Technical Guide

High Availability

Feature Overview and Configuration Guide

Introduction

This guide describes the operation of High Availability (HA) on Allied Telesis security appliances, and how to configure and monitor it. The HA capability in the security appliances consists of a combination of the Virtual Router Redundancy Protocol (VRRP) and a physical WAN relay.

Products and software version that apply to this guide

This guide applies to AlliedWare Plus™ products that support HA, running version **5.4.5** or later.

Version 5.4.6-2.x introduces firewall control for VRRPv4 packets received by the device. High Availability (HA) uses VRRP, so if you have the firewall enabled, you need to configure it to allow IPv4 VRRP packets. See "Firewall control for VRRP and High Availability" on page 10 for an example of the configuration to create.

Version 5.5.0-1.x introduces the ability to manually enable and disable the Bypass. See "Manual control of the bypass port" on page 11 for more information.

To see whether your product supports HA, see the following documents:

- The product's Datasheet
- The product's Command Reference

These documents are available from the above links on our website at alliedtelesis.com.

Feature support may change in later software versions. For the latest information, see the above documents.

Content

Designing for High Availability

Organizations are increasingly reliant on their data networks. Network outages can be costly, so designing networks for HA is important. A key element to HA design is to duplicate critical components or functions.

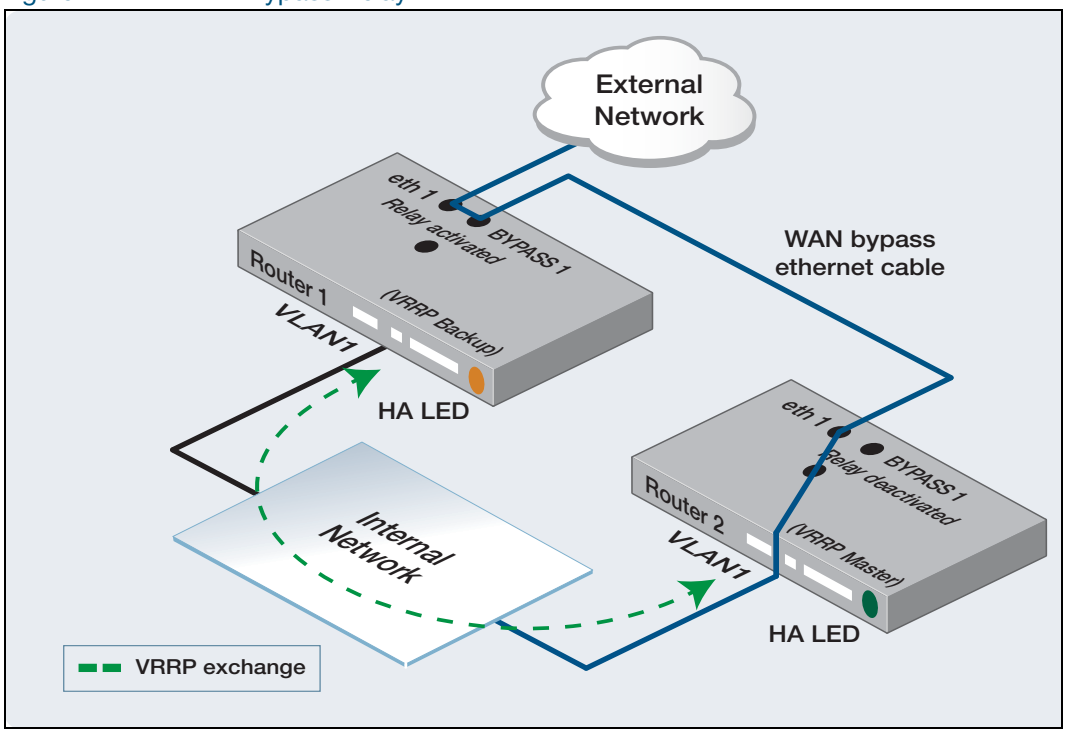
HA can be achieved in many ways that can be used separately or in combination. For example you can achieve HA by:

- Deploying multiple redundant devices into a network so that if one fails, one or more of the other devices can take over and provide the services and functions of the failed device. This can require that specific protocols be implemented on the devices involved, such as VRRP.
- Deploying multiple redundant links in a network so that if one link fails, the remaining links can continue to provide connectivity (possibly at a reduced capacity), such as WAN redundancy.

High Availability on security appliances

Security appliances provide an HA solution that combines VRRP with an internal relay switch (called the Bypass Relay) that creates a direct physical connection between a unit's WAN port and an accompanying bypass port. The following figure shows the operation of a pair of devices, one connected to the Internet, and each connected to a LAN switch. The WAN port of one device is connected to the bypass port of the other. VRRP is operating between the two devices.

Figure 1: VRRP with Bypass Relay

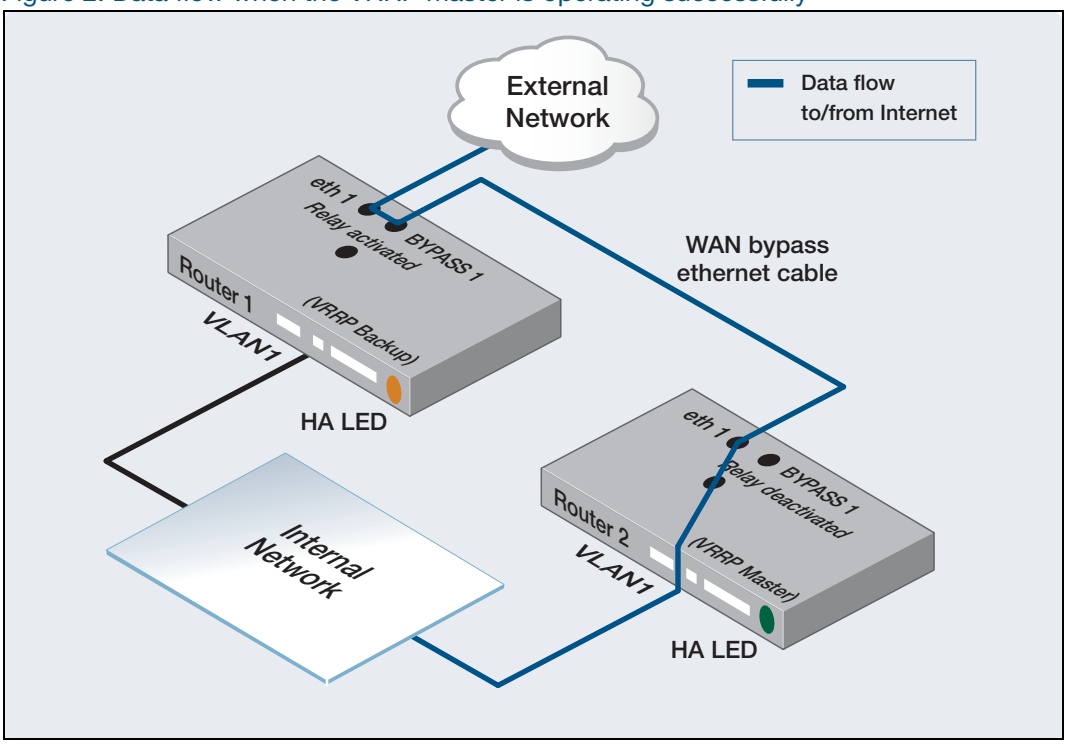


The two devices operate as a VRRP Master and Backup. The device on the right is the VRRP Master, as indicated by the label in the diagram. You can see that the WAN port of this device is not connected directly to the Internet, but is connected to the bypass port of the VRRP backup unit. When a unit is operating as a VRRP backup (and has been configured to also control the Bypass Relay), it activates the Bypass Relay so that the data pins of the backup port are directly connected to the data pins of the WAN port.

