Configuring IP Load Sharing in AOS – Quick Configuration Guide

ADTRAN Operating System (AOS) includes IP Load Sharing for balancing outbound IP traffic across multiple interfaces. This feature can be used to increase perceived throughput while also providing Layer 3 route redundancy.

Completing this guide requires understanding the topics in the following guides:

- Configuring IP Routing in AOS
- Configuring Access-Lists and Policy-Classes in AOS

Requirements

IP Load Sharing requires each of the following pieces of information, hardware and software. There may be additional requirements for peer devices such as ISP routers.

Information Requirements

- Multiple known routes to a single destination network. This may also be multiple default routes; I.E. multiple Internet connections
  - Destination Network and Subnet Mask for each route
  - Next Hop IP for each route
- Network Address Translation (NAT) Requirements

Software Requirements

- AOS Version 10 and higher Support IP Load Balancing without NAT
- AOS Version 12 and higher support IP Load Balancing with NAT

Hardware Requirements

- 1st Generation NetVanta 3200/3205 do not support AOS 10 or higher
- All other AOS hardware supports AOS 10 or higher

Understanding IP Load Sharing

IP Load Sharing uses multiple routes, with equal administrative distances, to route IP packets to a single destination. These routes may or may not use the same outbound interface. There are two methods of IP Load Sharing: Per-Packet and Per-Destination.

Per-Packet IP Loading Sharing:
Per-Packet load sharing alternates using equal administrative distance routes in round robin fashion. The first packet is sent using the first route, the second using the second route and so-on, repeating first to last.

When the AOS firewall is enabled, Per-Packet sharing is altered to a "Per-Session" fashion to facilitate firewall functionality. This functionality is automatic and requires no extra configuration. Starting with AOS 17.1 the firewall will NAT packets in the same session using the same source address, however they will be routed between the different interfaces in a per packet fashion. This can look like spoofing to an ISP, and will most likely be blocked. If load sharing to two ISPs, per-destination load sharing is suggested instead of per-packet. Per-packet load sharing is best suited for scenarios not involving the firewall (NAT, ALGs, etc), VoIP, or VPN.

Per-Destination IP Load Sharing:
Per-Destination load sharing alternates using the destination IP address in a round robin. All packets with matching destination and source IP addresses will always use the same route. Per-Destination should be used when other firewall devices exist in the path to the destination network. This ensures that all data for a single session will always use the same path, ensuring the other firewall device will be able to maintain proper sessions.

Uni-directional Load Sharing vs Bi-directional Load Sharing:
Uni-directional load sharing means that outbound load sharing is performed but the traffic is not load shared when it comes back to the AOS router. This means that, even if per-packet load sharing is being performed, all the return packets within a session are sent back to the AOS router on a single interface. This is typically the case with load sharing configurations involving the firewall where particular interface addresses are used for NAT on the AOS unit. Even if the outgoing traffic uses a different interfaces (from per-packet load sharing) the return traffic for a particular NAT'ed session will be directed to the address of a specific interface utilizing it more than the other outbound interfaces.

Bi-directional load sharing means that the traffic is load shared when it comes back to the AOS router. To configure bi-directional load sharing, all of the load shared traffic should be given the same source NAT address no matter what interface with which the session is associated. This address should be a publicly routable loopback interface address. The remote unit can then be configured to load share all traffic destined to that address

Load Sharing With the Firewall but Without Source NAT:
When load sharing traffic with the AOS firewall enabled, and the traffic is not being source NAT'ed, inbound traffic may or may not be load shared. This depends on whether or not the user has logged in to the remote unit and configured the remote unit's route table that way. In either case, the load shared outbound traffic should use stateless allow statements in case one of the interfaces goes down. This is to allow the TCP sessions to be able to continue through the unit after being reworked even though the new

association will not be aware of a TCP session ever having been established. For example, if the AOS firewall sees a SYN-ACK without ever having seen a SYN, it would reject the traffic when using stateful inspection.

