACL, specifying the filtering criteria, creating the hardware access map, and applying the hardware access map to **VLAN 10**. In this example, the filtering criteria is specified by a MAC address and a wildcard mask for the source information, and **any** for the destination information.

```
mac hw-access-list extended Allowadtn
    permit mac 00:a0:c8:00:00:00 00:00:00:ff:ff:ff any
!
hw-access-map Map1
    forward mac Allowadtn
    vlans 10
!
```

Configuration Example 2

In this example, a hardware ACL is used to filter traffic only on **VLAN 1**, denying traffic from MAC address **00:a0:c8:00:11:22** while allowing only TCP traffic with a destination port of **80** or UDP traffic with a destination port of **161**. In this scenario, both ACLs must indicate traffic is to be forwarded for the access map to forward the traffic. This configuration includes creating both a MAC and IP hardware ACL, specifying their filtering criteria, creating a hardware access map, and applying the access map to **VLAN 1**.

```
mac hw-access-list extended Badmac
    deny mac 00:a0:c8:00:11:12 00:00:00:00:00:00 any
    permit any any
!
ip hw-access-list extended Allowlist
    permit tcp any any eq 80
    permit udp any any eq 161
!
hw-access-map Map1
    forward mac Badmac and ip Allowlist
    vlans 1
!
```

Hardware ACL Command Summary

The following tables summarize the commands used in different CLI configurations of hardware ACLs. Command summaries include the commands for configuring IP hardware ACLs, MAC hardware ACLs, and hardware access maps.

Table 1. IP Hardware ACL Command Summary

Access Prompt	Command	Description
(config)#	**[no] ip hw-access-list extended** *<name>*	Creates an IP hardware ACL, indicates the ACL's name, and enters the ACL's configuration mode.
(config-ext-ip-hw-nacl)#	**[no] remark** *<text>*	Specifies a comment for this IP hardware ACL.

Table 1. IP Hardware ACL Command Summary *(Continued)*

Access Prompt	Command	Description
(config-ext-ip-hw-nacl)#	**[permit | deny] ip [any | host** *<ip address>* **|** *<ip address> <wildcard>***] [any | host** *<ip address>* **|** *<ip address> <wildcard>***] [log]**	Specifies that this ACL will filter IP traffic. Also specifies whether the matched traffic will be permitted or denied and the packet source and destination information. Optionally specifies if ACL matches are logged. All IP and wildcard bits should be in the format **X.X.X.X**. All masks should be in the wildcard format where **0** is used for matching.
(config-ext-ip-hw-nacl)#	**[permit | deny] tcp [any [eq** *<port>* **| range** *<min> <max>***] | host** *<ip address>* **[eq** *<port>* **| range** *<min> <max>***] |** *<ip address> <wildcard>* **[eq** *<port>* **| range** *<min> <max>***]] [any [eq** *<port>* **| range** *<min> <max>***] | host** *<ip address>* **[eq** *<port>* **| range** *<min> <max>***] |** *<ip address> <wildcard>* **[eq** *<port>* **| range** *<min> <max>***]] [log]**	Specifies that this ACL will filter TCP traffic. Also specifies whether the matched traffic will be permitted or denied and the packet source and destination information. Optionally specifies if ACL matches are logged. All IP and wildcard bits should be in the format **X.X.X.X**. All masks should be in the wildcard format where **0** is used for matching and **1** for "don't care bits." Port number range is **0** to **65535**.

Table 1. IP Hardware ACL Command Summary *(Continued)*

Access Prompt	Command	Description
(config-ext-ip-hw-nacl)#	**[permit | deny] udp [any [eq** *<port>* **| range** *<min> <max>*] **| host** *<ip address>* **[eq** *<port>* **| range** *<min> <max>*] **|** *<ip address> <wildcard>* **[eq** *<port>* **| range** *<min> <max>*] **] [any [eq** *<port>* **| range** *<min> <max>*] **| host** *<ip address>* **[eq** *<port>* **| range** *<min> <max>*] **|** *<ip address> <wildcard>* **[eq** *<port>* **| range** *<min> <max>*] **] [log]**	Specifies that this ACL will filter UDP traffic. Also specifies whether the matched traffic will be permitted or denied and the packet source and destination information. Optionally specifies if ACL matches are logged. All IP and wildcard bits should be in the format **X.X.X.X**. All masks should be in the wildcard format where **0** is used for matching and **1** for “don’t care bits.” Port number range is **0** to **65535**.