Data that exits via the WAN port of the VRRP Master is transported to the bypass port of the backup unit and then to its WAN port, and onwards out to the Internet. The transmission of data through the bypass and WAN ports of the VRRP backup unit is performed purely by physical connection, there is no software involvement in that transmission. So, the WAN and bypass ports of the VRRP backup operate purely as passive pieces of conducting copper wires in this case. The Internet connection is thereby connected to the WAN port of the right-hand device.

When the VRRP Master is operating successfully, data from the LAN is routed by the device out through its WAN port, and out to the Internet via the connection through the bypass and WAN ports of the VRRP backup. Similarly, data from the Internet arrives at the master's WAN port via the connection through the VRRP backup's WAN and bypass ports, to be routed out through the master's LAN port.

Figure 2: Data flow when the VRRP master is operating successfully

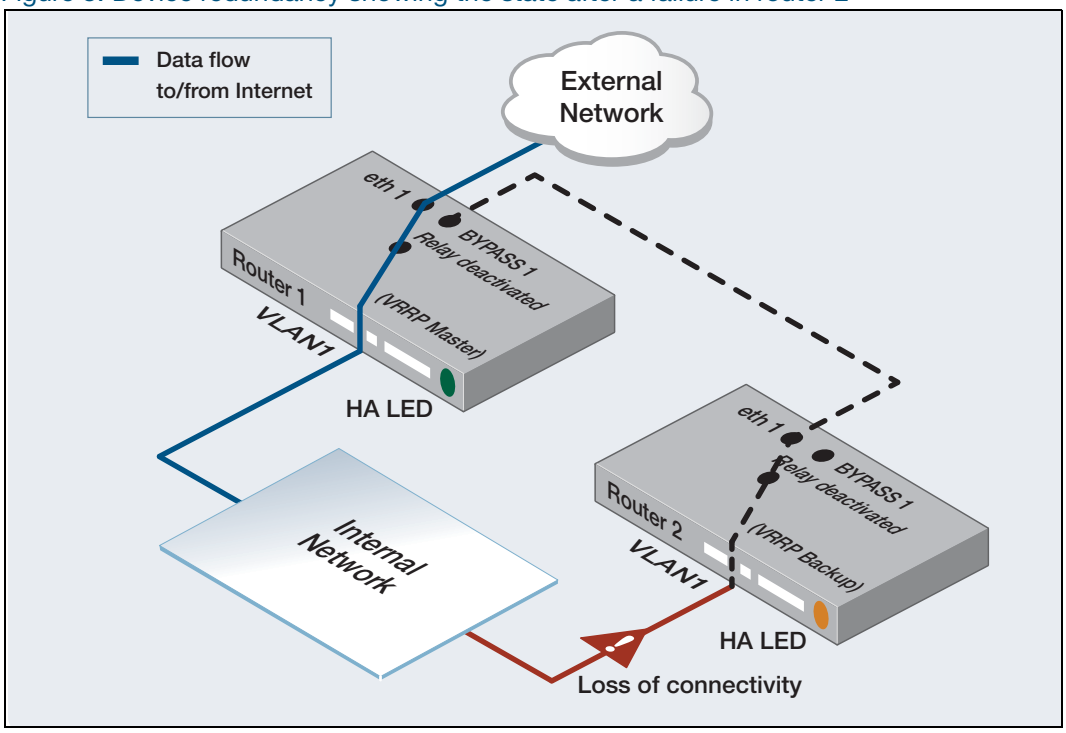


If the VRRP Master fails, the following happens:

- It will no longer transmit VRRP keepalives, so the other device will soon transition to the VRRP Master.
- Upon transitioning to the VRRP Master, the left-hand device will deactivate its Bypass Relay, so the Data Pins in its WAN ports will no longer be directly connected to the Data Pins in its backup port. With the Bypass Relay deactivated in the left-hand device, its WAN port will instead now be connected to the internal LAN port connection.

Therefore, data from the LAN will be routed by the device on the left to the Internet, because it is now the VRRP Master. It will route the data to its WAN port. Similarly, data from the Internet will arrive at the WAN port of the left-hand device, and be routed out through its LAN port. The data flows are illustrated in the following figure:

Figure 3: Device redundancy showing the state after a failure in router 2



WAN Bypass Relay behavior

Because the Bypass Relays are the main component of the secure HA solution, this section describes their behavior in more detail.

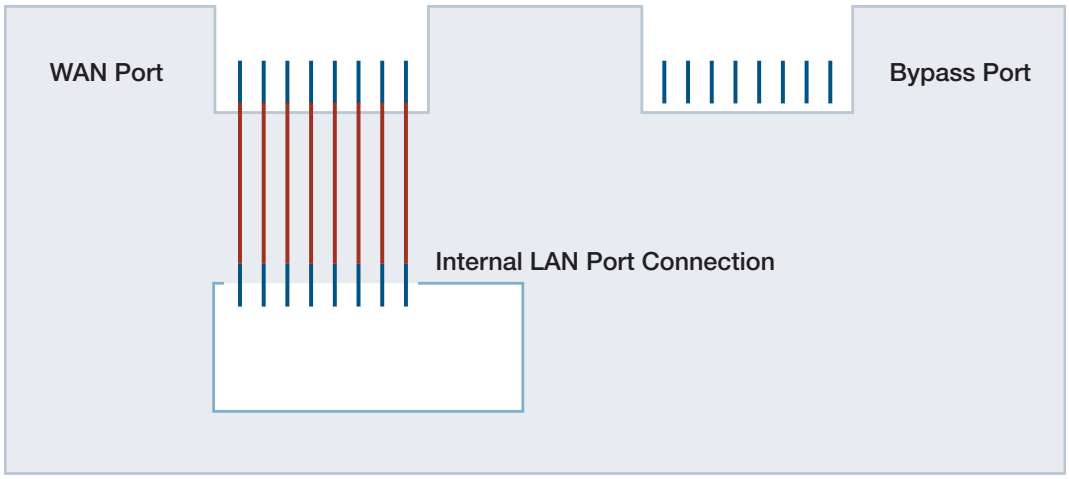
Relays in a deactivated state

On the secure device, a Bypass Relay will be in a deactivated state when:

- The device is powered up, and the system software has loaded, placing the relay under software control.
- No HA functionality is configured, or
- An HA VRRP instance is configured without enabling relay control.
- An HA VRRP instance has been configured, with relay control enabled, and the device is the VRRP master.

When the relay is in a deactivated state, the WAN port associated with that relay is internally connected to the device's VLAN switch ports, and internally disconnected from the bypass port. Therefore, data flows directly between the internal LAN port connection and the external WAN port as shown in the following figure.

Figure 4: WAN Bypass Relay deactivated



When no HA functionality is configured the default behavior of the WAN Bypass Relay is to be in a deactivated state, as the system software boots. The Bypass Relay remains deactivated after the software boot. For example, when there is no HA-Mode VRRP instance configured on the device, but the device is powered up and running.

Therefore by default, if the device is running normally, but without HA functionality configured, then the default behavior of the relay is to be deactivated. This allows internal LAN to external WAN communications to occur.

