



Configuration Guide

Configuring a Backup Path Test Using Network Monitoring

This configuration guide describes how to configure a demand routing test call to test the availability of backup paths in ADTRAN Operating System (AOS) products. The backup path test in this configuration guide is associated with the AOS network monitoring feature, which provides a method for testing the backup path on a scheduled interval without affecting the primary path. The configuration of network monitoring, policy based routing (PBR), and the demand interface using both the Web-based graphical user interface (GUI) and the command line interface (CLI) are provided in this document, along with a configuration example and additional documentation resources.

This guide consists of the following sections:

- [*Overview of Backup Path Testing with Network Monitoring on page 2*](#)
- [*Hardware and Software Requirements and Limitations on page 4*](#)
- [*Configuring the Backup Path Test Using the GUI on page 4*](#)
- [*Configuring the Backup Path Test Using the CLI on page 18*](#)
- [*Configuration Examples on page 31*](#)
- [*Configuration Command Summary on page 34*](#)
- [*Additional Resources on page 38*](#)

Overview of Backup Path Testing with Network Monitoring

Demand routing and PBR, as well as network monitoring, can be used to schedule a test of the backup path of your network. These features allow you to schedule the backup path test at a specific time, and to specify parameters that keep the test from occurring when the backup path is in use, thus providing a method for testing paths that does not adversely affect the use of the network. The following illustration describes a typical network path, with both a primary and backup path, and the typical flow of network traffic when network monitoring is used.

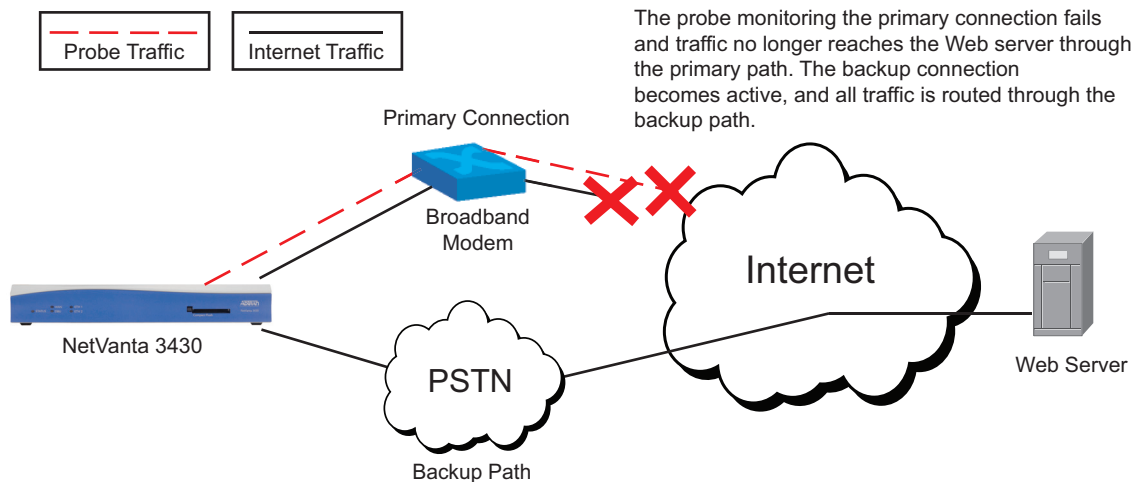


Figure 1. Typical Network with Primary and Backup Paths

In order to verify the integrity of the backup path, periodically the path can be tested. To test the backup path, network monitoring, in conjunction with PBR, is used to monitor the integrity of the primary path. When the integrity of the primary path is verified, the backup path is determined to be available for testing. Network monitoring and PBR help to determine when the backup test occurs and where the collected information from the test is logged.

A demand routing test call that uses network monitoring operates in the following manner:

- A schedule is created to identify the time frame in which the backup path should be verified.
- Two probes are created: one for testing the primary path, and another for testing the backup path.
- The primary path is verified by sending a probe packet across the primary path. If the primary path is verified by a successful response to the probe, the backup path test call occurs and a probe is sent through the demand interface to verify the backup path.
- If the probe for the primary path fails, the primary path is removed from the route table. The demand routing interface is then used as the backup path for the network, and the test is aborted because the demand interface is in use.
- When the scheduled window for the test expires, the call is terminated.
- The test begins again at the next scheduled interval.

The following sections give a brief overview of the features used to configure the backup path demand routing test.

Demand Routing

Demand routing is an AOS feature that creates and terminates dialup links based on more specific parameters than the status of an interface. Access control lists (ACLs) can be used with demand routing to determine when to initiate a dialup connection or a dial-backup connection, based on the interesting traffic defined in the ACL. Demand routing is configured on the demand interface, and demand routing configuration for a backup path test call with network monitoring is based upon determined interesting traffic for the interface.

Network Monitoring

Network monitoring is an AOS feature composed of multiple parts designed to test and control connectivity routes within a network structure. The primary function of network monitoring is to detect and remove failed routes so that backup routes can take effect, and then restore the failed routes when they are functioning properly again. The network monitoring feature is composed of three main mechanisms: probes, tracks, and schedules. Probes are objects in the unit's configuration that collect information about network connectivity by sending test traffic across network paths. Tracks are objects in the unit's configuration created to monitor probes for state changes (from PASS to FAIL or vice versa), and cause other objects to take action based on the probe's state. A probe can monitor network conditions, but cannot take any action on its own. The track is tied to the probe through configuration, and specifies that an object (interface, schedule, etc.) will perform an action based on the probe's (track's) state. Schedules are objects in the unit's configuration that monitor the time of day and day of the week, and are used to determine what times during the day and how often tracks and probes are active. Network monitoring configuration for a backup path test call includes creating two probes, one to test the primary path to make sure it is functional, and one to test the backup path. In addition, a schedule is created for the test, and two tracks are created to associate the schedule with the test actions and to monitor the two test probes.

Policy Based Routing

PBR is an AOS feature that allows you to implement basic traffic engineering on your network. You can use this feature to manipulate the path that a packet follows based on the characteristics of that packet, and route traffic with the same destination over different paths according to the traffic's priority, source, or size. PBR configuration for a demand routing test call includes creating two route maps: one for when the test is conducted normally (the backup dial path is not in use), and one for when the test is aborted (the backup dial path is in use). PBR provides a method for routing the probe traffic either to the null interface or to the demand interface.

SNMP (Optional)

Simple Network Management Protocol (SNMP) can be used with network monitoring to report changes in track states, whether from a PASS to a FAIL state, or a FAIL to a PASS state. When used with network monitoring, SNMP can alert you when the track has changed states and makes network management of monitored devices and the condition of the track more easily monitored. Using SNMP with network monitoring and the dial backup path test is optional. To use SNMP with network monitoring, you must enable SNMP, specify the type of SNMP used, enable network monitoring SNMP traps (either all network monitoring traps or traps for a specific host), and add SNMP trap capabilities in the network monitoring track.

Configuration Steps

Configuring the backup path test consists of these steps:

1. Create an Internet Control Messaging Protocol (ICMP) probe to test the primary path for use.
2. Create an ICMP probe to test the backup path.
3. Create the test schedule.
4. Create a Primary track that becomes active based on the schedule and is used to monitor the status of the primary path. This track monitors the ICMP probe that tests the primary path. When that probe is in a PASS state, the track is also in a PASS state.
5. Create a Standby track that becomes active based on the status of the ICMP probe used to test the primary path. This track monitors the second ICMP probe, and when that probe is in a PASS state, the track is also in a PASS state, indicating that the backup test has either passed or failed.
6. Create the PBR route maps and ACLs to route the probe traffic. These ACLs route the probe traffic based on the Primary track state.
7. Configure the demand interface and define the interesting traffic for the interface.
8. Enable SNMP network monitoring track traps in both SNMP configuration and in the track configuration (optional).

Hardware and Software Requirements and Limitations

To create a backup path test using network monitoring, your AOS product must support network monitoring and demand routing. To check that your platform has these features, refer to the [Product Feature Matrix](#) (Knowledge Base article 2272).

SNMP traps for network monitoring are available in AOS firmware release 18.01.00 or later.

When a backup path test using network monitoring is created, a probe is sent out over the backup wide area network (WAN) connection as long as the primary default route is in the routing table. Once the primary default route is removed from the routing table, this probe is sent to the null interface.

Each feature used in the backup path test has its own requirements and limitations. For more information about these features, refer to the feature-specific documentation provided online at ADTRAN's knowledge base, <http://kb.adtran.com>. These documents are also outlined in [Additional Resources on page 38](#).

Configuring the Backup Path Test Using the GUI

The backup path test can be configured using either the CLI or the GUI. To configure the backup path test using the GUI, complete the following tasks:

- Access the GUI.
- Create the ICMP probe to test the primary path for functionality.
- Create the ICMP probe to test the backup path.
- Create the test schedule.
- Create the Primary track.
- Create the Standby track.

- Create the PBR route maps and ACLs to route the probe traffic.
- Configure the demand interface and define the interesting traffic for the interface.
- Configure SNMP network monitoring traps (optional).