Table 2. MAC Hardware ACL Command Summary

Access Prompt	Command	Description
(config)#	**[no] mac hw-access-list extended** *<name>*	Creates a MAC hardware ACL, indicates the ACL’s name, and enters the ACL’s configuration mode.
(config-ext-mac-hw-nacl)#	**[no] remark** *<text>*	Specifies a comment for this MAC hardware ACL.
(config-ext-mac-hw-nacl)#	**[permit | deny] mac [any | address** *<mac address>* **|** *<mac address> <wildcard>*] **[any | address** *<mac address>* **|** *<mac address> <wildcard>*] **[log]**	Specifies that this ACL will filter traffic based on MAC address. Also specifies whether the matched traffic will be permitted or denied and the frame source and destination information. Optionally specifies if ACL matches are logged. All MAC addresses should be in the format **XX:XX:XX:XX:XX:XX**. All wildcard masks should be in the format where **0** is used for matching and **f** is used for wildcard bits.

Table 3. Hardware Access Map Command Summary

Access Prompt	Command	Description
(config)#	**[no] hw-access-map** <*name*>	Creates and names a new hardware access map. Also enters the access map configuration mode.
(config-hw-access-map)#	**[no] forward mac** <*acl name*> **[[and] ip** <*acl name*>**]**	Specifies which ACL(s) the access map will use. Also specifies the logical relationship between multiple ACLs.
(config-hw-access-map)#	**[no] forward ip** <*acl name*> **[[and] mac** <*acl name*>**]**	Specifies which ACL(s) the access map will use. Also specifies the logical relationship between multiple ACLs.
(config-hw-access-map)#	**[no] vlans** <*vlan id*>	Specifies to which VLAN(s) this map is applied. This can be a single VLAN, a list of VLANs, or a range of VLANs.

Troubleshooting

The hardware ACL parameters can be viewed using the CLI. The CLI **show** and **debug** commands aid in troubleshooting by allowing a quick picture of hardware ACL component configurations. The following sections describe the CLI troubleshooting commands.

CLI Troubleshooting

The following table provides a quick look at the hardware ACL CLI troubleshooting commands.

Table 4. Hardware ACL Troubleshooting Commands

Access Prompt	Command	Description
#	**show hw-access-list [**<*name*>**]**	Displays hardware ACL configuration and statistics. The ACL list name is optional. If no name is specified, all hardware ACLs are displayed.
#	**show hw-access-map** <*name*>	Displays hardware access map configuration information.
#	**show hw-filter-resource**	Displays used and available hardware filter resources.
#	**debug hw-access-list** <*name*>	Displays hardware ACL matches associated with traffic filtering activities performed by the named hardware ACL.

Show Commands

Show commands are issued from the Enable mode prompt, and display configuration information and statistics for hardware ACLs, access maps, and filter resources. Using the <*name*> parameter for ACLs and access maps displays only the information about a specific ACL or map, rather than all configured ACLs or maps.

The following is sample output from the **show hw-access-list [**<*name*>**]** command. The first example specifies a hardware ACL by name, the second requests information on all configured hardware ACLs.

```
>enable
#show hw-access-list Trusted
IP Hardware access list extended Trusted
    permit tcp any eq 94 host 10.10.10.1 (0 matches)
```

```
>enable
#show hw-access-list
IP Hardware access list extended Trusted
    permit tcp any eq 94 host 10.10.10.1 (0 matches)
MAC Hardware access list extended Untrusted
    deny mac 00:a0:c8:00:00:00 00:00:00:ff:ff:ff any (1 match)
```

The following is sample output from the **show hw-access-map** <*name*> command:

```
>enable
#show hw-access-map Map1
    forward: IP Trusted AND Mac Untrusted
    VLANs: 10-12
```

The following is sample output from the **show hw-filter-resource** command:

```
>enable
#show hw-filter-resource
Total Rules: 512
Rules Used: 26
Total Slices: 4
Slices Used: 1
Total Ranges: 16
Ranges Used: 0
```