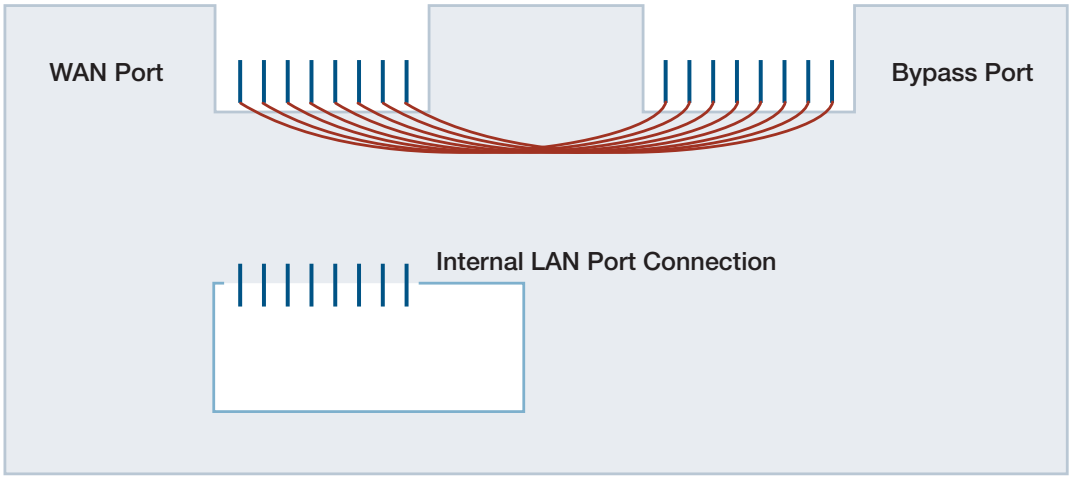
Relays in an activated state

On the security device, a Bypass Relay will be in an activated state when:

- The device has no power, or
- An HA VRRP instance is configured to control the Bypass Relays, and the device is in a VRRP backup state.

When the relay is in an activated state, the WAN port associated with that relay is internally disconnected from the device's VLAN switch ports, and internally connected to the relevant bypass port. Therefore, data flows between the external WAN port and the bypass port, as shown in the following figure:

Figure 5: WAN Bypass Relay activated



Each Bypass Relay on the security device is activated when the device loses power, or when the front-panel reset button is pressed.

Configuring High Availability

VRRP is the function that controls the Bypass Relays on the security device.

- Each Bypass Relay can be controlled by only one VRRP instance.
- When a VRRP instance is configured to control a Bypass Relay, that VRRP instance is then considered to be an HA-Mode VRRP instance.
- Each HA-Mode VRRP instance is operationally identical to a standard VRRP instance except where explicitly stated in this document. Standard VRRP instances can operate side-by-side, and independently of, HA-Mode VRRP instances on the same device.
- A single HA-Mode VRRP instance can be configured to control either one Bypass Relay, or both Bypass Relays on devices that have more than one relay.
- Whenever an HA-Mode VRRP instance is in Master state, it will deactivate all the Bypass Relays it controls.
- Whenever an HA-Mode VRRP instance is in Backup or Init state, it will activate all the Bypass Relays it controls.

The following table shows how to create a VRRP instance and then associate it with a Bypass port.

Table 1: How to create a VRRP instance and then associate it with a Bypass port

Creating a VRRP instance and associating it with a Bypass port	
`awplus#` `configure terminal`	Enter Configuration mode.
`awplus(config)#` `router vrrp <vrid> <interface>`	Enter the virtual router ID to create a VRRP session and associate it with a VLAN interface.
`awplus(config-router)#` `ha associate`	Enter the **ha associate** command to configure the device for the specified VRRP session into HA-Mode so that it can control the HA LED.
`awplus(config-router)#` `ha associate [wan-bypass <1-2>]`	Enter the Bypass Relay ID to bond the control Bypass Relay to a specified VRRP session. ■ WAN-Bypass Relay 1 is used to bypass eth1 interface. ■ WAN-Bypass Relay 2 is used to bypass eth2 interface. If the optional **wan-bypass <1-2>** parameter is not configured, then the WAN-Bypass Relay is not associated with the VRRP session, so only the LED is controlled, not the relay.

LED behavior with High Availability

WAN port LEDs

- These LEDs operate as normal WAN port status, when their corresponding WAN Bypass Relay is in the deactivated state.
- They operate as if the WAN link has gone down, when their corresponding WAN Bypass Relay is in the activated state.

High Availability LEDs

The behavior of the HA LED is dependent on the states of the HA-Mode VRRP sessions.

Table 2: HA LED display descriptions

HA LED DISPLAY	DESCRIPTION
Off	When there are no HA-Mode VRRP sessions configured on a device.
Flashing amber	When an HA-Mode VRRP session is in the initial state (administratively disabled or the VRRP link is down), or when an HA-Mode VRRP session is in the backup state after having failed over from the master state.
Steady green	When an HA-Mode VRRP session on that device is in the master state.
Steady amber	When an HA-Mode VRRP session on that device is in the backup state and no failover has occurred.

Given that there is only one HA LED on the device, there needs to be a rule governing what state the LED is in when the device is configured with multiple VRRP instances that are in different states. The rule is that the VRRP state instances are assigned priority values, as described in the following table.

Table 3: VRRP HA-Mode instance states

PRIORITY	VRRP HA-MODE INSTANCE STATE
1	Initialization (Administratively disabled or VRRP VLAN link down).
2	Init This state can occur when an HA-Mode VRRP session is in the init state (Administratively disabled or VRRP backup has changed from master) (a failover event)).
3	Master (Irrespective of previous state).
4	Configured backup.

The VRRP instance that has the lowest priority value governs the state of the LED. If there is any VRRP instance in the Init state the LED will flash amber. If there are no VRRP instances in Init state, but one is in Master state, then the LED will be a steady green, and so on.

WAN ports with combo SFP sockets

HA VRRP functionality is only relevant to the RJ45 copper Ethernet WAN port.

Combo SFP sockets cannot be used. If an SFP is plugged into a combo port that is associated with an HA-Mode VRRP instance controlled bypass port, then it will be administratively disabled. The user will be notified with a log message.

After the SFP is removed, the HA-Mode VRRP instance will become enabled again. The user will be notified with a log message.

SFP(s) are electrically independent of the Bypass Relays and so cannot be controlled by them.

Firewall control for VRRP and High Availability

Version 5.4.6-2.x adds firewall control for IPv4 VRRP packets received by the security device.

This means that if you have the firewall enabled, you need to configure the firewall to allow IPv4 VRRP packets. The firewall configuration needs to permit packets to IP subnet 224.0.0.18/32, which is the VRRP multicast address. You can limit the configuration so that it only applies to the VRRP application (protocol 112).

For example, if the firewall is enabled, and VRRP is configured on VLAN1, and VLAN1 has an IP address in the 172.20.10.0/24 subnet, the following configuration will allow VRRP packets to be received:

```
application vrrp
 protocol 112

zone private
 network vlan1
  ip subnet 172.20.10.0/24 interface vlan1
 network vrrp_subnet
  ip subnet 224.0.0.18/32

firewall
 rule 10 permit vrrp from private.vlan1 to private.vrrp_subnet
 protect
```

Note that the device only controls incoming VRRP packets. During normal device operation, outgoing VRRP packets are not processed by the device. They will be sent regardless of the device configuration.

Manual control of the bypass port

Version 5.5.0-1.x adds the ability to manually activate and deactivate the Bypass port.