Accessing the GUI

To begin configuring the backup path test through the GUI, follow these steps:

1. Open a new Web page in your Internet browser.
2. Enter 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**.

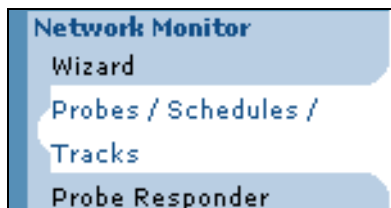


*The default user name is **admin** and the default password is **password**.*

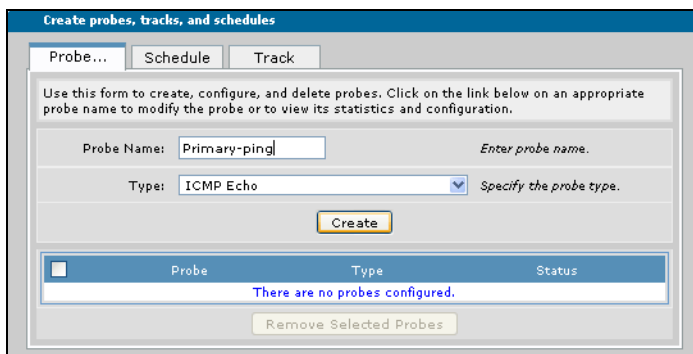
Creating the ICMP Probes for Primary and Backup Path Testing

The first ICMP probe is used in the backup path test to determine if the primary path is functioning properly. If the probe fails, the primary path is not up, which indicates that the backup path is in use. If the backup path is in use, the backup path test sends the probe packets to the null interface to avoid adversely affecting the backup path. If the probe passes, the primary path is functional, which indicates the backup path is not in use. If the backup path is unused, the backup path test occurs normally. To create the ICMP probe using the GUI, follow these steps:

1. Navigate to **Network Monitor > Probes/Schedules/Tracks**.



2. In the **Probe** menu, define the ICMP probe. Enter a name for the probe in the **Probe Name** field. The ICMP probe is used to test the primary path for traffic, so this probe is named **Primary-ping**. Specify the probe type as **ICMP Echo** using the **Type** drop-down menu. Select **Create** to create the probe.

A screenshot of the "Create probes, tracks, and schedules" dialog box. The dialog has three tabs: "Probe...", "Schedule", and "Track". The "Probe..." tab is selected. Below the tabs, there is a text area with instructions: "Use this form to create, configure, and delete probes. Click on the link below on an appropriate probe name to modify the probe or to view its statistics and configuration." Below this, there are two input fields: "Probe Name:" with the value "Primary-ping" and "Type:" with a dropdown menu set to "ICMP Echo". There is a "Create" button below these fields. At the bottom, there is a table with columns "Probe", "Type", and "Status". The table is currently empty, with a message "There are no probes configured." below it. There is also a "Remove Selected Probes" button at the bottom.

- After selecting **Create**, the probe's configuration menu appears. Here you will enable the probe and specify the probe's period, timeout, tolerance, and destination.

"Probe Primary-ping" Configuration

Edit the information for probe Primary-ping below.

Enable: *Enable the probe.*

Probe Period: (secs) *Time between probe test attempts in seconds. (ICMP range 1-65535), (TCP & HTTP range 60-65535)*

Timeout: (msecs) *Time to wait before declaring test failed (msec). Must be less than the probe-period. (250-4,294,967,295)*

Mode: *Configure the tolerance and its specifications for probe state transitions.*

Tolerance: Number of failures: Number of successes:

Destination hostname: *Enter destination hostname or an IP address. (required)*

Source IP address: . . . *Enter source IP address. (optional)*

Data size: *Length of the ICMP packet (0-1462)*

Data pattern: *Hexadecimal pattern for the ICMP packet (without the 0x)*

Enable the probe by selecting the **Enable** check box.

The probe's period is the time between probe test attempts (in seconds). Specify this period by entering a time (in seconds) in the **Probe Period** field. The period range for ICMP probes is **1** to **65535** seconds. By default, the ICMP probe period is **60** seconds. For most ICMP echo probes, the period will need to be reduced to much less than 60 seconds. For the backup path test in this example, the probe's period is **10** seconds.

The probe's timeout value is the determined time (in milliseconds) in which a returned packet must be received before a test is considered failed. The timeout value ranges from **1** to **900000** milliseconds, and the ICMP probe default is **1500** milliseconds. For the backup path test, leave the timeout at the default value.

The probe's tolerance is the number of tests that must pass or fail before the probe changes states. Probe tolerances can be either consecutive, which means the probe must either pass or fail a certain number of times in a row for the probe to change states, or based on a rate, which means the probe must either fail or pass a certain number of times in a specified number of tests before changing states. The tolerance in this example is set to **Consecutive** for the backup path test. When you select **Consecutive** from the **Mode** drop-down menu, you must also specify the consecutive number of failures required for the probe to change states, as well as the number of successes required for the probe to change states. Valid ranges for consecutive failures and successes are **1** to **255**. For the backup path test, set the **Number of failures** to **3**, and the **Number of successes** to **2**.

Next, specify the ICMP probe's **Destination hostname**. The destination can be a host name or an IP address, and it should be the public IP address of the primary connection. In the previous illustration, the **Destination hostname** is **192.0.2.1**.

You do not need to specify the probe's **Source IP address**, **Data size**, or **Data pattern** for the backup path test. When you have configured the probe's period, timeout, tolerance, and destination and enabled the probe, select **Apply** to apply the settings. The newly created probe appears in the list of probes. The probe's configuration can be edited by selecting the probe's name from the list.



For more information about probes, probe configuration, and how probes work, refer to the configuration guide [Network Monitoring in AOS](#) (Knowledge Base article 3007).

4. Create the second ICMP probe to test the backup path by repeating Steps 1 to 3 and entering the following configuration parameters:
 - Probe Name: **Standby-ping**
 - Probe Type: **ICMP Echo**
 - Destination: **companyx.net**



For backup path testing, the destination host name of the second ICMP probe should be the host name of a remote host routed through the backup Internet connection.

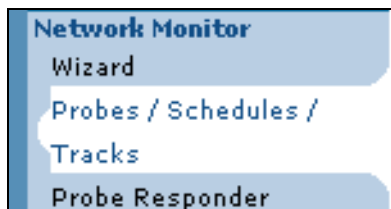
- Period: **60**
- Tolerance Mode: **Consecutive**
- Tolerance Number of Failures: **2**
- Tolerance Number of Successes: **2**

The second ICMP probe (**Standby-ping**) is used to test the backup path when the initial probe (**Primary-ping**) determines that the backup path is not in use (primary path is found to be valid). If the primary probe detects that the primary path is not valid (thus indicating the backup path is in use), the second ICMP probe is sent to the null interface to avoid adversely affecting network traffic.

Creating the Backup Path Test Schedule

The backup path test schedule is used to determine when the backup path is tested. To configure the schedule using the GUI, follow these steps:

1. Navigate to **Network Monitor > Probes/Schedules/Tracks**.



2. Select the **Schedule** tab and enter a name for the schedule in the **Schedule Name** field. For the backup path test in the illustration below, the schedule is named **Daily**. Select **Create** to create the schedule.

 A screenshot of the "Create probes, tracks, and schedules" wizard. The "Schedule" tab is selected. The form contains a "Schedule Name" field with the value "Daily" and a "Create" button. Below the form is a table with columns "Schedule", "Type", and "Status". The table is currently empty, with the text "There are no schedules configured." displayed. A "Remove Selected Schedules" button is located at the bottom of the table.

3. After selecting **Create**, the schedule configuration menu appears. Here you will specify the type of schedule, the days the schedule is active, the start and end time that the schedule runs, and whether the schedule runs to the specified ending time or whether the schedule runs for a specified amount of time.

 A screenshot of the "Schedule Daily" configuration window. The window title is "Schedule Daily Configuration". It contains the following fields:

- Type:** A dropdown menu set to "Periodic".
- Day(s):** A list of days with checkboxes: Daily, Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday. All checkboxes are checked.
- Start time:** A text field containing "12:00".
- To or For:** A dropdown menu set to "For".
- End time:** A text field containing "00:10".

 At the bottom of the window are "Reset" and "Apply" buttons.

For the backup path test schedule, from the **Type** drop-down menu, select **Periodic**. Next, specify the **Day(s)** the schedule is active as **Daily** by selecting the check box next to that option. Specify the schedule **Start time** by entering the time (in military HH:MM format) in the appropriate field. In the previous example, the schedule starts at **12:00** p.m. Next, specify that the schedule is active for a specific amount of time by selecting **For** from the **To or For** drop-down menu. Lastly, enter the schedule **End time** by entering the time (in HH:MM format) in the appropriate field. Select **Apply** to apply the schedule settings.

- The newly created schedule appears in the list of schedules. The schedule's configuration can be edited by selecting the schedule's name from the list.

Schedule	Type	Status
<input type="checkbox"/>	Daily	Periodic
		Inactive

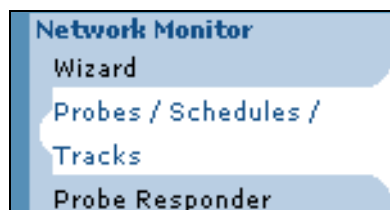


For more information about schedules, schedule configuration, and how schedules work, refer to the configuration guide [Network Monitoring in AOS](#) (Knowledge Base article 3007).

Creating the Primary and Standby Tracks

The Primary track is the track used to activate the backup path test. The track is associated with both the backup path test schedule and the **Primary-ping** ICMP probe. When the schedule becomes active, the track changes from a FAIL to a PASS state and activates the **Primary-ping** ICMP probe to test the primary path. To configure the Primary (and Standby) track using the GUI, follow these steps:

- Navigate to **Network Monitor > Probes/Schedules/Tracks**.



2. Select the **Track** tab and enter the track's name in the appropriate field. For the backup path test, this track is named **Primary**. Select **Create** to create the track.

The screenshot shows the 'Create probes, tracks, and schedules' dialog box with the 'Track' tab selected. The 'Track Name' field contains 'Primary'. Below the field is a 'Create' button. At the bottom, there is a table with columns 'Track', 'Status', and 'Test Logic'. The table is currently empty, with a message 'There are no tracks configured.' and a 'Remove Selected Tracks' button below it.

3. After selecting **Create**, the track configuration menu appears. Here you will enable the track, specify the logical operation the track uses, and associate the track with the schedule and probe.