Load Sharing With VPN:
When load sharing VPN traffic, there should be a different crypto map on each outbound interface. This is because, if the same crypto map is used on the outbound interfaces, then load shared traffic going out different interfaces will all use the same crypto map entry, meaning that they will also use the same peer address. This will break the case in which the load shared traffic is meant to go to different interfaces on the VPN endpoint, each of which will be configured as a different VPN peer. For the same reason described above under "Load Sharing Without Source NAT", the load shared traffic should use stateless allow statements.

Policy Classes on Load Shared Interfaces:
The load shared interfaces must all use the same policy class if the inbound traffic will be load shared by the remote unit (bidirectional load sharing). This is because selectors are associated with policy classes rather than specific interfaces, and so in order for the unit to match the incoming traffic for one flow on multiple interfaces to the same selector, the interfaces must all use the same policy class. The interfaces must also all use the same policy class if a loopback address or fake address is being used for source NAT'ed outbound traffic. Because an actual interface address is not being used as the source NAT address, there is not guarantee of which interface the traffic will return, and therefore the policy class used by both the outgoing and incoming interfaces must be the same.

Analyzing the AOS Firewall for IP Load Sharing

When the IP Firewall in AOS is enabled, special considerations must be taken for IP Load Sharing. Because the firewall applies logic based on communications sessions, the IP Load Sharing feature must not alter the communications session in unexpected ways. Therefore the firewall makes use of a "destination policy-class" feature to differentiate between sessions for appropriate load balancing. It will be important to configure the firewall so that IP Load sharing considerations are handled.

Multiple Different Policy-Classes for Each Public Interface:
Each "Public" or outbound interface must be assigned a different Policy-Class (Security-Zone). This allows the AOS firewall to maintain per-session load sharing appropriately.

Single Policy-Class with Multiple NAT Statements for Private Interface:
The private Policy-Class (Security Zone) must have at least one "Allow" or "NAT" policy for each outbound interface. These "Allow" and "NAT" policies should use the same access-lists (traffic matching parameters) but should each define a different "Destination Policy-Class" (or "Destination Security Zone" in the Web Interface).

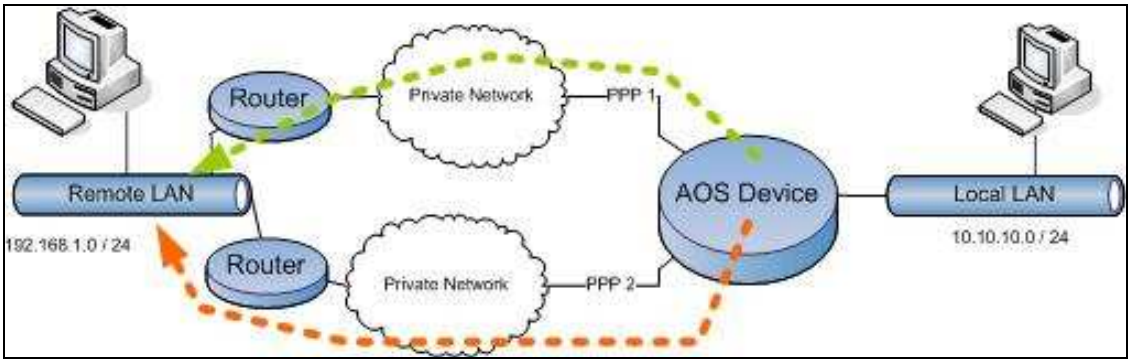
Fast NAT Failover:
Fast-NAT Failover should be used just in case one of the load balanced interfaces goes down. This will ensure that any open sessions involving NAT out the unavailable interface will be terminated properly and allowed to be recreated out the new policy-class. This is accomplished with the global configuration command "ip firewall fast-nat-failover" in the command line interface. For sessions that do not involve NAT but still need to be allowed (like passing public IPs through to an internal interface) the "ip firewall fast-allow-failover" command added in AOS 18.01.01.00 is required. Both of these commands will essentially kill the session open in the firewall and attempt to send a TCP RST to both ends for appropriate sessions when a route table change occurs. In the majority of cases the TCP RST will only make it to internal endpoint because the path to the external endpoint is gone or has changed.

Example IP Load Sharing Scenarios

The following are common example uses of IP Load Sharing.