By default, when the router is running, the Bypass port is deactivated. When the router is powered down, the Bypass port is activated. The Bypass port can also be managed automatically by VRRP, as described above.

If the Bypass port is not being managed by VRRP, it is possible to activate and deactivate it manually from the CLI. The **wan-bypass** command lets you activate the Bypass port, while the **no wan-bypass** command lets you deactivate it.

Table 4: How to manually activate and deactivate the Bypass port

Manually activating and deactivating the Bypass port	
`awplus#` `configure terminal`	Enter Configuration mode.
`awplus(config)#` `interface eth1`	Enter the WAN interface.
`awplus(config-if)#` `wan-bypass`	Enter the **wan-bypass** command to activate the Bypass port.
`awplus(config-if)#` `no wan-bypass`	Enter the **no wan-bypass** command to deactivate the Bypass port.

For more information, refer to the product's Command Reference.

High Availability Configuration Examples

There are several different ways of configuring HA for routers. The following WAN and router redundancy scenarios are supported:

- Device redundancy
- Router device and asymmetric access line redundancy
- Router device and symmetric access line redundancy

Example 1: Device redundancy, IPv4

This configuration uses two routers with a single WAN link allowing physical router redundancy only, not WAN link redundancy. This example shows normal operation with a HA-Mode VRRP session configured. In this scenario router 2 is the VRRP master and router 1 is the VRRP backup. Router 1 is configured to control its Bypass Relay.

In this example relay control is only configured on router 1. HA LED control is configured on both routers. External WAN link status can be monitored to adjust (reduce) VRRP priority. This option allows traffic to flow if one of the external network connections fails.

WAN circuit monitoring is configured in router 2 only, to monitor the connection to the external network via eth1 bypass port. If the electrical connection fails, via eth1 in router 2, then this failover event causes router 2 to reduce its VRRP priority by the configured delta in the circuit-failover command. Router 1 becomes the VRRP master to restore WAN link connectivity from the internal network via router 1.

If this failover event occurs, then there is no way to automatically failback. User intervention is required to fix the issue that caused the failover and return to the original HA state with the redundant pair. This is because the bypass port will be electrically disconnected from the external network (see Figure 7 on page 13), thus keeping the WAN bypass link cable down in router 2, regardless of whether the WAN bypass Ethernet on router 2 is restored.

Figure 6: Device redundancy

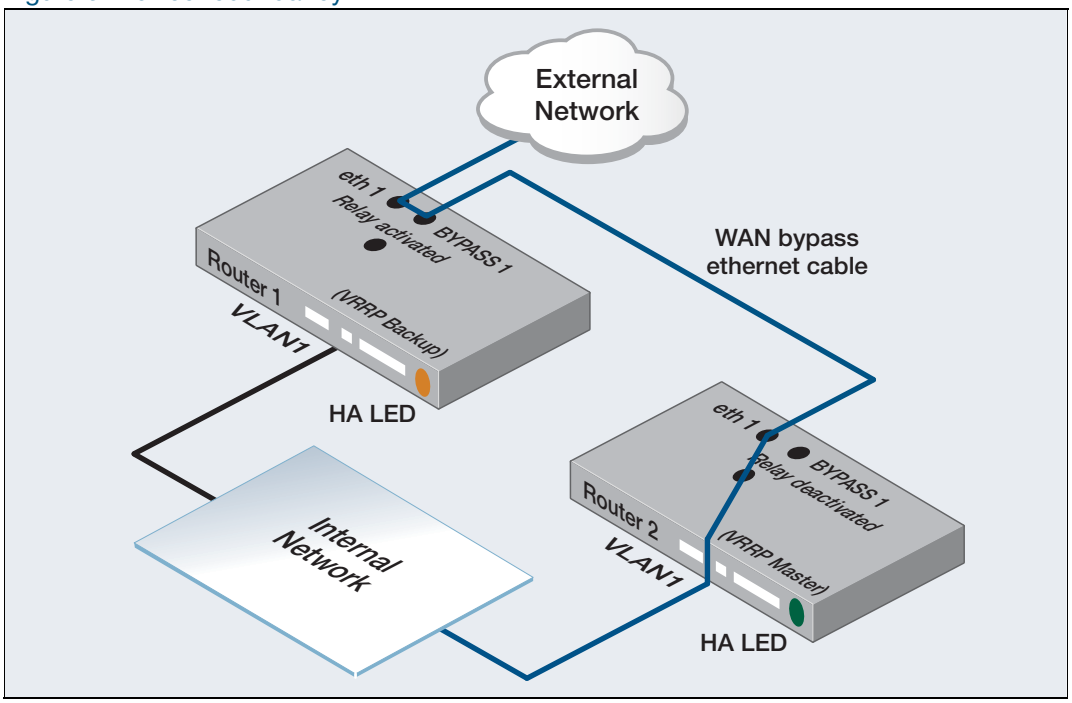
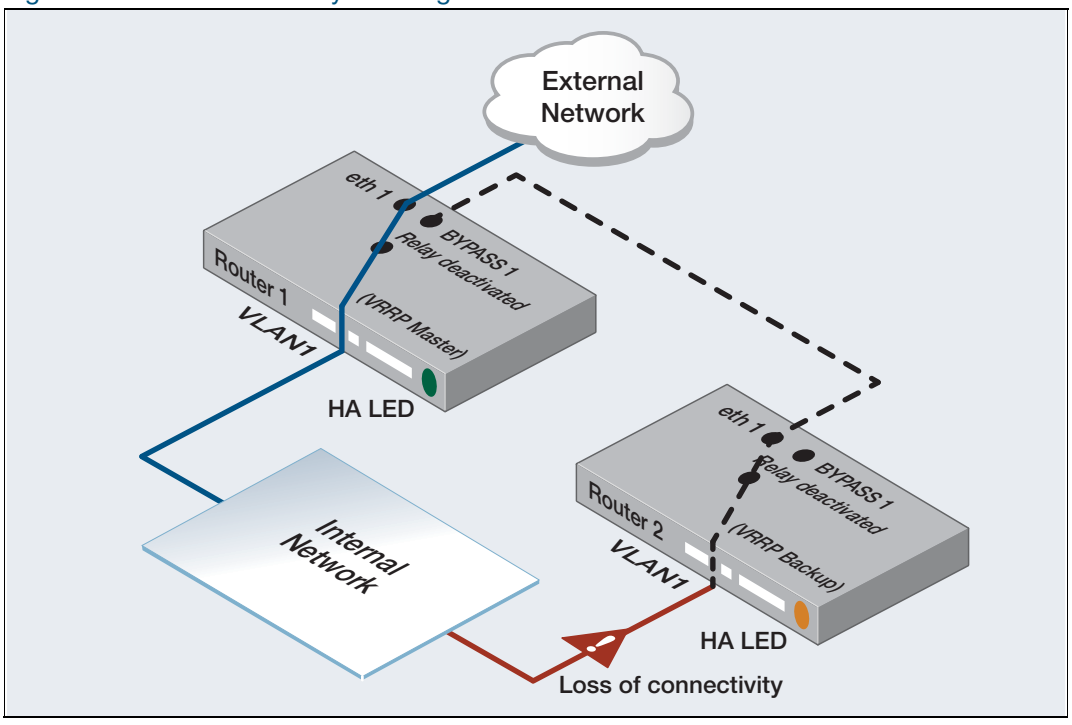


Figure 7: Device redundancy showing the state after a failure in router 2



If connectivity to the internal network fails in router 2, router 1 will transition to master, and deactivate its Bypass Relay, so that packets can be routed from the internal network to the external network connection shared by the redundant pair of devices.