The screenshot shows the 'Track Primary' Configuration dialog box. It contains several fields and options:

- Enable:** A checked checkbox.
- Dampening-interval:** A text box containing '1'.
- Logical Operator:** A dropdown menu set to 'None'.
- Set Test Objects:** A table with columns 'Object Type', 'Object', and 'Negate'.

Object Type	Object	Negate
Schedule	Daily backu...	<input type="checkbox"/>
Probe	Primary-pin...	<input type="checkbox"/>
<Select>		
<Select>		
<Select>		
- Execute TCL:** An unchecked checkbox.

Buttons for 'Reset' and 'Apply' are at the bottom.

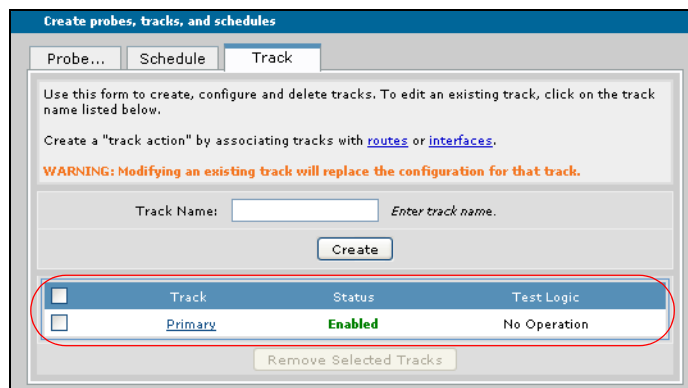
Enable the track by selecting the **Enable** check box.

Specify the logical operation of the track by selecting **None** from the **Logical Operator** drop-down menu.

Associate the track with the backup path test schedule and the ICMP probe. To associate the track and the schedule, select **Schedule** from the **Object Type** drop-down menu, and then select **Daily backup test** (name of the created schedule) from the **Object** drop-down menu. To associate the track and the ICMP probe, select **Probe** from the **Object Type** drop-down menu, and then select **Primary-ping** (name of the created ICMP probe) from the **Object** drop-down menu.

You do not need to configure the track's **Dampening-interval**. Tool command language (Tcl) scripts can optionally be associated with the track, which provides you with a method of determining how track changes are reported to you. For more information about configuring and using Tcl scripts, refer to the configuration guide [Tcl Scripting in AOS](#) (Knowledge Base article 2159).

- Once you have enabled the track and associated the track with the schedule and probe, select **Apply** to apply the settings. The newly configured track appears in the track listing. To edit the track, select the track's name from the list.



- Create the second track (**Standby**) to monitor the secondary probe (**Standby-ping**) by repeating Steps 1 to 4 and entering the following configuration parameters:
 - Track Name: **Standby**
 - Logical Operator: **None**
 - Object Type: **Probe**
 - Object: **Standby-ping**

The second track (**Standby**) monitors the secondary probe (**Standby-ping**), which verifies the backup path. This track changes states based on the state of the **Standby-ping** probe. When the probe is in a PASS state (indicating the backup path is valid), the track is in a PASS state. When the probe is in a FAIL state (indicating the backup path is not valid), the track is in a FAIL state. Various methods, such as Tcl scripts, event logs, and email logs, can be used to report track state changes to you. You should use the reporting method that best matches your network needs.

Creating PBR Route Maps and ACLs

The PBR route maps and ACLs are used to route the probe traffic. In configuring PBR for the backup path test, you will configure two different maps and two different ACLs. One route map and ACL is used to route the **Standby-ping** probe traffic to the null interface if the backup path is in use. The second route map and ACL is used to route the **Standby-ping** probe traffic to the demand interface to test the backup path. PBR must be configured before configuring the demand interface parameters for the backup path test; however, PBR can only be configured using the CLI. Refer to [Creating PBR Route Maps and ACLs on page 24](#) now to configure PBR using the CLI.

Configuring the Demand Interface

To configure the demand interface for the backup path test, you will need to define interesting traffic for the interface. It is assumed that your demand interface is already configured and operational. If you need assistance configuring the demand interface, refer to the common application guide [Configuring Demand Routing in AOS](#) (Knowledge Base article 2225).

Defining Interesting Traffic

Interesting traffic must be defined for the demand interface by configuring an ACL. When packets matching the ACL are detected by the demand interface, it will attempt to connect to the backup path.

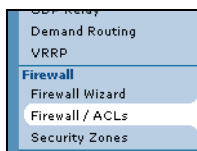
Interesting traffic can be specified for inbound or outbound traffic directions. When the demand interface matches interesting outbound traffic, it can attempt to originate a connection and will reset the idle timer on a connected link. When the demand interface matches interesting inbound traffic, it allows the call to remain connected.



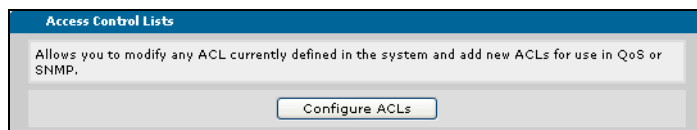
By default, the demand interface is configured to either answer or originate a call. If you have changed your demand interface configuration, you will need to make sure it can originate calls for the backup path test to function properly.

To create an ACL used for defining demand interface interesting traffic, follow these steps:

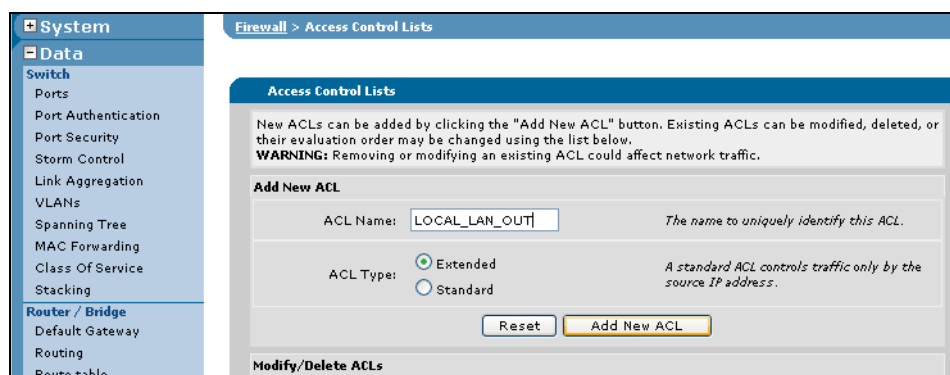
1. Navigate to **Data > Firewall > Firewall/ACLs**.



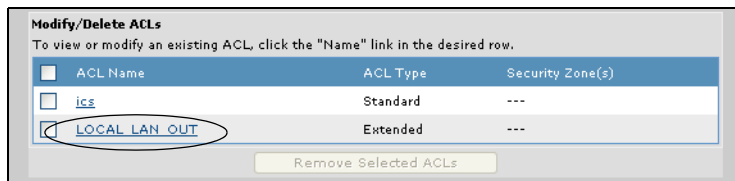
2. Scroll down to the **Access Control Lists** dialog box, and select **Configure ACLs**.



3. Enter a name for the ACL in the **ACL Name** field (**LOCAL_LAN_OUT** in this example) and select **Extended** for the **ACL Type**. Then select **Add New ACL**.

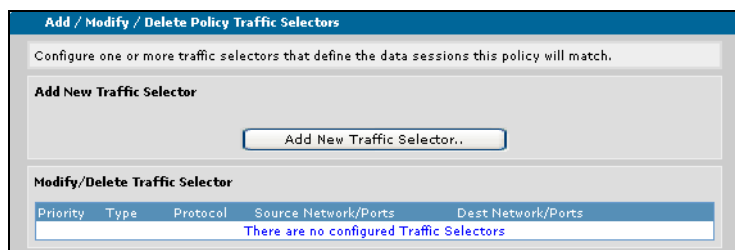


4. The new ACL will appear in the ACL list.

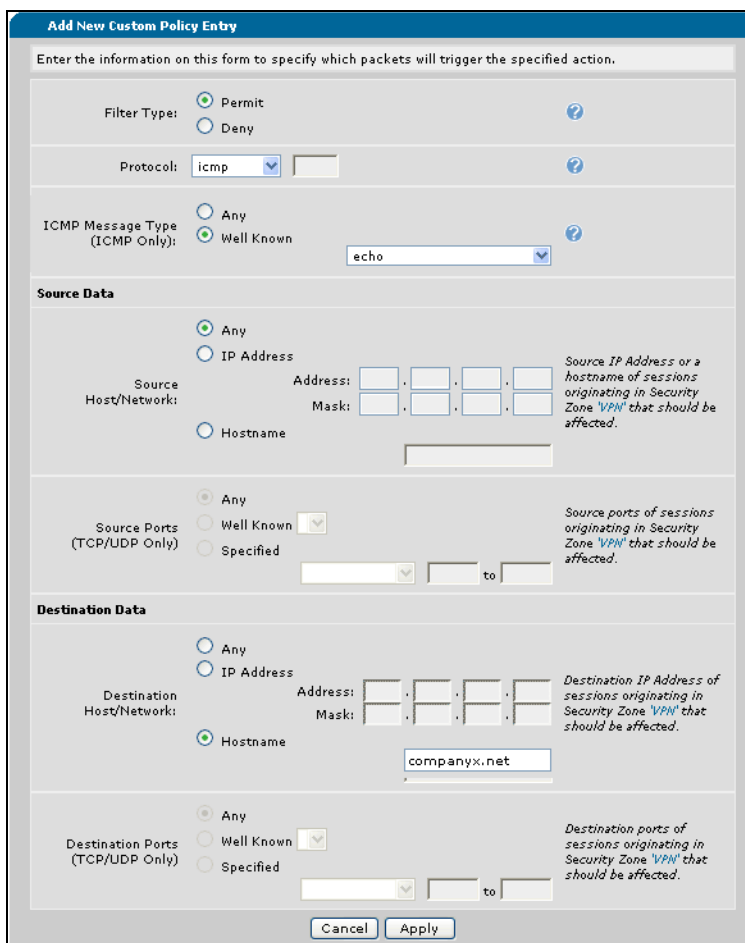


5. Using the check box, select the ACL that will be applied to the demand interface from the ACL list.

6. Select **Add New Traffic Selector**.



7. Enter the parameters to define which packets will be monitored by the ACL.



8. In this example, the ACL is set to:
- Filter Type: **Permit**
 - Protocol: **ICMP**
 - ICMP Message Type: **Well Known, echo**

NOTE *To limit what brings up the demand interface, or what brings it down, consider setting the protocol to your specific network needs.*

- Source Data: **Any**
- Destination Data: **Hostname, companyx.net**

NOTE *The destination for the demand interface ACL should be the same as the destination for the ICMP probe that tests the backup path.*

9. Once the action, source, and destination information for the ACL has been entered, select **Apply**. The ACL has now been defined, and can be applied to the demand interface.