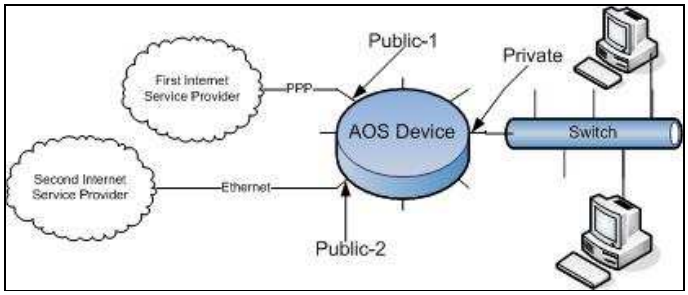
Private WAN Load Sharing:

This example shows multiple IP routes to a single private subnet across a private network. Note that this depicts load sharing only in one direction.



Load Sharing Multiple Internet Access Links:

This example shows multiple internet access links, and identifies the example policy-class names used this guide.



Configuring via the Web Interface

AOS includes a Web Interface that can be used to complete most of the IP Load Sharing configuration tasks. However, ***IP Load Sharing cannot be fully configured via the Web Interface***, and some tasks must be enabled via the Command Line Interface. Consult the section titled "Configuring Via the Command Line Interface" for more information.

Consult the guide titled "Accessing the Web Interface in AOS" for more information about gaining access to the Web Interface in AOS.

Configuring Multiple Routes:

1) Click **Route Table** in the left menu under "Router" to access the Route Table configuration page.

2) Add one route for each available path to the destination network. All "load shared" routes should have the same destination network, destination mask and administrative distance. All "load shared" routes will differ only by their gateway address or interface.

    a. Enter a **Destination Network Address** that identifies the network for which packets will be load shared across multiple routes. This setting will be the same for all load shared routes.

        i. Example: 0.0.0.0 ; for Internet access load sharing
        ii. Example: 192.168.1.0 ; for private access load sharing

    b. Enter a **Destination Subnet Mask** that identifies the subnet mask of the network for which packets will be load shared across multiple routes. This setting will be the same for all load shared routes.

        i. Example: 0.0.0.0 ; for Internet Access load sharing
        ii. Example: 255.255.255.0 ; for private access load sharing

    c. Choose either **Address** or **Interface** based on the method you would like to use to identify the gateway for this route.

    d. For **Address,** enter the gateway IP Address (directly connected device) for the destination network. This will be different for each similarly load shared route.

    e. For **Interface,** choose the outbound interface for the destination network. This will differ for each similarly load shared route.

Note: After enabling IP Load Sharing via the CLI, and completing these steps, IP Load Sharing is now configured. If the AOS firewall will not be enabled, you have completed this guide.

Note: If the AOS Firewall is or will be enabled, continue reading.

Creating Security Zones:

3) Click **Security Zones** in the left menu, under "Firewall".

4) Create one Security Zone for each outbound interface and one for all private interfaces. You may re-use Security Zones that already exist.

a. Click **“<click to add a Security Zone>”** to create a new Security Zone.

b. Enter a **Name** for the Security Zone.

   i. Example: Public-1
   ii. Example: Public-2
   iii. Example: Private

c. Click **Apply**.

d. Click **Security Zones** in the left menu under “Firewall” to return to the Security Zones configuration page to add additional Security Zones.

Creating NAT Policies for Private Security Zone:

5) Click **Security Zones** in the left menu, under “Firewall”.

6) Click on the “**Private**” Security Zone you created for your private interfaces.

7) Add one NAT policy for each outbound interface that requires NAT. Usually only interfaces that connect to the Internet require NAT. All “NAT” policies for the same Load Sharing set should use the same “Source” and “Destination” data settings.

   a. Click “**Add Policy to Zone…”**

   b. Select **Advanced** to add a NAT with specific Destination Security Zone.

   c. Click **Continue**.

   d. Enter a **Policy Description** such as “NAT to Public-1”.

   e. Select **NAT** as the **Policy Action.**

   f. Select a **Destination Security Zone**. This should be the Security Zone that is associated with the intended outbound interface.