Table 5: Example 1: Device redundancy, IPv4

Step 1. Configure router 1	
`awplus#` `configure terminal`	Enter Configuration mode.
`awplus(config)#` `interface eth1`	Enter the WAN interface.
`awplus(config)#` `ip address 192.168.11.1/24`	Enter the IP address for the WAN interface.
`awplus(config)#` `interface vlan1`	Enter the VLAN interface.
`awplus(config)#` `ip address 192.168.24.1/24`	Enter the IP address for the VLAN interface.
`awplus(config)#` `router vrrp 1 vlan1`	Enter the virtual router ID and VLAN interface.
`awplus(config-router)#` `virtual-ip 192.168.24.12 backup`	Enter the VRRP virtual router IP address and set the default state to backup.
`awplus(config-router)#` `priority 90`	Set priority to 90.
`awplus(config-router)#` `ha associate wan-bypass 1`	Control the HA LED and associate the relay on eth1 with the configured VRRP session.
`awplus(config-router)#` `enable`	Enable the configured VRRP session so it will participate in virtual routing.
Step 2. Configure router 2	
`awplus#` `configure terminal`	Enter Configuration mode.
`awplus(config)#` `interface eth1`	Enter the WAN interface.
`awplus(config)#` `ip address 192.168.11.2/24`	Enter the IP address for the WAN interface.
`awplus(config)#` `interface vlan1`	Enter the VLAN interface.
`awplus(config)#` `ip address 192.168.24.2/24`	Enter the IP address for the VLAN interface.
`awplus(config)#` `router vrrp 1 vlan1`	Associate VRRP instance 1 with VLAN1 and enter VRRP Config mode.
`awplus(config-router)#` `virtual-ip 192.168.24.12 backup`	Enter the virtual router IP address.

`awplus(config-router)# priority 100`	Set VRRP priority to 100.
`awplus(config-router)# ha associate`	Control the HA LED only, without relay control.
`awplus(config)# circuit fail-over eth1 20`	Monitor the link connectivity for the eth1 WAN circuit.
`awplus(config-router)# enable`	Enable the configured VRRP session so it will participate in virtual routing.

Verify the WAN-bypass status

This example shows how to run the **show vrrp** command on the backup router using IPv4. The output is used to check if HA is enabled and display the WAN-bypass status. This example is in HA-Mode and has control of the WAN bypass that is activated in the state.

Note: The state of the Bypass Relay is only displayed in the **show vrrp** command output when the WAN Bypass Relay is explicitly associated with the VRRP instance, which in this example is only the backup master (router 1).

Output 1: Example output from the **show vrrp** command on the backup router.

```
awplus# show vrrp
VMAC enabled
Address family IPv4
VRRP Id: 1 on interface: vlan1
 State: AdminUp    - Backup
 Virtual IP address: 192.168.24.12 (Not-owner)
 Priority is 90
 Advertisement interval: 100 centiseconds
 Preempt mode: TRUE
 Multicast membership on IPv4 interface vlan1: JOINED
 Transition mode: FALSE
 Accept mode: TRUE
 Master address: 192.168.24.2
 High Availability: enabled
  wan-bypass 1 (eth1) is on
```

This example shows how to run the **show vrrp** command on the master router using IPv4. The output is used to check if HA is enabled and displays the WAN-bypass status. In this example VRRP is in HA mode and is not controlling a WAN bypass.

Output 1: Example output from the **show vrrp** command on the master router.

```
awplus# show vrrp
VMAC enabled
Address family IPv4
VRRP Id: 1 on interface: vlan1
 State: AdminUp    - Master
 Virtual IP address: 192.168.24.12 (Not-owner)
 Priority is 200
 Advertisement interval: 100 centiseconds
 Preempt mode: TRUE
 Multicast membership on IPv4 interface vlan1: JOINED
 Transition mode: FALSE
 Accept mode: TRUE
 Master address: 192.168.24.2
 High Availability: enabled
```

Example 2: Device and asymmetric access line redundancy, IPv4

This configuration uses two routers with dual WAN links connected to a single router to provide HA redundancy from a single internal network VLAN1. This example shows normal operation with a single HA-Mode VRRP session configured. In this example relay control is only configured on router 1. Router 1 is configured to control both Bypass Relays. HA LED control is configured on both routers. External WAN link status can be monitored to adjust (reduce) VRRP priority. This allows traffic to flow to the external network if one of the external network connections fails.

In this scenario router 2 is the VRRP master and router 1 is the VRRP backup. Router 1 is configured to control both its Bypass Relays at the same time. Additionally WAN circuit monitoring is configured in router 2 only, to monitor the connection to the external networks via both the eth1 and eth2 bypass ports.

If the electrical connection fails (breaking LAN to WAN connectivity), via the eth1 or eth2 port (or both) in router 2, then its VRRP priority is reduced. The priority is reduced by the configured delta in the circuit-failover commands for each monitored interface. This results in Router 1 becoming the VRRP master, restoring WAN link connectivity for both WAN links from the internal network via Router 1. Load sharing across the two external networks is separately controlled via Policy Based Routing.

Figure 8: Router device and asymmetric access line redundancy

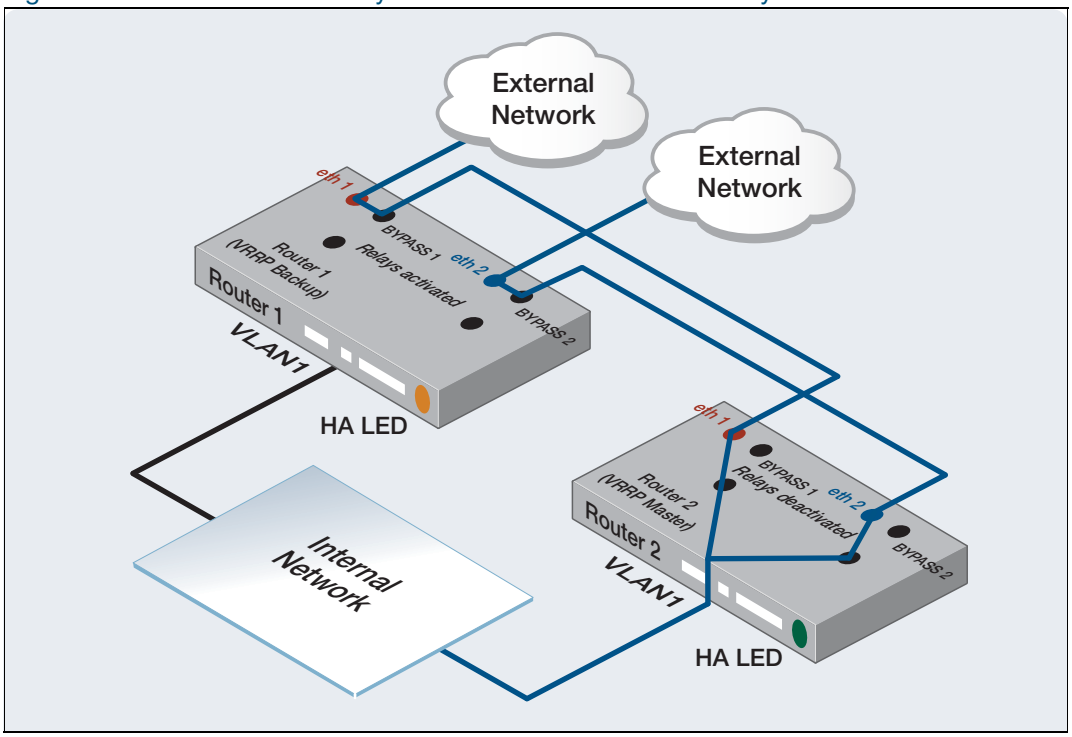


Figure 9: Router device and asymmetric access line redundancy state, after a failure in router 2