> NOTE *Available hardware filter resources can also be viewed using the GUI. To view these statistics using the GUI, follow the directions as outlined in Editing Hardware ACLs on page 10.*

Understanding Hardware Resources

Hardware resources can play an important part in the functioning of hardware ACLs. Each time changes are made to a hardware ACL, the hardware is reinitialized. If there are not enough hardware resources to install the new criteria in the hardware, an error message is displayed. To avoid an error, you can monitor the amount of hardware resources used by using either the **show hw-filter-resource** command described above, or you can view these statistics using the GUI as explained in *Editing Hardware ACLs on page 10*.

Hardware Resource Statistics

The statistics displayed by either method include the number of rule resources supported and the rules used, the available number of slice resources supported and the slices used, and the number of range resources supported and the ranges used. Each slice resource contains 128 rule resources and is designed to support only one feature at a time. Three features in AOS products that consume slice resources are: hardware ACLs, quality of service (QoS) class of service (CoS) untrust, and storm control. Each of these features uses at least one slice of resources, which means each feature earmarks 128 rules. Even if all the rules within a slice are not used, they are reserved for the feature using the slice and are unavailable for other features to use.

In the **show hw-filter-resource** command example (on *page 25*), we see that there are 512 total rules supported in hardware. The output also shows us that only one feature (presumably QoS CoS untrust since it is enabled by default) is currently active since only one slice is being used. Even though all the rule resources are not used in this slice resource (only 26 are used), the entire slice (and its 128 rules) is set aside for this feature. Therefore, we can deduce from the command output that there are still three slices (384 rules) available for use.

The range resource is the number of Layer 4 port ranges used and available. The unit supports a small table in the hardware that allows rules to match a range of TCP and/or UDP source and/or destination ports. For example, you might have many slices and rules available on the unit, but if you've used all 16 range resources in other hardware ACLs, and you try to apply a new ACL that filters a new range of TCP ports, you will run out of range resources. Viewing the range statistics shows you how many port ranges have been used and how many are available.

Optimizing Hardware Resources

As previously mentioned, three hardware features use hardware resources: QoS CoS untrust, storm control, and hardware ACLs. It is possible to run out of hardware resources depending on what hardware features you have configured or enabled. For example, if you have a unit that supports four total slice resources and you have configured QoS CoS untrust (**no qos trust cos**), storm control, and enough hardware ACLs to use 256 rules, you are using all four slices: one for **no qos trust cos**, one for storm control, and two for the hardware ACLs. If you adjust your hardware ACLs or the VLANs to which they are applied making the ACLs require greater than 256 rules, you are out of rule resources on the slices used by the hardware ACLs and you are out of other slice resources because they are being used by other features, so you are out of rules and your adjustment will fail. In this scenario, you need to free some hardware resources to make your adjustments.The following section describes methods for freeing hardware resources.

By default, QoS CoS is set to **no qos trust cos**, which means that the CoS value of each incoming frame on an interface is changed to the value specified by the **qos default-cos** command. This means that by default, one slice resource is set aside for QoS CoS, even if only one interface is using it. If all interfaces are changed to **qos trust cos**, the entire block of resources is freed and can be used for hardware ACLs (one slice or 128 rules). For more information about configuring QoS CoS, refer to the guide *Configuring Ethernet Switch QoS and CoS in AOS* available online at https://supportforums.adtran.com.

> NOTE
>
> *The command **no qos trust cos** is enabled by default and is hidden in the output of the **show running-config** command. You can view this switchport interface level command in the output of the **show running-config verbose** command. For more information about any of these commands, refer to the AOS Command Reference Guide available online at https://supportforums.adtran.com.*

Storm control is a feature used to configure the limits of broadcast, multicast, and unicast traffic rates on a port. By default, storm control is disabled on AOS units. If you have enabled storm control on any interface, it requires at least one slice resource, or 128 rule resources. If you disable storm control on all interfaces, the slice and rule resources are freed and can be used by hardware ACLs.