      i. Example: “Public-1”
      ii. Example: “Public-2”

   g. Select “**Source with Overloading”** as the **NAT Type**.

h. Choose either a **Specified Address** or choose an **Interface** that will be used for the Source NAT. This should be either the interface or IP address of the outbound interface that will be associated with the *Destination Security Zone*.

i. Click **Apply** to move onto Traffic Selection for this Policy.

j. Scroll to the bottom, and click "**Add New Traffic Selector…**"

Creating a Traffic Selector for NAT:

k. Choose **Permit** as the **Filter Type** .

l. Choose **Any** as the **Protocol**.

m. Under "Source Data," choose either **Any** or **IP Address** for the **Source Host/Network**.

    i. Choose **Any** to allow any source network behind the private interface to use this NAT.

    ii. Choose **IP Address** to restrict the use of this NAT to a specific source network behind the private interface.

        1. Example Address: 10.10.10.0
        2. Example Mask: 255.255.255.0

n. Under "Destination Data", choose either **Any** or **IP Address** for the **Destination Host/Network**.

    i. Choose **Any** to allow access to any network ("Internet") using this NAT.

    ii. Choose **IP Address** to restrict the use of this NAT to a specific destination network across the destination security zone.

        1. Example Address: 192.168.1.0
        2. Example Mask: 255.255.255.0

o. Click **Apply**.

p. Return to step 5 of this series to add additional NAT policies, one for each outbound interface that requires NAT.

Creating "Allow" Policies for Private Security Zone:

8) Click **Security Zones** in the left menu, under "Firewall."

9) Click on the "**Private**" security zone you created for your private interfaces.

10) Add one "Allow" policy for each outbound interface that does not require NAT; usually private connections. All "Allow" policies for the same Load Sharing set should use the same "Source" and "Destination" data settings.

    a. Click "**Add Policy to Zone…"**

    b. Choose a Policy Type of "**Allow**"

    c. Click **Continue.**

    d. Enter a **Policy Name** such as "Allow for Public-1".

    e. Optionally, enable **"Stateless Processing"** to reduce compatibility issues with some persistent connection applications.

    f. Select a **Destination Security Zone**. This should be the Security Zone that is associated with the intended outbound interface.

        i. Example: "Public-1"
        ii. Example: "Public-2"

    g. Under "Source Data," choose either **Any** or **IP Address** for the **Source Host/Network**.

        i. Choose **Any** to allow any source network behind the private interface to use this NAT.

        ii. Choose **IP Address** to restrict the use of this NAT to a specific source network behind the private interface.

            1. Example Address: 10.10.10.0
            2. Example Mask: 255.255.255.0

    h. Under "Destination Data", choose either **Any** or **IP Address** for the **Destination Host/Network**.

        i. Choose **Any** to allow access to any network using the intended outbound interface.

ii. Choose **IP Address** to restrict the use of this NAT to a specific destination network across the destination security zone.

1. Example Address: 192.168.1.0
2. Example Mask: 255.255.255.0

i. Choose **Any** for the **Protocol**.

j. Click **Apply**.

k. Return to step 8 of this series to add an additional allow policy for each outbound interface that requires an "Allow."

Assigning Interfaces to Security Zones:

11) Click **Security Zones** in the left menu, under "Firewall."

12) Apply each interface to a Security Zone created above.

a. From the select box for each interface, choose the appropriate Security Zone. These selections correspond with the "Destination Security Zone" made for each "Private" Security Zone policy created above.

b. Example: PPP 1 might be assigned the Security Zone "Public-1".

c. Example: Eth 0/1 (LAN) might be assigned Security Zone "Private"

13) Click **Apply** to assign Interfaces to each Security Zone.

Enabling the AOS Firewall:

Note: These steps will enable the AOS firewall. If you have a not created policies that allow your own administrative access, you will lose connectivity.

14) Click **General Firewall** in the left menu, under "Firewall".

15) Check the **Enable** check box.

16) Click **Apply**.

Saving Configuration Changes

Note: Saving your configuration changes is **important**! If you do not save these changes, they will be lost on the next reboot or power cycle.

17) Click **Save** in the upper right corner.