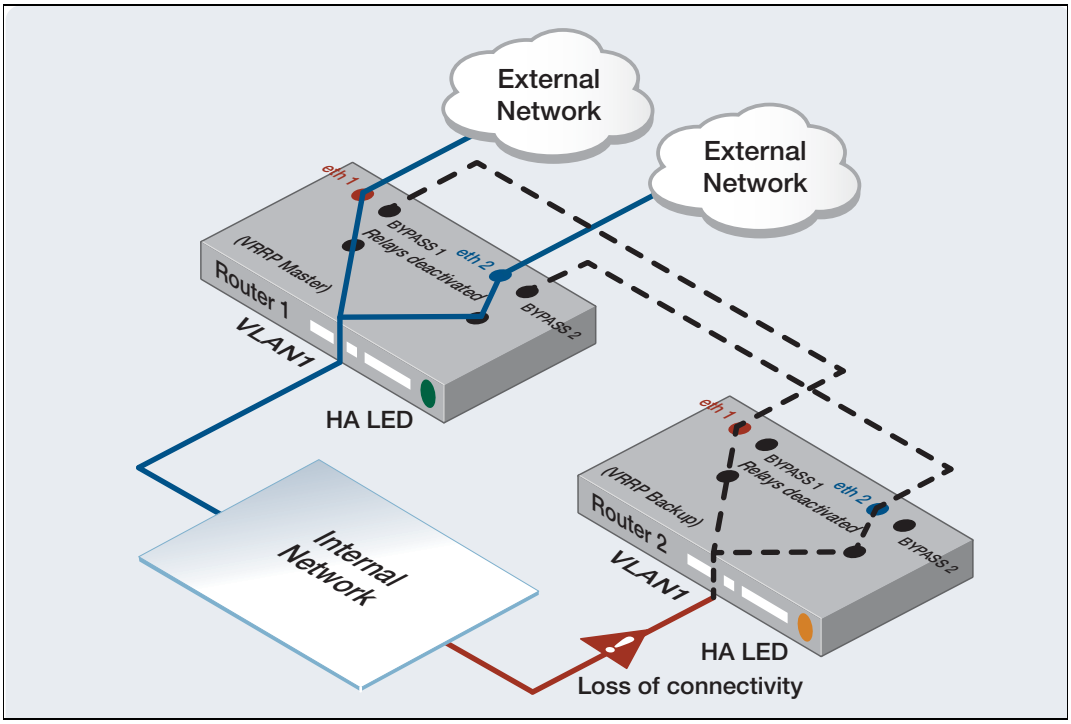


Table 6: Example 2: Device and asymmetric access line redundancy, IPv4

Step 1. Configure router 1	
`awplus#` `configure terminal`	Enter Configuration mode.
`awplus(config)#` `interface eth1`	Enter the WAN interface.
`awplus(config)#` `ip address 192.168.11.1/24`	Enter the IP address for the WAN interface.
`awplus(config)#` `interface eth2`	Enter the second WAN interface.
`awplus(config)#` `ip address 192.168.22.1/24`	Enter the IP address for the second WAN interface.
`awplus(config)#` `interface vlan1`	Enter the VLAN interface.
`awplus(config)#` `ip address 192.168.24.1/24`	Enter the IP address for the VLAN interface.
`awplus(config)#` `router vrrp 1 vlan1`	Associate the VRRP instance with interface VLAN1 and enter VRRP config mode.
`awplus(config-router)#` `virtual-ip 192.168.24.12 backup`	Enter the virtual router IP address and set its default state to backup.
`awplus(config-router)#` `priority 90`	Set VRRP priority to 90.

`awplus(config-router)# ha associate wan-bypass 1`	Control the HA LED and the bypass on eth1.
`awplus(config-router)# ha associate wan-bypass 2`	Control the HA LED and the bypass on eth2.
`awplus(config-router)# enable`	Enable the configured VRRP session to make it participate in virtual routing.
Step 2. Configure router 2	
`awplus# configure terminal`	Enter Configuration mode.
`awplus(config)# interface eth1`	Enter the WAN interface.
`awplus(config)# ip address 192.168.11.2/24`	Enter the IP address for the WAN interface.
`awplus(config)# interface eth2`	Enter the second WAN interface.
`awplus(config)# ip address 192.168.22.2/24`	Enter the IP address for the second WAN interface.
`awplus(config)# interface vlan1`	Enter the VLAN interface.
`awplus(config)# ip address 192.168.24.2/24`	Enter the IP address for the VLAN interface.
`awplus(config)# router vrrp 1 vlan1`	Associate the VRRP instance with interface VLAN1 and enter VRRP config mode.
`awplus(config-router)# virtual-ip 192.168.24.12 backup`	Enter the virtual router IP address.
`awplus(config-router)# priority 100`	Set VRRP priority to 100.
`awplus(config-router)# ha associate`	Control the HA LED.
`awplus(config-router)# enable`	Enable the configured VRRP session so it will participate in virtual routing.
`awplus(config-router)# circuit fail-over eth1 20`	Monitor the by-pass link connection between the redundant pair for eth1.
`awplus(config-router)# circuit fail-over eth2 20`	Monitor the by-pass link connection between the redundant pair for eth2.

Example 3: Device and symmetric access line redundancy, IPv4

This configuration uses two routers with symmetric WAN link redundancy, where each WAN link is attached to a different router. This example shows normal operation with an HA-Mode VRRP instance configured separately. Optionally, Policy Based Routing can be used to load share traffic across the two WAN links from two internal networks, VLAN1 and VLAN2. External WAN link status can be monitored to adjust (reduce) VRRP priority. This allows traffic to flow to the external network if one of the external network connections fails. Relay control and HA LED control are configured in both routers.

This scenario gives router and WAN link redundancy.