NOTE *The ACL examples in this configuration guide are specific to using the ACLs for demand interface activation and modem connection. For more options and configurations of ACLs, refer to the configuration guide [Configuring IP ACLs in AOS](#) (Knowledge Base article 3087).*

Applying the ACL to the Demand Interface

The ACL must be applied to the demand interface for the interface to determine interesting traffic. To apply the ACL to the demand interface, follow these steps:

1. Navigate to **Data > Router/Bridge > Demand Routing**.

The screenshot shows the network management GUI. On the left is a navigation menu with categories like 'Port Authentication', 'Router / Bridge', and 'Firewall'. The main content area is titled 'Add New Demand Interface'. It has a 'Demand Number' input field and an 'Add New Interface' button. Below this is a table with columns: Number, Description, Resource Pool, and State. The table contains one entry: '1' in the Number column, 'demand 1' in the Description column (circled in red), and 'Enabled' in the State column. Below the table is a 'Remove Selected Interfaces' button. The second section is titled 'Assign Dial Interfaces to a Resource Pool'. It contains a message: 'There are no resource pools for a member to be assigned.' and an 'Add' button. Below this is another table with columns: Interface, Current Pool, and Current Priority. The message 'There are no members set.' is displayed in the table area. A 'Remove Selected Members' button is at the bottom.

2. Select the demand interface to which to apply the ACL (**demand 1** in this example).

- After selecting the interface, the demand interface configuration menu appears. Scroll to the **Demand Configuration** portion of this menu.

Demand Configuration	
Called Number:	<input type="text"/> <i>Called party's telephone number</i>
Caller Number:	<input type="text"/> <i>Calling party's telephone number</i>
Connect Mode:	Originate&Answer <input type="button" value="v"/> <i>Connection Mode</i>
Connect Order:	Beginning <input type="button" value="v"/> <i>Connection order</i>
Connect Sequence Attempts:	<input type="text" value="1"/> <i>Number of attempts (0-65535, 0 is unlimited)</i>
Interface Recovery:	<input type="checkbox"/> <i>Enable interface recovery mode.</i>
Interface Recovery Retry Interval:	<input type="text" value="120"/> <i>Number of seconds delay between connect sequence cycles (1-65535)</i>
Demand Hold Queue:	<input type="text" value="200"/> <i>Demand hold queue size (packets) (0-200)</i>
Demand Hold Queue Timeout:	<input type="text" value="3"/> <i>Demand hold queue timeout (0-255)</i>
Idle Timeout:	<input type="text" value="120"/> <i>Number of idle timeout seconds (1-2147483)</i>
Fast Idle Timeout:	<input type="text" value="120"/> <i>Number of fast-idle seconds (1-2147483)</i>
Match-interesting Traffic:	ACL Name: <input type="text" value="MatchAll"/> <input type="button" value="v"/> Match Logic: <input type="text" value="Normal"/> <input type="button" value="v"/> <i>Configure match-interesting traffic. To add a new ACL, go to the "Firewall" page and click on the "Configure ACLs" button at the bottom of the page.</i>
Match traffic Direction:	<input type="text" value="both"/> <input type="button" value="v"/>

- In the **Match-interesting Traffic** section, select the appropriate ACL from the **ACL Name** drop-down menu. Select **Normal** from the **Match Logic** drop-down menu, and specify the match direction from the **Match Traffic Direction** drop-down menu.
- Select **Apply** at the bottom of the demand interface configuration menu to apply the ACL to the demand interface.

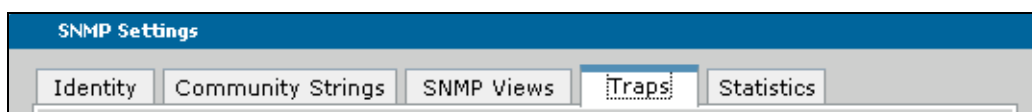
Configuring SNMP Traps for Network Monitoring Track State Changes (Optional)

SNMP traps can optionally be enabled for network monitoring track state changes using the GUI. Enabling these tracks allows an SNMP trap to be sent whenever the associated track changes states. To configure SNMP traps for track state changes, you must enable the SNMP agent, configure the version of SNMP to use, and enable track traps either on a per-host basis, or for all SNMP monitoring. Lastly, you must add the SNMP trap reporting capability to the network monitoring track. To configure SNMP network monitoring track traps using the GUI, follow these steps:

1. Navigate to **System > SNMP**.



2. Select **Traps** from the **SNMP Settings** menu.



3. In the **SNMP Traps** menu, specify the **Destination** IP address to which the trap is sent, the **Community String** to include in the trap, and the **SNMP Version** of the trap to send. In the following example, the **Destination Address** is **10.23.1.181**, the **Community String** is **Public**, and the **SNMP Version** is **1**. Next, select **Track** from the list of traps by selecting the appropriate box. This specifies that network monitoring SNMP traps are enabled for all configured tracks. Select **Add** when all information has been entered.

 A screenshot of the "SNMP Settings" configuration page, specifically the "Traps" tab. The page has a blue header with the text "SNMP Settings". Below the header is a horizontal row of five tabs: "Identity", "Community Strings", "SNMP Views", "Traps", and "Statistics". The "Traps" tab is selected. Below the tabs is a text box containing the following text: "A SNMP trap allows the NetVanta to send a trap message to a specified destination when an event occurs. To modify an existing trap destination entry or add another trap destination entry based on a previously configure entry, click on a row in the list." Below this text are three rows of configuration fields: "Destination Address: 10 . 23 . 1 . 181" with a tooltip "The destination address to send the SNMP trap to.", "Community String: Public" with a tooltip "The community string to include in the SNMP trap.", and "SNMP Version: 1" with a dropdown arrow and a tooltip "The version of SNMP trap to send." Below these fields is a section labeled "Enable Traps:" with four checkboxes: "SNMP", "Frame Relay", "BGP", and "Track". The "Track" checkbox is checked. Below the checkboxes is a tooltip "Select the trap(s) the NetVanta will send." At the bottom right of the form is an "Add" button.


For more information about the configurable SNMP parameters, refer to the configuration guide [SNMP in AOS](#) (Knowledge Base article 1134).

4. After selecting **Add**, the SNMP trap configuration information is listed at the bottom of the **SNMP Settings** menu, and tracks that have SNMP traps enabled are listed. In the following example, the **STANDBY** track is listed with **State-Change** traps enabled. All configured tracks will be displayed with the option to enable the state change trap when SNMP track traps are enabled using the GUI. If you need to remove SNMP traps from a track, deselect the check box next to the appropriate track in the list and select **Apply**.

The screenshot shows the SNMP Settings GUI. At the top, there is a table with columns: Destination Address, Community String, Version, and Traps. Below this is a 'Remove Selected Traps' button. A message states: 'This is a list of all entities that support sending a trap and the trap that is currently enabled.' Below this is a table with columns: Device, Link-Status Trap, and Other Traps. The 'STANDBY' track is highlighted with 'State-Change' checked. An 'Apply' button is at the bottom.

Destination Address	Community String	Version	Traps
<input type="checkbox"/>	10.23.1.181	Public	SNMPv1 Track

Remove Selected Traps

This is a list of all entities that support sending a trap and the trap that is currently enabled.

Device	Link-Status Trap	Other Traps
eth 0/1	<input checked="" type="checkbox"/>	
eth 0/2	<input checked="" type="checkbox"/>	
t1 1/1	<input checked="" type="checkbox"/>	<input type="checkbox"/> Line Status <input type="checkbox"/> Threshold
swx 0/1	<input checked="" type="checkbox"/>	
swx 0/2	<input checked="" type="checkbox"/>	
swx 0/3	<input checked="" type="checkbox"/>	
swx 0/4	<input checked="" type="checkbox"/>	
swx 0/5	<input checked="" type="checkbox"/>	
swx 0/6	<input checked="" type="checkbox"/>	
swx 0/7	<input checked="" type="checkbox"/>	
swx 0/8	<input checked="" type="checkbox"/>	
vlan 1	<input type="checkbox"/>	
bvi 6	<input checked="" type="checkbox"/>	
ppp 1	<input type="checkbox"/>	
demand 1	<input type="checkbox"/>	
vlan 2	<input type="checkbox"/>	

Track: STANDBY State-Change

Apply

Once you have configured the network monitor schedule, probes, and track, the PBR route maps and ACLs, and applied the interesting traffic ACL to the demand interface and optionally enabled SNMP traps for network monitoring tracks, the backup path test configuration is complete.