Configuring via the Command Line Interface

AOS includes a Command Line Interface that can be used to completely configure IP Load Sharing, and is the only method to enable the IP Load Sharing feature; routes and firewall settings can be made in the Web Interface.

Fore more information about accessing the Command Line Interface, consult the guide titled "Accessing the Command Line Interface."

Accessing Global Configuration Mode:

1) Type **enable** to gain access to Privileged Exec Mode.

    a. Enter your *enable password* if prompted.
    b. By default the *enable password* is the word 'password'.
    c. If you do not know the password, consult the guide titled "Password Recovery in AOS."

2) Type **configure terminal** to access Global Configuration Mode.

Enabling IP Load Sharing

3) Enable either Per-Packet or Per-Destination IP Load Sharing. Consult the section titled "Understanding IP Load Sharing" for more information.

    a. Syntax: *ip load-sharing < [per-packet] | [per-destination]>*
    b. Example: **ip load-sharing per-packet**
    c. Example: **ip load-sharing per-destination**

Note: IP Load Sharing is now enabled, and you may either return to the Web Interface or continue reading to configure routes and firewall policies.

Configuring Multiple Routes:

4) Add multiple routes, with the same destination network, destination subnet mask and administrative distance. Each route should have a different outbound interface or gateway. These routes could also be learned via routing protocols such as RIP, OSPF or BGP.

    a. Syntax: *ip route <destination> <mask> < [interface] | [gateway]>*

    Default ("Internet Access") Route Examples:
    b. Example*:* **ip route 0.0.0.0 0.0.0.0 ppp 1**

c. Example: **ip route 0.0.0.0 0.0.0.0 5.5.5.5**

Private Route Examples:
d. Example: **ip route 192.168.1.0 255.255.255.0 ppp 1**
e. Example: **ip route 192.168.1.0 255.255.255.0 5.5.5.5**

Note: If the AOS firewall will not be enabled, IP Load Sharing is complete, and you should not continue.

Note: If the AOS firewall is or will be enabled, you should read the section titled "Analyzing the AOS Firewall for IP Load Sharing Considerations" and continue.

Creating an Access-List for Traffic Matching:

5) Create an Extended Access-List that will identify traffic destined for the network that has multiple routes.

   a. Syntax: *ip access-list extended <name>*
   b. Example: **ip access-list extended TRAFFIC**

6) Add a "permit" statement that identifies traffic destined to the destination network referenced in your route statements.

   a. Syntax: *permit ip <source-network> <source-mask> <destination-network> <desitnation-mask>*

   Example for Default Routes::
   b. Example: **permit ip any any**

   Example for Specific Network:
   c. Example: **permit ip any 192.168.1.0 0.0.0.255**

Creating Policy-Classes:

7) Create one policy-class for each public interface and only one policy-class for the private interfaces. Consult the section titled "Analyzing the AOS Firewall for IP Load Sharing" for important information.

   a. Syntax: *ip policy-class <name>*
   b. Example: **ip policy-class Public-1**
   c. Example: **ip policy-class Public-2**
   d. Example: **ip policy-class Private**

Creating Private Policies:

Note: You only need to create one NAT or "Allow" policy for each outbound interface. There must be at least one policy of either type for each outbound interface ("Destination Policy-Class").

8) Create multiple NAT policies as necessary. Create one policy for each outbound interface that requires NA.T. Usually when connected to an ISP.

    a. Syntax: *nat source list <ACL-name> <address [ip-address] | interface [interface]> overload policy <destination-policy-class>*

    Examples using "Interface" option:
    b. **nat source list TRAFFIC interface ppp 1 overload policy Public-1**
    c. **nat source list TRAFFIC interface hdlc 1 overload policy Public-2**

    Examples using "Address" option:
    d. **nat source list TRAFFIC address 5.5.5.5 overload policy Public-1**
    e. **nat source list TRAFFIC address 6.6.6.6 overload policy Public-2**

9) Create multiple "Allow" policies as necessary. Create one "Allow" policy for each outbound interface that requires an allow, usually for private connections.

    a. Syntax: *allow list <name> policy <policy-name>*
    b. Example: **allow list TRAFFIC policy Public-1**
    c. Example: **allow list TRAFFIC policy Public-2**

10) Type **exit** to return to Global Configuration Mode.