Figure 10: Router device and symmetric access line redundancy

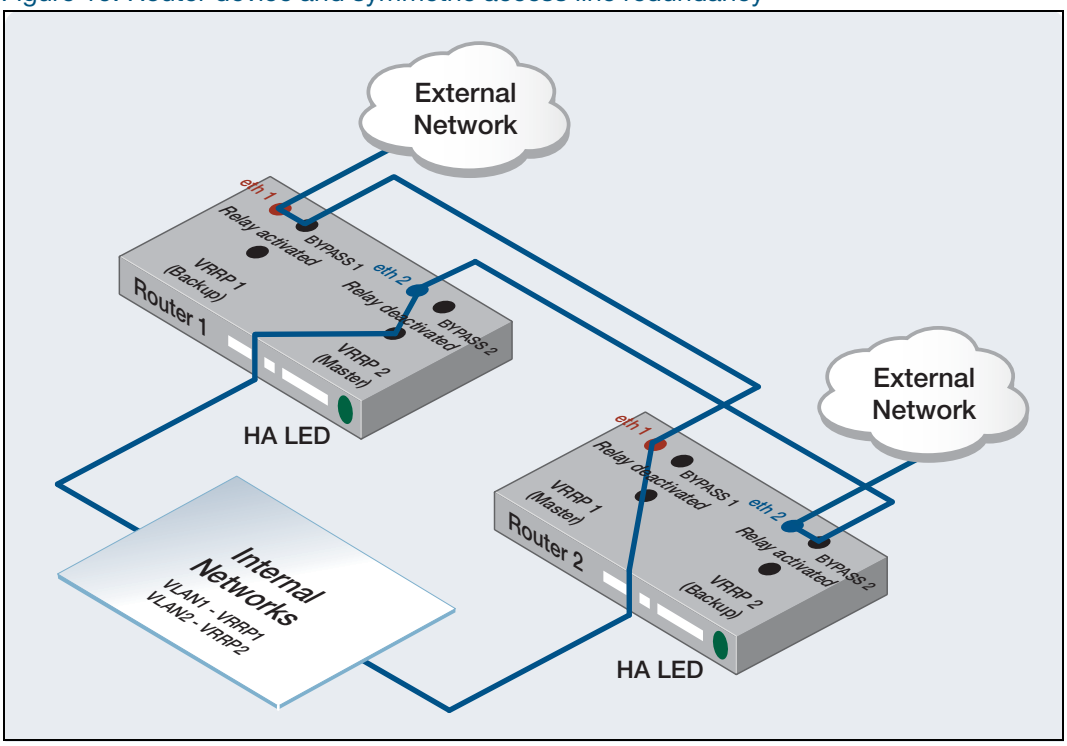


Figure 11: Router device and symmetric access line redundancy, the state after a failure in router 2

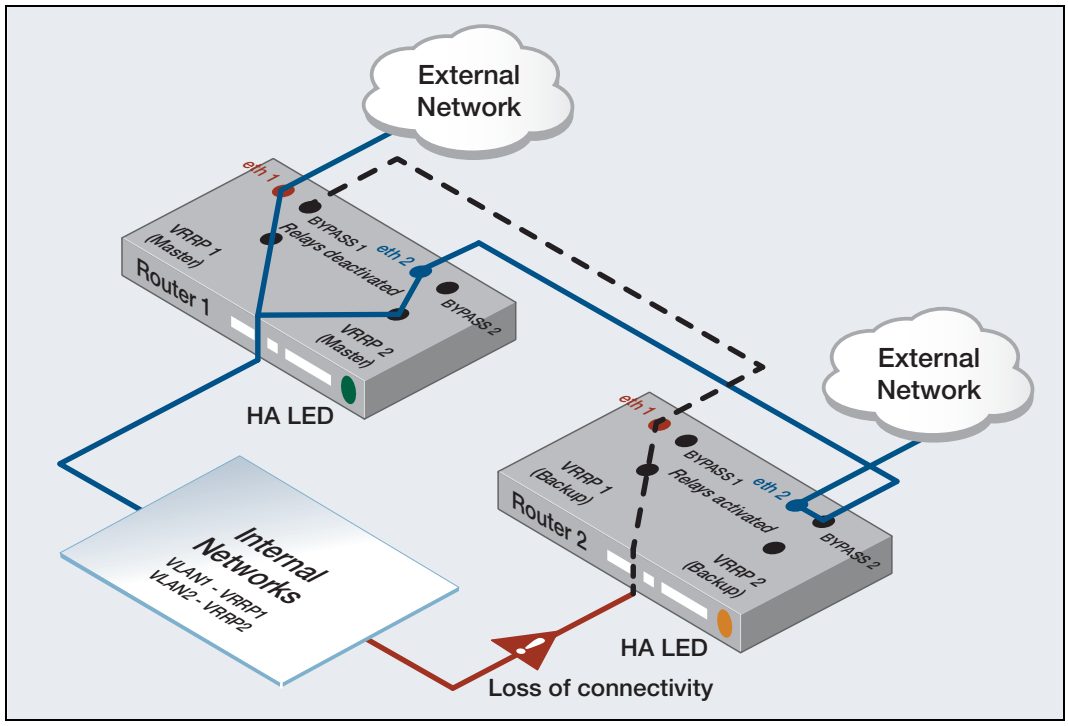


Table 7: Example 3: Device and symmetric access line redundancy, IPv4

Step 1. Configure router 1	
`awplus#` `configure terminal`	Enter Configuration mode.
`awplus(config)#` `interface eth1`	Enter the first WAN interface.
`awplus(config)#` `ip address 192.168.11.1/24`	Enter the IP address for the first WAN interface.
`awplus(config)#` `interface eth2`	Enter the second WAN interface.
`awplus(config)#` `ip address 192.168.22.1/24`	Enter the IP address for the second WAN interface.
`awplus(config)#` `interface vlan1`	Enter the first VLAN interface.
`awplus(config)#` `ip address 192.168.24.1/24`	Enter the IP address for the first VLAN interface.
`awplus(config)#` `interface vlan2`	Enter the second VLAN interface.
`awplus(config)#` `ip address 192.168.12.1/24`	Enter the IP address for the second VLAN interface.
`awplus(config)#` `router vrrp 1 vlan1`	Associate VRRP instance 1 with VLAN1 and enter VRRP config mode.

`awplus(config-router)#` `virtual-ip 192.168.24.12 backup`	Enter the virtual router IP address and set the default state to backup.
`awplus(config-router)#` `priority 90`	Set VRRP priority to 90.
`awplus(config-router)#` `ha associate wan-bypass 1`	Control the HA LED and the bypass on eth1.
`awplus(config-router)#` `enable`	Enable the configured VRRP session so it will participate in virtual routing.
`awplus(config)#` `router vrrp 2 vlan2`	Associate VRRP instance 2 with VLAN2 and enter VRRP config mode.
`awplus(config-router)#` `virtual-ip 192.168.12.12  backup`	Enter the virtual router IP address.
`awplus(config-router)#` `priority 200`	Set VRRP priority to 200.
`awplus(config-router)#` `ha associate wan-bypass 2`	Control the HA LED and the bypass on eth2.
`awplus(config-router)#` `circuit-failover eth2 120`	Configure VRRP WAN circuit monitoring. By configuring the delta value, the virtual router will decrement the VRRP session priority value during a monitored circuit failure event. eth2 is the monitored circuit interface.
`awplus(config-router)#` `enable`	Enable the configured VRRP session so it will participate in virtual routing.
Step 2. Configure router 2	
`awplus` `configure terminal`	Enter Configuration mode.
`awplus(config)` `interface eth1`	Enter the first WAN interface.
`awplus(config)` `ip address 192.168.11.2/24`	Enter the IP address for the first WAN interface.
`awplus(config)` `interface eth2`	Enter the second WAN interface.
`awplus(config)` `ip address 192.168.22.2/24`	Enter the IP address for the second WAN interface.
`awplus(config)#` `interface vlan1`	Enter the first VLAN interface.
`awplus(config)#` `ip address 192.168.24.2/24`	Enter the IP address for the first VLAN interface.