Configuring the Backup Path Test Using the CLI

The backup path test can be configured by either using the CLI or the GUI. To configure the backup path test using the CLI, complete the following tasks:

- Access the CLI.
- Create the ICMP probe to test the primary path for functionality.
- Create the ICMP probe to test the backup path.
- Create the test schedule.
- Create the Primary track.
- Create the Standby track.
- Create the PBR route maps and ACLs to route the probe traffic.
- Configure the demand interface and define the interesting traffic for the interface.
- Configure SNMP traps for network monitoring track state changes (optional).

Accessing the CLI

To access the CLI on your AOS unit, follow these steps:

1. Boot up the unit.
2. Telnet to the unit (**telnet** <ip address>). For example:

```
telnet 208.61.209.1.
```



If during the unit's setup process you have changed the default IP address (10.10.10.1), use the configured IP address.

3. Enter your user name and password at the prompt.



*The AOS default user name is **admin** and the default password is **password**. If your product no longer has the default user name and password, contact your system administrator for the appropriate user name and password.*

4. Enable your unit by entering **enable** at the prompt as follows:

```
>enable
```

5. Enter your Enable mode password at the prompt.
6. Enter the unit's Global Configuration mode as follows:

```
#configure terminal
(config)#
```

Creating the ICMP Probes for Primary and Backup Path Testing

The first ICMP probe is used in the backup path test to determine if the primary path is valid. If the probe fails, the primary path is not valid, which indicates that the backup path is in use. If the backup path is in use, the backup path test sends the results to the null interface to avoid adversely affecting the backup path. If the probe passes, the primary path is valid, which indicates the backup path is not in use. If the backup path is unused, the backup path test occurs normally. To create the ICMP probe using the CLI, follow these steps:

1. Specify a name for the probe and the probe type using the **probe** <name> [**http-request** | **icmp-echo** | **tcp-connect**] command from the Global Configuration mode prompt. Enter the command as follows:

```
(config)#probe Primary-ping icmp-echo
(config-probe-Primary-ping)#
```

In the previous example, the probe's name is **Primary-ping**, the probe type is **icmp-echo**. The probe's configuration mode has been entered, indicated by the config-probe-Primary-ping prompt.

- Specify the probe's destination using the **destination** *<ip address | hostname>* command from the probe's configuration mode. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**) and host names should be fully qualified (for example, **www.company.com**). Enter the command as follows:

```
(config-probe-Primary-ping)#destination 10.10.10.1
```

```
(config-probe-Primary-ping)#
```



For the backup path test, the destination IP address of the ICMP probe should be the IP address of the remote host routed through the primary Internet connection.

- Specify the probe's period using the **period** *<value>* command from the probe's configuration mode. The period specifies the time (in seconds) between probe test attempts. Valid range is **1** to **65535** seconds, with a default value of **60** seconds. For most ICMP echo probes, the period will need to be reduced to much less than 60 seconds. For the backup path test, the probe's period in this example is **10** seconds. Enter the command as follows:

```
(config-probe-Primary-ping)#period 10
```

```
(config-probe-Primary-ping)#
```

- Specify the probe's tolerance by using the **tolerance consecutive** [**pass** *<number>* | **fail** *<number>*] command. The **consecutive** keyword indicates that the probe must either pass or fail a certain number of times in a row to change states. Valid range for consecutive passes and failures is **1** to **255**. For the backup path test, set the number of failures to **3**. Enter the command from the probe's configuration mode as follows:

```
(config-probe-Primary-ping)#tolerance consecutive fail 3
```

```
(config-probe-Primary-ping)#
```

The proceeding example specifies that the probe **Primary-ping** will change to a FAIL state if **3** tests in a row fail.

- Activate the probe using the **no shutdown** command. Enter the command at the probe's configuration mode as follows:

```
(config-probe-Primary-ping)#no shutdown
```

```
(config-probe-Primary-ping)#
```



For more information about probes, probe configuration, and how probes work, refer to the configuration guide [Network Monitoring in AOS](#) (Knowledge Base article 3007).

- Create the second ICMP probe to test the backup path by repeating Steps 1 to 5 and entering the following configuration parameters:
 - Probe Name: **Standby-ping**
 - Probe Type: **ICMP Echo**

- Destination: **companyx.net**



For backup path testing, the destination host name of the second ICMP probe should be a remote host routed through the backup Internet connection.

- Period: **60**
- Tolerance Mode: **Consecutive**
- Tolerance Number of Failures: **2**
- Tolerance Number of Successes (Passes): **2**

The second ICMP probe (**Standby-ping**) is used to verify the backup path when the initial probe (**Primary-ping**) determines that the backup path is not in use (primary path is found to be functional). If the primary probe detects that the primary path is not functional (thus indicating the backup path is in use), the second ICMP probe is sent to the null interface to avoid adversely affecting network traffic.

The **Standby-ping** probe configuration should appear as follows:

```
(config)#probe Standby-ping icmp-echo
(config-probe-Standby-ping)#destination companyx.net
(config-probe-Standby-ping)#period 60
(config-probe-Standby-ping)#tolerance consecutive fail 2 pass 2
(config-probe-Standby-ping)#no shutdown
```

Creating the Backup Path Test Schedule

The backup path test schedule is used to determine when the backup path is tested. To configure the schedule using the CLI, follow these steps:

1. Create a schedule using the **schedule <name>** command entered from the Global Configuration mode prompt. Creating a schedule enters the Schedule Configuration mode. Enter the command as follows:


```
(config)#schedule Daily
(config-schedule-Daily)#
```

Using the **no** form of this command removes the specified schedule from the unit's configuration.
2. Specify the schedule type, start time, and end time using the **periodic** command.

You can choose to configure a periodic schedule using a variety of command variations. To specify a periodic schedule that occurs on a specific day (or range of days) and begins and ends at specified times, you would use the **periodic <day> <time> to <time>** command. In this case, the day parameter can be one day of the week (**monday**, for example) or could be up to seven days of the week (**monday tuesday thursday**, for example). The **to** parameter denotes that you are configuring the schedule's start and end times. Enter the command as follows:

```
(config-schedule-Daily)#periodic monday wednesday friday 17:30 to 18:00
```

The previous periodic schedule is configured to run three days a week (**monday**, **wednesday**, and **friday**) from 5:30 p.m. to 6:00 p.m.

To specify a periodic schedule that occurs on a specific day (or range of days) and begins at a certain time, but runs for a duration of time, you would use the **periodic** *<day>* *<time>* **for** *<time>* command. The **for** parameter denotes that you are configuring the schedule's duration. The duration is entered in the HH:MM format. To create a schedule that runs every Monday, beginning at 6:00 p.m., that runs for two hours, enter the command as follows:

```
(config-schedule-Daily)#periodic monday 18:00 for 02:00
```

Periodic schedules can also be configured to run **daily**, to run Monday through Friday (**weekday**), or to run on the **weekend**. These schedules are created by using the **periodic** [**daily** | **weekday** | **weekend**] *<time>* [**to** | **for**] *<time>* command. Again, the **to** parameter denotes that you are specifying a start and end time for the schedule, and the **for** parameter denotes that you are specifying a duration for the schedule to be active. To create a schedule that runs Monday through Friday, beginning each day at 5:00 a.m. and running for an hour, enter the command as follows:

```
(config-schedule-Daily)#periodic weekday 05:00 for 01:00
```



For more information about schedules, schedule configuration, and how schedules work, refer to the configuration guide [Network Monitoring in AOS](#) (Knowledge Base article 3007).

Creating the Primary and Standby Tracks

The Primary track is the track used to activate the backup path test. The track is associated with both the backup path test schedule and the **Primary-ping** ICMP probe. When the schedule becomes active, the track changes from a FAIL to a PASS state and activates the **Primary-ping** ICMP probe to test the primary path. To configure the Primary (and Standby) track using the CLI, follow these steps:

1. Create and name the track using the **track** *<name>* command from the Global Configuration mode prompt. Enter the command as follows:

```
(config)#track Primary
(config-track-Primary)#
```

2. Associate the track to the backup path test schedule **Daily** using the **time-schedule** *<name>* **fail** command. The *<name>* parameter specifies the name of the schedule you are associating with the track. The **fail** parameter specifies that the track status is FAIL when the schedule is inactive. Enter the command from the track's configuration mode as follows:

```
(config-track-Primary)#time-schedule Daily fail
(config-track-Primary)#
```

3. Associate the appropriate probes with the track and specify the track's testing conditions using the **test if probe** *<name>* command. Using the **test if** command allows you to select one object to be associated with and tested by the track. This command ties the Primary track with the Primary-ping probe, ensuring that the track only acts when the Primary-ping probe changes states. To associate the Primary-ping probe with the Primary track, enter the command as follows:

```
(config-track-Primary)#test if probe Primary-ping
```

4. Unlike probes, tracks are active as soon as they are created. You can manually shut down the track, using the **shutdown** command from the track's configuration mode, which forces the track into a permanent FAIL state. To shut down the track manually, enter the command as follows:

```
(config-track-Primary)#shutdown
(config-track-Primary)#
```



If the track is monitoring a route, the route will be removed if the track is shut down. This could cause network issues if the route is a vital one. If you want to stop the track from monitoring the network, shut down the probes associated with the track, not the track itself.



For more information about tracks, track configuration, and how tracks work, refer to the configuration guide [Network Monitoring in AOS](#) (Knowledge Base article 3007).

5. Create the second track (**Standby**) to monitor the secondary probe (**Standby-ping**) by repeating Steps 1 to 4 and entering the following configuration parameters:

- Track Name: **Standby**
- Associated Probe: **Standby-ping**

The second track (**Standby**) monitors the secondary probe (**Standby-ping**), which tests the backup path. This track changes states based on the state of the **Standby-ping** probe. When the probe is in a PASS state (indicating the backup path is valid), the track is in a PASS state. When the probe is in a FAIL state (indicating the backup path is not valid), the track is in a FAIL state. Various methods, such as Tcl scripts, event logs, and email logs, can be used to report track state changes to you. You should use the reporting method that best matches your network needs.