You can also free resources by optimizing the VLANs to which hardware ACLs are applied. For example, an ACL with 10 permit or deny entries, applied to four different hardware access maps which in turn are applied to four different VLANs likely uses at least 40 resources. Applying that same ACL to one hardware access map that is applied to a list or range of the same four VLANs will likely use fewer resources. Generally, continuous lists (ranges) of VLANs use fewer resources than noncontinuous lists.

Choosing a special optimized range of VLANs can help save even more hardware resources. The reduction algorithm is complicated, but examples of perfectly reduced VLAN ranges are supplied in *Table 5 on page 28*. For example, if you choose VLANS 1 through 4094, they can be optimized to use only one rule resource per ACL entry. However, if you choose VLANs 2 through 4094, they would need eleven rule resources per ACL entry, even though there is only one less VLAN in the range.

Using these techniques of resource usage reduction, the ACL with 10 entries applied to one access map that is applied to four different VLANs can use fewer resources when applied specifically to VLANs 4 through 7 (only using about 10 resources) than when applied to VLANs 2 through 5 (using about 20 resources). Compared to the first example, that used as many as 40 resources, you can see that changing VLAN ranges can reduce the number of resources consumed.

Table 5 lists VLAN ranges that have binary high/low boundaries that optimize perfectly, and therefore use the least amount of hardware resources. The table lists VLAN ranges that use the least amount of resources and can aid you in choosing the most optimized VLAN ranges to use for your configuration.

Table 5. VLAN Ranges That Optimize Hardware Resources

VLAN Range Breakdowns from Largest to Smallest Ranges							
1-4094							
1-2047	2048-4094						
1-1023	1024-2047	2048-3071	3072-4094				
1-511	512-1023	1024-1535	1536-2047	2048-2559	2560-3071	3072-3583	3584-4094
1-255	256-511	512-767	768-1023	1024-1279	1280-1535	1536-1791	1792-2047...
1-127	128-255	256-383	384-511	512-639	640-767	768-895	896-1023...
1-63	34-127	128-191	192-255	256-319	320-383	384-477	448-511...
1-31	32-63	64-95	96-127	128-195	160-191	192-223	224-255...
1-15	16-31	32-47	48-63	64-79	80-95	96-111	112-127...
1-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63...
1-3	4-7	8-11	12-15	16-19	20-23	24-27	28-31...
1	2-3	4-5	6-7	7-8	8-9	10-11	12-13...

NOTE

Applying a perfectly optimized list of VLANs from Table 5 could mean you have to pick a list that contains more VLANs than you need. It is acceptable to apply nonconfigured VLANs to a hardware access map. Frames received on VLANs that do not exist in the configuration and are not dynamically added through Generic Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP) will be discarded, so no security is sacrificed by choosing a longer list of VLANs.

In AOS firmware release 17.7, a Denial of Service (DoS) protection feature was implemented. This feature allows you to protect against DoS attacks on a per-attack type basis. This protection can be implemented using hardware ACLs, however, the DoS protection feature uses fewer hardware resources than hardware ACLs. If hardware ACLs are using more resources than you prefer, and your hardware ACLs are currently providing protection for your network that DoS protection can provide, you may want to implement the DoS feature to save hardware resources. For more information about DOS protection, refer to the configuration guide *Denial of Service Protection in AOS* available online at https://supportforums.adtran.com.

Debug Commands

Debug commands are issued from the Enable mode prompt, and display information associated with activities performed by hardware ACLs. Debug messages are printed every **5** seconds, and the match counts are the number of matches since the last debug message was printed.Using the <*name*> parameter displays only the information about a specific ACL. Only the ACL entries that include the **log** keyword are displayed by the debug command. Refer to *Configuring an IP Hardware ACL on page 14* and *Configuring a MAC Hardware ACL on page 17* for more information about the **log** keyword in ACL entries.

NOTE *Turning on a large amount of debug information can adversely affect the performance of your unit.*

Enter the command as follows to enable debug messages for the hardware ACL **Trusted**:

```
>enable
#debug hw-access-list Trusted
HARDWARE_ACCESS_LIST Trusted permit ip 10.1.1.0 0.0.0.15 192.168.0.0 0.0.255.255 (1 matches)
```

NOTE *Only hardware ACL debug messages can be displayed using this command. If you enter a software ACL name in this command, you will receive an error message.*