Applying Policy-Classes to Interfaces:

11) Apply each policy class to its respective interface. From the examples above, the policy-class "Public-1" would be applied to PPP 1 or the interface with the IP Address 5.5.5.5, and the policy-class "Private" might be applied to "eth 0/1"

    Gaining Access to Interface Configuration Mode:
    a. Syntax: *interface <name> <number>*
    b. Example: **interface ppp 1**
    c. Example: **interface eth 0/1**

    Applying the Policy-Class to the Interface:
    d. Syntax: *access-policy <policy-name>*
    e. Example: **access-policy Public-1**

f. Example: **access-policy Public-2**
g. Example: **access-policy Private**

12) Type **exit** to return to Global Configuration Mode.

Enabling the Firewall:

Note: This step enables the AOS firewall, and if you have not made a specific policy in your policy-classes that allows your administrative access (not covered in this guide), you will lose connectivity to your AOS device.

13) Enable the AOS firewall, to begin using the "Allow" and "NAT" policies previously created.

    a. Syntax: ***ip firewall***

Note: IP Load Sharing is now configured and the AOS Firewall is properly configured and enabled.

Saving Configuration Changes

14) Return to Privileged Exec Mode.

    a. Syntax: ***end***

15) Write configuration changes to permanent storage

    a. Syntax: ***write***

Example Configurations

These example configurations correspond to the scenarios at the beginning of this guide. You should not use these configurations verbatim. You should evaluate your own network and apply the concepts detailed in this guide as needed.

For brevity, these are not complete configurations, but do include all IP Load Sharing configuration requirements. Your application may require additional configuration.

Simple IP Load Sharing – To Private Network, No Firewall:

This example shows a simple load sharing scenario for use with private WAN connections where the AOS firewall is not enabled. This example would load share IP packets over PPP 1 and PPP 2 to the remote 192.168.1.0/24 network.

```
!
no  ip  firewall
ip  load-sharing  per-packet
!
interface eth 0/1
        description Private LAN Connection
        ip address  10.10.10.1  255.255.255.0
        no shutdown
!
interface ppp 1
        description First WAN Connection
        ip address  172.16.0.1  255.255.255.252
        no shutdown
!
interface ppp 2
        description Second WAN Connection
        ip address  172.16.0.5  255.255.255.252
        no shutdown
!
!
! Route using  "First WAN Connection"
ip route 192.168.1.0  255.255.255.0   ppp 1
!
! Route using  "Second WAN Connection"
ip route 192.168.1.0  255.255.255.0   ppp 2
!
```

Dual Redundant Internet Access IP Load Sharing

This example shows load sharing across two Internet connections that require NAT.

Make note of the two NAT policies in the Private Policy class, and their corresponding Public policies. Note that the NAT statements use the "interface" option for ease.

The example also shows two default routes (one using the "interface" option and the other using the "address" option for a subnet that is connected via Ethernet). Because of the multi-access nature of Ethernet, the "interface" option does not include Ethernet; there would be no way to determine the next-hop gateway.

```
!
ip firewall
ip load-sharing per-destination
!
interface eth 0/1
        description Private LAN Connection
        ip address 10.10.10.1  255.255.255.0
        access-policy Private
        no shutdown
!
interface eth 0/2
        description First Public Internet Connection (External ADSL or Cable Modem)
```

```
        ip address 5.5.5.5  255.255.255.252
        access-policy Public-1
        no shutdown
!
interface ppp 1
        description Second Public Internet Connection
        ip address negotiated
        access-policy Public-2
        no shutdown
!
!
! Default route for Ethernet 0/2 Internet Connection
ip route 0.0.0.0  0.0.0.0  5.5.5.6
!
! Default route for PPP Internet Connection
ip route 0.0.0.0  0.0.0.0  ppp 1
!
!
ip access-list extended TRAFFIC
        remark match only local LAN to any destination (Internet)
        permit  ip  10.10.10.0  0.0.0.255   any
!
ip policy-class Private
        nat source list TRAFFIC interface eth 0/2 overload policy Public-1
        nat source list TRAFFIC interface ppp 1 overload policy Public-2
!
ip policy-class Public-1
!(implicit discard)
!
ip policy-class Public-2
! (implicit discard)
```