The **Standby** track configuration should appear as follows:

```
(config)#track Standby
(config-track-Standby)#time-schedule Daily pass
(config-track-Standby)#test if probe Standby-ping
```



Tcl scripts can optionally be associated with the track, which provides you with a method of determining how track changes are reported to you. For more information about configuring and using Tcl scripts, refer to the configuration guide [Tcl Scripting in AOS](#) (Knowledge Base article 2159). Various other methods, such as event and email logs, can also be used to report track state changes to you. You should use the reporting method that best matches your network needs.

Creating PBR Route Maps and ACLs

The PBR route maps and ACLs are used to route the probe traffic. In configuring PBR for the backup path test, you will configure two different maps and two different ACLs. One route map and ACL is used to route the **Standby-ping** probe traffic to the null interface if the backup path is in use. The second route map and ACL is used to route the **Standby-ping** probe traffic to the demand interface to test the backup path. To configure the PBR route maps and ACLs, first create the necessary ACLs and then create the route maps and associate them with the ACLs.

Creating the PBR ACLs

Extended ACLs are used in PBR to match packets that PBR will use as probe traffic for the backup path test call. Extended ACLs allow you to route traffic according to both the source and destination of the traffic. To create an ACL used by PBR for the backup path test, follow these steps:



The ACLs used to route the probe traffic can be configured using the GUI. However, they cannot be applied to the route map using the GUI. If you want to configure the ACLs using the GUI, follow the steps outlined in [Configuring the Demand Interface on page 12](#).

1. Create an extended ACL using the **ip access-list extended** *<name>* command from the Global Configuration mode prompt. This ACL will be used to match the probe traffic from the **Standby-ping** probe. The ACL is named accordingly (**Standby-ping-acl**). Remember that you will need two ACLs for the **Standby-ping** probe, one to match the traffic to the demand interface (to test the backup path), and one to match the traffic to the null interface (when the backup path is in use). Enter the command as follows:

```
(config)#ip access-list extended Standby-ping-acl
Configuring New Extended ACL "Standby-ping-acl"
(config-ext-nacl)#
```

If the ACL name already exists, the command enters the existing ACL's configuration mode. Using the **no** form of this command removes the ACL from the unit's configuration.

2. Next, specify whether the ACL will **permit** or **deny** traffic based on protocol, source information, and destination information. Use the following command to specify this information:

```
[permit | deny] <protocol> <source> <source port> <destination> <destination port> [log]
[track <name>]
```

Permit indicates that traffic matching the criteria is allowed to be used by the feature using the ACL. **Deny** indicates that traffic matching the criteria is not considered by the feature using the ACL.

The *<protocol>* parameter specifies the protocol used by the packet. You can select from **ip**, **icmp**, **tcp**, **udp**, **ahp**, **esp**, **gre** or you can enter a specific protocol. Specific protocol range is **0** to **255**.

The *<source>* parameter specifies the source used for packet matching. Sources can be expressed in one of four ways:

1. Using the keyword **any** to match any IP address.
2. Using **host** *<ip address>* to specify a single host address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
3. Using the *<ip address>* *<wildcard mask>* format to match all IP addresses in a range. The wildcard mask corresponds to a range of IP addresses (network) or a specific host. Wildcard masks are also expressed in dotted decimal notation (for example, **0.0.0.255**) and they work in reverse logic from subnet masks. When broken out into binary form, a **0** indicates which bits of the IP address to consider, and a **1** indicates which bits are disregarded. For example, specifying 255 in any octet of the wildcard mask equates to a “don’t care” for that octet in the IP address. Additionally, a 30-bit mask would be represented with the wildcard string **0.0.0.3**, a 28-bit mask with **0.0.0.15**, a 24-bit mask with **0.0.0.255**, and so forth.
4. Using the keyword **hostname** *<hostname>* to match traffic based on a domain naming system (DNS) name. The unit must be configured with DNS servers for this function to work.

The *<source port>* parameter is optional, and allows you to specify the monitored traffic source port. The source port is used only when the *<protocol>* is specified as **tcp** or **udp**. The following selections are available for specifying source port information:

any matches any port.

eq *<port number/name>* matches only packets equal to a specified port number.

gt *<port number/name>* matches only packets with a port number greater than the specified port number.

lt *<port number/name>* matches only packets with a port number less than the specified number.

neq *<port number/name>* matches only packets that are not equal to the specified port number.

range *<starting port number/name>* *<ending port number/name>* matches only packets that contain a port number in the specified range.

Port numbers are those ports used by Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) to pass information to upper layers and range from **0** to **65535**. All ports below **1024** are considered well-known ports, and are controlled by the Internet Assigned Numbers Authority (IANA). All ports above **1024** are dynamically assigned ports that include registered ports for vendor-specific applications. UDP and TCP ports can also be entered by port name. [Table 1](#) lists the UDP port names and numbers. [Table 2](#) lists the TCP port names and numbers.

Table 1. UDP Port Numbers and Associated Names

biff (Port 512)	bootpc (Port 68)	bootps (Port 67)
discard (Port 9)	dnsix (Port 195)	domain (Port 53)
echo (Port 7)	isakmp (Port 500)	dnsix (Port 195)
nameserver (Port 42)	mobile-ip (Port 434)	netbios-dgm (Port 138)
netbios-ns (Port 137)	netbios-ss (Port 139)	ntp (Port 123)
pim-auto-rp (Port 496)	rip (Port 520)	snmp (Port 161)
snmptrap (Port 162)	sunrpc (Port 111)	syslog (Port 514)
tacacs (Port 49)	talk (Port 517)	tftp (Port 69)
time (Port 37)	who (Port 513)	xdmcp (Port 177)

Table 2. TCP Port Numbers and Associated Names

bgp (Port 179)	chargen (Port 19)	cmd (Port 514)
daytime (Port 13)	discard (Port 9)	domain (Port 53)
echo (Port 7)	exec (Port 512)	finger (Port 79)
ftp (Port 21)	gopher (Port 70)	hostname (Port 101)
ident (Port 113)	irc (Port 194)	klogin (Port 543)
kshell (Port 544)	login (Port 513)	lpd (Port 515)
nntp (Port 119)	pim-auto-rp (Port 496)	pop2 (Port 109)
pop3 (Port 110)	smtp (Port 25)	sunrpc (Port 111)
syslog (Port 514)	tacacs (Port 49)	talk (Port 517)
tftp (Port 69)	telnet (Port 23)	time (Port 37)
uucp (Port 540)	whois (Port 43)	www (Port 80)

The *<destination>* parameter specifies the destination used for packet matching. Destinations can be expressed in the same four ways as the source information.

The *<destination port>* parameter is optional, and allows you to specify the monitored traffic source port. The destination port is also used only when the *<protocol>* is specified as **tcp** or **udp**. The same selections available for source port selection are available for destination port selection.

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 ip access-list** command, which displays the number of times in the last five seconds that an inspected packet has matched the entry.

The optional **track** *<track>* parameter associates the ACL entry with a particular track. This association allows the ACL entry to be applied when a track changes states (from PASS to FAIL or vice versa). The track is configured independently, but the association between the track and ACL entry allows the entry to be disabled or enabled if certain events take place.

For example, to create an extended ACL entry for routing the **Standby-ping** probe traffic to the demand interface, you should specify the following: that the ACL permits ICMP traffic (**icmp**) from any source (**any**), that the ACL permits traffic destined for the backup path (**hostname companyx.net**) using ping traffic (**echo**), and that the ACL is associated with the Primary track (**track Primary**). In addition, the ACL should be configured so that all other traffic is denied. Enter the commands as follows:

```
(config-ext-nacl)#permit icmp any hostname companyx.net echo track Primary
(config-ext-nacl)#deny ip any any
```

These are the basic steps for configuring an extended ACL. You can enter as many criteria as you need to have the ACL monitor traffic for your network. It is important to remember that the order of your entries is crucial: the ACL will match traffic based on criteria from the top down. If the order of the entries is not correct, you will have to remove the applicable ACL entries and then reenter them in the correct order. If a new entry needs to be at the top of the entry list, all the previous entries must be removed. You should also remember that each ACL has an implicit **deny any** as the last criteria if there are other explicit criteria entries within the ACL and each empty ACL has an implicit **permit any** when there are no other explicit criteria entries within the ACL. Once you have configured the ACL, you can use it with the appropriate feature.

3. Repeat Steps 1 and 2 in [Creating PBR Route Maps and ACLs on page 24](#). This time you will create the second ACL that routes the **Standby-ping** probe traffic to the null interface. This ACL is not associated with the Primary track. Configure the ACL as follows from the Global Configuration mode:

```
(config)#ip access-list extended Standby-ping-acl2
Configuring New Extended ACL "Standby-ping-acl2"
(config-ext-nacl)#permit icmp any hostname companyx.net echo
(config-ext-nacl)#deny ip any any
```

Creating the PBR Route Maps

The PBR route maps are used to route the probe traffic to either the demand or null interface, and they use the ACLs to determine which traffic is to be routed. If the traffic matches the configured ACLs, then that traffic is routed according to the route map. As with the ACLs, you will need to create two route maps for the backup path test. The first map routes the traffic to the demand interface (to complete the backup path test), and the second map routes the traffic to the null interface (when the backup path is in use). To create route maps using the CLI, follow these steps:

1. Create a route map entry by entering the **route map <name> permit <number>** command from the Global Configuration mode. The **<name>** parameter is the name of the map. The **permit** parameter applies PBR when the criteria are matched inside the route map. The **<number>** parameter specifies the number of the route entry. Valid range is **1 to 4294967295**. To create the route map, enter the command as follows:

```
(config)#route map LOCAL_POLICY permit 10
(config-route-map)#
```

2. Configure the route map entry's traffic matching criteria using the **match ip address <name>** command from the route map's configuration mode. The **<name>** parameter specifies the name of the ACL used to match traffic for routing. The ACLs created for the PBR portion of the backup path test should be used in both route map entries. To add the ACL that matches the **Standby-ping** probe traffic going to the demand interface (**Standby-ping-acl**) to the route map, enter the command as follows:

```
(config-route-map)#match ip address Standby-ping-acl
(config-route-map)#
```

3. Specify the output interface for the **Standby-ping** probe traffic using the **set interface** *<interface>* command from the route map's configuration mode. This command can specify multiple interfaces. Interfaces should be specified in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a demand interface, use **demand 1**, for a PPP interface, use **ppp 1**.

To specify that the probe packets are sent to the null interface if the demand interface is down, enter the command as follows:

```
(config-route-map)#set interface demand 1 null 0
(config-route-map)#
```

4. Configure the second route map using the **route map** *<name>* **permit** *<number>*, **match ip address** *<name>*, and **set interface** *<interface>* commands. This route map is used to route the **Standby-ping** probe traffic to the null interface and abort the backup path test, and it uses the ACL **Standby-ping-acl2** to match traffic. Configure this route map entry as follows:

```
(config)#route map LOCAL_POLICY permit 11
(config-route-map)#match ip address Standby-ping-acl2
(config-route-map)#set interface null 0
```

5. Once you have configured both ACLs and both route maps, the PBR portion of the backup path test configuration is complete.



For more information about PBR configuration and operation, refer to the configuration guide [Policy Based Routing](#) (Knowledge Base article 2010).

Configuring the Demand Interface

To configure the demand interface for the backup path test, you will need to define interesting traffic for the interface. It is assumed that your demand interface is already configured and operational. If you need assistance configuring the demand interface, refer to the common application guide [Configuring Demand Routing in AOS](#) (Knowledge Base article 2225).

Defining Interesting Traffic

Interesting traffic must be defined for the demand interface by configuring an ACL. When the traffic matching the ACL is detected by the demand interface, it will attempt to connect to the backup path.

Interesting traffic can be specified for inbound or outbound traffic directions. When the demand interface matches interesting outbound traffic, it will attempt to originate a connection and will reset the idle timer on a connected link. When the demand interface matches interesting inbound traffic, it allows the call to remain connected.

Interesting traffic is defined using the **ip access-list extended** *<name>* command. The **ip access-list extended** command is issued from the Global Configuration mode, and creates an empty ACL. The ACL is used in conjunction with the demand interface to determine which traffic is deemed interesting and will cause the demand interface to dial. When the **ip access-list extended** *<name>* command is entered, the extended access control list command set becomes accessible. In the extended access control list command set, specify the action, protocol, source, and destination to be used for the ACL. To enter the extended access control list command set, enter the **ip access-list extended** command as follows:

```
(config)#ip access-list extended BACKUP_CONN_TEST
(config-ext-nacl)#
```

BACKUP_CONN_TEST is an example name, but serves to describe the type of ACL that will be used to activate the demand interface. Once you have access to the extended access control list commands, enter the `<action> <protocol> <source> <destination>` parameters to define traffic to be observed for packet matching purposes. Enter the parameters as follows:

```
(config-ext-nacl)#permit ip any any
```

In creating ACLs for connection purposes, the action will be **permit**, the protocol will be **ip**, the source will be **any**, and the keyword **any** will be specified so that attempted connection to any external IP address will be deemed interesting.



*The **ip access-list extended** command has many uses not always associated with using the demand interface to connect to a backup path. The ACL examples in this configuration guide are specific to using the ACLs for demand interface activation for a backup path test. For more options and configurations of ACLs, refer to the configuration guide [Configuring IP ACLs in AOS](#) (Knowledge Base article 3087).*

Interesting traffic has now been defined, and the demand interface (once configured) will use detection of the specified traffic to attempt to dial the backup network path.

Applying the ACL to the Demand Interface

For the demand interface to begin dialing when interesting traffic is detected, the configured ACL must be applied to the demand interface. To apply the ACL to the demand interface, enter the **match-interesting ip list <name> [in | out]** command from the demand interface configuration mode. The `<name>` parameter is the ACL name, and the optional **in** and **out** parameters specify that either only inbound or outbound traffic is interesting. Enter the command as follows:

```
(config)#interface demand 1
(config-demand 1)#match-interesting ip list BACKUP_CONN_TEST
(config-demand 1)#
```

Configuring SNMP Traps for Network Monitoring Track State Changes (Optional)

SNMP traps can optionally be enabled for network monitoring track state changes using the CLI. Enabling these tracks allows an SNMP trap to be sent whenever the associated track changes states. To configure SNMP traps for track state changes, you must enable the SNMP agent, configure the version of SNMP to use, and enable track traps either on a per-host basis, or for all SNMP monitoring. Lastly, you must add the SNMP trap reporting capability to the network monitoring track. To configure SNMP network monitoring track traps using the CLI, follow these steps:



For more detailed information about the configuration of SNMP, refer to the configuration guide [SNMP in AOS](#) (Knowledge Base article 1134).

1. Enable the SNMP agent by entering the **ip snmp agent** command from the Global Configuration mode prompt. Enter the command as follows:

```
(config)#ip snmp agent
```

2. Specify that SNMP track traps are enabled by either enabling all network monitor traps (using the **snmp-server enable traps track** command from the Global Configuration mode prompt) or by enabling network monitoring traps only for a specified SNMP destination (using the **snmp-server host <ip address> traps version <1 | 2c | 3> <community> track** command from the Global Configuration mode prompt). Using the **no** form of either command disables the SNMP traps for network monitoring. By default, SNMP traps for network monitoring are disabled. To enable all network monitoring SNMP traps, enter the command as follows:

```
(config)#snmp-server enable traps track
```

To enable SNMP traps for network monitoring tracks for a specified host and destination, use the **snmp-server host** command. The *<ip address>* parameter is the destination address that receives the SNMP notifications. Enter IP addresses in the dotted decimal notation (for example, **10.10.10.1**). The **version** parameter of the command specifies the SNMP version and security model used. The *<community>* parameter is the community name used for the SNMP traps. Enter the command as follows:

```
(config)#snmp-server host 10.23.1.181 traps version 1 Public track
```

3. Enable SNMP traps on the tracks you want to monitor using the **snmp trap state-change** command from the track's configuration mode prompt. You will need to enable SNMP traps on both the Primary and Standby tracks for use with the backup path test. Using the **no** form of this command disables SNMP traps on the track. By default, SNMP traps for tracks are disabled. For example, to enable SNMP traps on the **Standby** track, enter the command as follows from the track configuration mode:

```
(config)#track Standby
```

```
(config-track-Standby)#snmp trap state-change
```



For more information about the configuration and use of SNMP, refer to the configuration guide [SNMP in AOS](#) (Knowledge Base article 1134).

Once you have configured the network monitor schedule, probes, and track, the PBR route maps and ACLs, applied the interesting traffic ACL to the demand interface, and optionally enabled SNMP network monitoring traps, the backup path test configuration is complete.

Configuration Examples

The following examples show how to configure network monitoring, PBR, and ACLs for a backup path test. This scenario is provided for example purposes only. Example configurations should be modified to fit your specific configuration needs.

Backup Path Test Configuration

The following example configures the backup path test to be a daily occurrence at **12:00** for **10** minutes. When the schedule is active, the **Primary** track is activated and the **Primary-ping** probe is tracked. In addition, the ACL which allows interesting traffic through the demand interface (**Standby-ping-acl2**), begins the dialing process from the demand interface. If the call connects, the **Standby-ping** probe changes to a PASS state. The **Standby** track also changes to a PASS state. When the schedule time elapses, the schedule returns to an inactive state and the **Primary** track fails. This causes the **Standby-ping-acl** to be removed from the route table, and the **Standby-ping** probe is sent to the null interface. After two consecutive **Standby-ping** probe failures, the probe changes to a FAIL state and the **Standby** track also changes to a FAIL state.

```
!  
probe Primary-ping icmp-echo  
  destination 192.0.2.5  
  period 10  
  tolerance consecutive fail 3  
  no shutdown  
!  
probe Standby-ping icmp-echo  
  destination companyx.net  
  period 60  
  tolerance consecutive fail 2 pass 2  
  no shutdown  
!  
schedule Daily  
  periodic daily 12:00 for 00:10  
!  
track Primary  
  time-schedule Daily fail  
  test if probe Primary-ping  
!  
track Standby  
  test if probe Standby-ping  
!  
ip access-list extended Standby-ping-acl  
  permit icmp any hostname companyx.net echo track Primary  
  deny ip any any  
!  
ip access-list extended Standby-ping-acl2  
  permit icmp any hostname companyx.net echo  
  deny ip any any  
!
```

```

route-map LOCAL_POLICY permit 10
  match ip address Standby-ping-acl
  set interface demand 1 null 0
!
route-map LOCAL_POLICY permit 11
  match ip address Standby-ping-acl2
  set interface null 0
!

```



In order for the demand interface to start the dialing process, the interesting traffic must be defined in an ACL, and the ACL must be applied to the demand interface.



*The output from this test can be received in a number of ways. A mail message or event log can be configured for the **Standby** track to specify the notification types you receive when the track changes states. In addition, you can associate the **Standby** track to the **Daily** schedule and configure it to pass when the schedule is inactive (by entering **time-schedule Daily pass** in the track's configuration). This configuration allows the track to be forced to a passing state while the schedule is inactive. Alternatively, the dampening interval can be set (using the **dampening-interval <value>** command), which ensures that the track does not move to a FAIL state before the dial connection occurs, and allows enough time for the number of probes needed to change to a PASS state are sent. If the dampening interval is changed, allow enough time for the probe periods and the time it takes to dial and connect.*

Backup Path Test Configuration with SNMP Network Monitoring Traps

The following configuration example is based on the same parameters as the preceding example except that it also employs SNMP traps for notification of track state changes. The following configuration includes the SNMP configuration necessary for SNMP trap use with network monitoring and the backup path test.

```

!
ip snmp agent
snmp-server enable traps track
!
probe Primary-ping icmp-echo
  destination 192.0.2.5
  period 10
  tolerance consecutive fail 3
  no shutdown
!
probe Standby-ping icmp-echo
  destination companyx.net
  period 60
  tolerance consecutive fail 2 pass 2
  no shutdown
!