Dual Redundant Internet Access using a Switch/Router Product:

Note that this is the same as above, simply using a VLAN interface as the routed interface, instead of an Ethernet interface. 1000 Series Switch/Router products use VLAN interfaces as routed interfaces, and Ethernet ports are simply switched access.

```
!
ip firewall
ip load-sharing per-destination
!
interface VLAN 1
        description Private LAN Connection
        ip address 10.10.10.1  255.255.255.0
        access-policy Private
        no shutdown
!
interface VLAN 2
        description First Public Internet Connection (External ADSL or Cable Modem)
        ip address 5.5.5.5  255.255.255.252
        access-policy Public-1
        no shutdown
!
interface ppp 1
```

```
        description Second Public Internet Connection (T1 to ISP)
        ip address negotiated
        access-policy Public-2
        no shutdown
!
!
! Default route for VLAN 2 Internet Connection
ip route 0.0.0.0  0.0.0.0  5.5.5.6
!
! Default route for PPP Internet Connection
ip route 0.0.0.0  0.0.0.0  ppp 1
!
!
ip access-list extended TRAFFIC
        remark match only local LAN to any destination (Internet)
        permit  ip  10.10.10.0  0.0.0.255   any
!
ip policy-class Private
        nat source list TRAFFIC interface vlan 2 overload policy Public-1
        nat source list TRAFFIC interface ppp 1 overload policy Public-2
!
ip policy-class Public-1
!(implicit discard)
!
ip policy-class Public-2
! (implicit discard)
```

Troubleshooting

IP Load Sharing simply lists two routes to the same destination network, instead of the normal one route. Be sure that all outbound interfaces have an "UP" status, and then check the output of **show ip route** to ensure that multiple routes exist to the destination.

Example Multiple Specific Private Network Route Output:

The output of **show ip route** for load shared routes to a specific network are highlighted in bold below. This output corresponds to the example configuration above.

Example "show ip route" Output:

```
Gateway of last resort is 10.10.10.254 to network 0.0.0.0

S    0.0.0.0/0 [1/0] via 10.10.10.254, eth 0/1
C    10.10.10.0/24 is directly connected, eth 0/1
C    172.16.0.0/30 is directly connected, ppp 1
C    172.16.0.4/30 is directly connected, ppp 2
S    192.168.1.0/24 [1/0] via 172.16.0.2, ppp 1
                    [1/0] via 172.16.0.6, ppp 2
```

Example Multiple Default (Internet) Route Output:

The output of **show ip route** for load shared default routes shows multiple 0.0.0.0 routes to different gateways. The "gateway of last resort" statement will list the first available route and will not show the second route. The second default route is visible under the "0.0.0.0" entry.

Example "show ip route" Output:
Gateway of last resort is 5.5.5.6 to network 0.0.0.0

S 0.0.0.0/0 [1/0] via 5.5.5.6, eth 0/1.1
[1/0] via 6.6.6.6, eth 0/1.2
C 5.5.5.4/30 is directly connected, eth 0/2
C 6.6.6.4/30 is directly connected, ppp 2
C 10.10.10.0/24 is directly connected, eth 0/1

Evaluating Firewall Session Associations:

When the AOS firewall is enabled, you can use the output of **show ip policy-sessions** or the "Active Sessions" table in the "Security Zones" section of the Web Interface, to view which sessions are using which NAT statements.

The following is an example output that shows ICMP (ping) traffic destined for 7.7.7.7 being NATed to 5.5.5.5, and ICMP (ping) traffic destined for 8.8.8.8 being NATed to 6.6.6.5. These were load shared across two default routes, one using the example "PPP 1" connection and the other using the example "Eth 0/2" connection.

Protocol	Source Address/Port	Destination Address/Port	Nat Address/Port
ICMP(1)	10.10.105	7.7.7.7	5.5.5.5
ICMP(1)	10.10.10.5	7.7.7.8	6.6.6.5