```



```

schedule Daily
  periodic daily 12:00 for 00:10
!
track Primary
  time-schedule Daily fail
  test if probe Primary-ping
  snmp trap state-change
!
track Standby
  test if probe Standby-ping
  snmp trap state-change
!
ip access-list extended Standby-ping-acl
  permit icmp any hostname companyx.net echo track Primary
  deny ip any any
!
ip access-list extended Standby-ping-acl2
  permit icmp any hostname companyx.net echo
  deny ip any any
!
route-map LOCAL_POLICY permit 10
  match ip address Standby-ping-acl
  set interface demand 1 null 0
!
route-map LOCAL_POLICY permit 11
  match ip address Standby-ping-acl2
  set interface null 0
!

```



In order for the demand interface to start the dialing process, the interesting traffic must be defined in an ACL, and the ACL must be applied to the demand interface.



*The output from this test can be received in a number of ways. A mail message or event log can be configured for the **Standby** track to specify the notification types you receive when the track changes states. In addition, you can associate the **Standby** track to the **Daily** schedule and configure it to pass when the schedule is inactive (by entering **time-schedule Daily pass** in the track's configuration). This configuration allows the track to be forced to a passing state while the schedule is inactive. Alternatively, the dampening interval can be set (using the **dampening-interval <value>** command), which ensures that the track does not move to a FAIL state before the dial connection occurs, and allows enough time for the number of probes needed to change to a PASS state are sent. If the dampening interval is changed, allow enough time for the probe periods and the time it takes to dial and connect.*

Configuration Command Summary

The following tables summarize the various configuration commands for each portion of the backup path test configuration. Included in these tables are the configuration commands for probes, tracks, schedules, ACLs, route maps, demand routing, and SNMP as they pertain to the backup path test.

Table 3. ICMP Probe Configuration Command Summary

Prompt	Command	Description
(config)#	probe <name> icmp-echo	Creates an ICMP probe and enters the probe's configuration mode. The <name> parameter is the name of the probe.
(config-probe-<name>)#	destination <ip address hostname>	Specifies the destination of the probe. IP addresses should be expressed in dotted decimal notation (for example, 10.10.10.1). Host names should be fully qualified (for example, www.company.com). For the backup path test, the destination IP address of the ICMP probes should be the IP address of a remote host routed through either the primary or backup Internet connections.
(config-probe-<name>)#	period <value>	Specifies the time (in seconds) between probe test attempts. By default, ICMP probes have a period of 60 seconds. Valid range is 1 to 65535 seconds. For most ICMP probes, the period will need to be reduced to much less than 60 seconds.
(config-probe-<name>)#	tolerance consecutive [pass <number> fail <number>]	Specifies the probe's tolerance. The consecutive keyword indicates that the probe must either pass or fail a certain number of times in a row to change states. Valid range for consecutive passes and failures is 1 to 255 .
(config-probe-<name>)#	no shutdown	Activates the probe. By default, probes are inactive.

Table 4. Schedule Configuration Command Summary

Prompt	Command	Description
(config)#	schedule <name>	Creates a schedule and enters the schedule's configuration mode. The <name> parameter is the name of the schedule.
(config-schedule-<name>)#	periodic <day> <time> [to for] <time>	Specifies that the schedule occurs on a specific day (or range of days) and begins and ends at specific times. The to parameter denotes that you are configuring the schedule's start and end times. The for parameter denotes that you are configuring the schedule's duration. Time is entered in military HH:MM format.
(config-schedule-<name>)#	periodic [daily weekday weekend] <time> [to for] <time>	Specifies that the schedule occurs daily, every weekday, or every weekend. The to parameter denotes that you are configuring the schedule's start and end times. The for parameter denotes that you are configuring the schedule's duration. Time is entered in military HH:MM format.

Table 5. Track Configuration Command Summary

Prompt	Command	Description
(config)#	track <name>	Creates a track and enters the track's configuration mode. The <name> parameter is the name of the track.
(config-track-<name>)#	time-schedule <name> fail	Associates a schedule to the track. The <name> parameter specifies the name of the schedule being associated with the track. The fail parameter specifies that the track's status is FAIL when the schedule is inactive.
(config-track-<name>)#	test if probe <name>	Associates the appropriate probes with the track, thus ensuring that the track only acts when the named probe changes states.

Table 5. Track Configuration Command Summary (Continued)

Prompt	Command	Description
(config-track- <name>)#	shutdown	Shuts down the track. By default, tracks are active as soon as they are created. Using this command forces the track into a permanent FAIL state. If the track is monitoring a route, the route will be removed if the track is shut down. This could cause network issues if the route is a vital one. If you want to stop the track from monitoring the network, shut down the probes associated with the track, not the track itself.

Table 6. ACL Configuration Command Summary

Prompt	Command	Description
(config)#	ip access-list extended <name>	Creates an extended ACL and enters the ACL configuration mode.
(config-ext-nacl)#	[permit deny] <protocol> <source> <source port> <destination> <destination port> [log] [track <name>]	Configures the parameters of an extended ACL. Includes the action, the protocol, source data, source port, destination data, and destination port. Optionally enables logging or optionally associates the ACL with a track. Refer to page 24 for more information.

Table 7. PBR Configuration Command Summary

Prompt	Command	Description
(config)#	route map <name> permit <number>	Creates a route map entry and enters the entry's configuration mode. The <name> parameter is the name of the map, and the permit parameter specifies that PBR is activated when traffic matches the criteria in the configured route map. The <number> parameter specifies the number of the route entry. Valid range is 1 to 4294967295 .
(config-route-map)#	match ip address <name>	Configures the route map's traffic matching criteria. The <name> parameter specifies the name of the ACL used to match traffic for routing.

Table 7. PBR Configuration Command Summary (Continued)

Prompt	Command	Description
(config-route-map)#	set interface <interface>	Specifies the output interface for the Standby-ping probe traffic. This command can specify multiple interfaces. Interfaces should be specified in the format <interface type [slot/port slot/port.subinterface id interface id interface id.subinterface id ap ap/radio ap/radio.vap]>. For example, for a demand interface, use demand 1 , for a PPP interface, use ppp 1 .

Table 8. Demand Interface Configuration Command Summary

Prompt	Command	Description
(config-demand 1)#	match-interesting ip list <name> [in out]	Applies a previously configured ACL to the demand interface to define interesting traffic. The <name> parameter is the ACL name. The in and out parameters are optional, and specify that either only inbound or outbound traffic is interesting.

Table 9. SNMP Configuration Command Summary

Prompt	Command	Description
(config)#	ip snmp agent	Enables the SNMP agent used for SNMP traps.
(config)#	snmp-server host <ip address> traps version <1 2c 3> <community> track	Enables SNMP network monitoring traps for a specified destination. The <ip address> parameter is the destination address that receives SNMP notifications. Enter IP addresses in dotted decimal notation (for example, 10.10.10.1). The <1 2c 3> parameter specifies the security model version used by SNMP. The <community> parameter is the community name used by SNMP. By default, network monitoring SNMP traps are disabled.
(config)#	snmp-server enable traps track	Enables all SNMP network monitoring traps. By default, network monitoring SNMP traps are disabled.

Table 9. SNMP Configuration Command Summary (Continued)

Prompt	Command	Description
(config-track-Primary)#	snmp trap state-change	Enables SNMP traps for the track state change. SNMP traps must be enabled on the track for network monitoring SNMP traps to be used for the backup path test. By default, SNMP traps are disabled on the track.

Additional Resources

Configuring the backup path test relies on the proper configuration of many AOS features and network configurations. The following table outlines additional documentation available for each of the features associated with the backup path test. These documents include configuration information, as well as troubleshooting tips and information.

Table 10. Additional Documentation for Backup Path Test Configuration

Feature	Article Title/Description	Knowledge Base Article Number
ACLs and Access Policies	Configuring Access Policies in AOS Technical Support Note describes the configuration of both ACLs and ACPs and how they work together.	1246
CLI Commands	AOS Command Reference Guide includes documentation of all CLI commands for AOS products.	2219
Demand Interface	Configuring Demand Routing in AOS Common Application Guide describes how to configure the demand interface and how to use ACLs to define interesting traffic for the demand interface.	2225
IP ACLs	IP ACLs in AOS Configuration Guide describes how ACLs are configured and used, as well as how to troubleshoot ACL configurations.	3087
Network Monitoring	Configuring Network Monitor in AOS Configuration Guide describes how to configure, use, and troubleshoot network monitoring.	3007
PBR	Policy Based Routing in AOS Configuration Guide describes how PBR can manipulate traffic paths based on ACL entry matching.	2010
SNMP	SNMP in AOS Configuration Guide describes the use and configuration of SNMP in AOS.	1134
Tcl Scripts	Tcl Scripting in AOS Configuration Guide describes how to configure and use Tcl scripts in AOS.	2159

Table 10. Additional Documentation for Backup Path Test Configuration (Continued)

Feature	Article Title/Description	Knowledge Base Article Number
WAN	<u>WAN Failover Using Network Monitor Common Application Guide</u> describes using ACLs to match ICMP traffic sent from a probe to determine connectivity, and describes how those ACLs can be used to direct traffic to another connection if a route fails.	2305