`awplus(config)#` `interface vlan2`	Enter the second VLAN interface.
`awplus(config)#` `ip address 192.168.12.2/24`	Enter the IP address for the second VLAN interface.
`awplus(config)#` `router vrrp 1 vlan1`	Associate VRRP instance with VLAN1 and enter VRRP config mode.
`awplus(config-router)#` `virtual-ip 192.168.24.12 backup`	Enter the virtual router IP address.
`awplus(config-router)#` `priority 200`	Set VRRP priority to 200.
`awplus(config-router)#` `ha associate wan-bypass 1`	Control the HA LED and the bypass on eth1
`awplus(config-router)#` `circuit-failover eth1 120`	Configure VRRP WAN circuit monitoring. By configuring the delta value, the virtual router will decrement the VRRP session priority value during a monitored circuit failure event. eth1 is the monitored circuit interface.
`awplus(config-router)#` `enable`	Enable the configured VRRP session so it will participate in virtual routing.
`awplus(config)#` `router vrrp 2 vlan2`	Associate VRRP instance 2 with VLAN2 and enter VRRP config mode.
`awplus(config-router)#` `virtual-ip 192.168.12.12 backup`	Enter the virtual router IP address and set the default state to backup.
`awplus(config-router)#` `priority 90`	Set VRRP priority to 90.
`awplus(config-router)#` `ha associate wan-bypass 2`	Control the HA LED and the bypass on eth2
`awplus(config-router)#` `enable`	Enable the configured VRRP session so it will participate in virtual routing.

Example 4: Device redundancy, IPv6

This configuration uses two routers with a single WAN link allowing router redundancy only. This example shows normal operation with an HA-Mode VRRP session configured.

In this scenario router 2 is the VRRP master and router 1 is the VRRP backup. Router 1 is configured to control its Bypass Relay. Relay control is only configured on router 1. HA LED control is configured on both routers.

Figure 12: Device redundancy

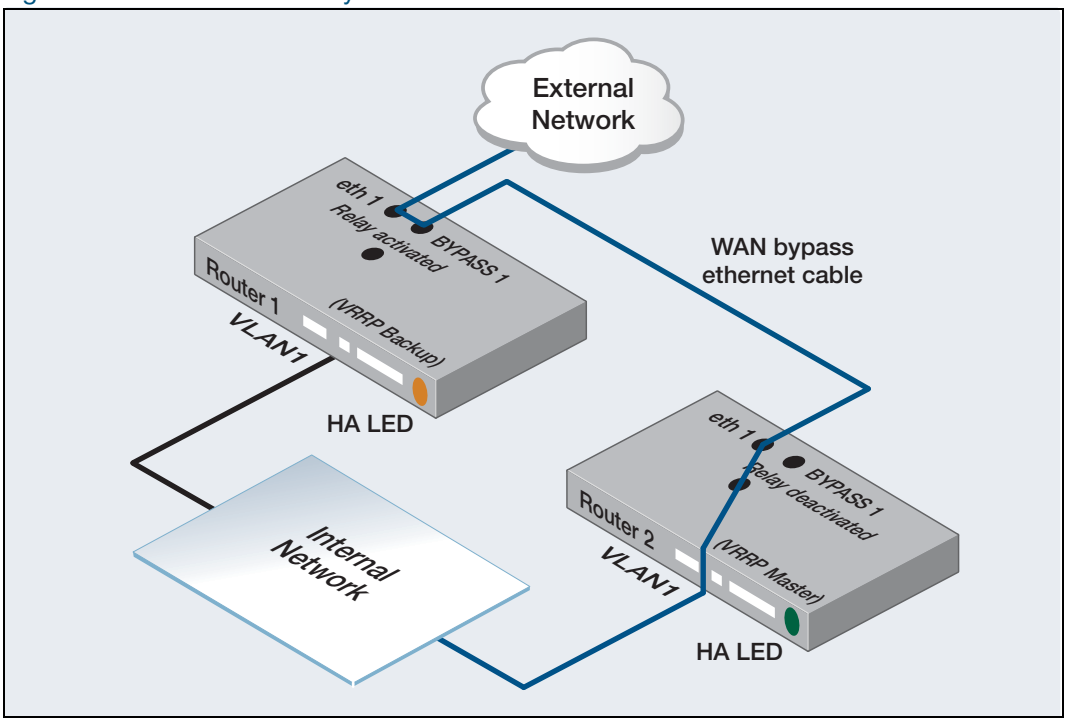
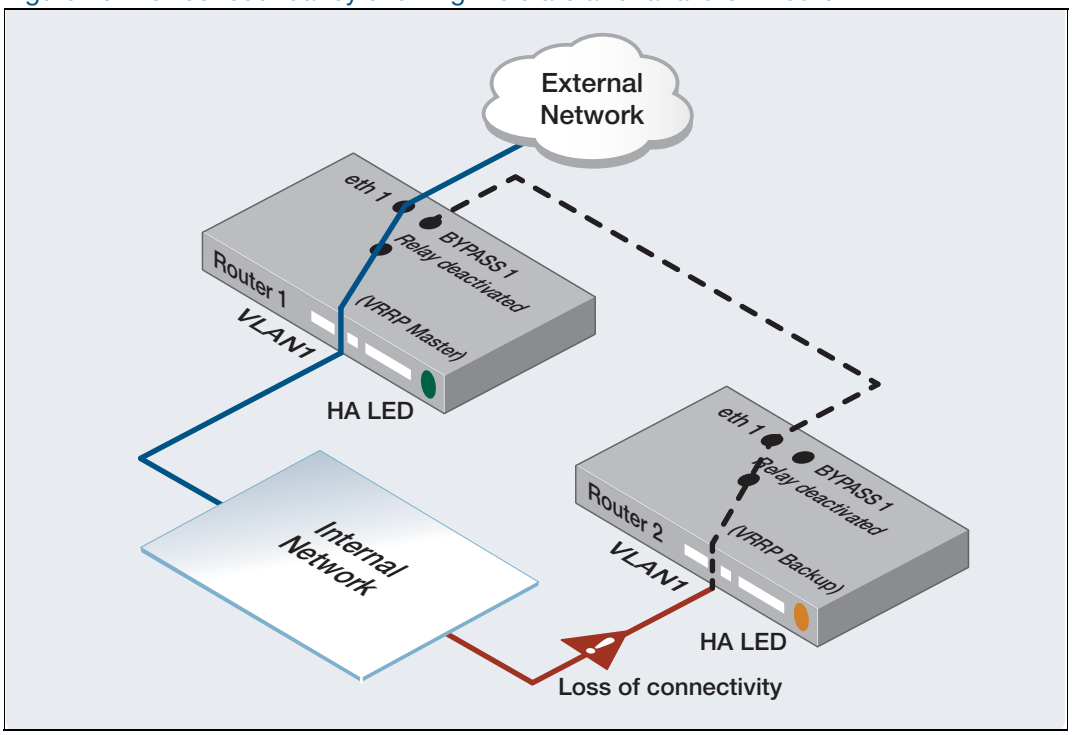


Figure 13: Device redundancy showing the state after a failure in router 2



If connectivity to the internal network fails in router 2, router 1 will transition to master, and deactivate its Bypass Relay, so that packets can be routed from the internal network to the external network connection shared by the redundant pair of devices.

When configuring VRRP for IPv6, the first virtual IP address must be a statically defined link local. You can then also configure a secondary global IPv6 address, however the statically configured virtual link-local IPv6 address must first be configured.

Table 8: Example 4: Device redundancy, IPv6

Step 1. Configure router 1	
`awplus#` `configure terminal`	Enter Configuration mode.
`awplus(config)#` `interface eth1`	Enter the WAN interface.
`awplus(config-if)#` `ipv6 address 2001:db8::1/64`	Enter the IPv6 address for the WAN interface.
`awplus(config-if)#` `interface vlan1`	Enter the VLAN interface.
`awplus(config-if)#` `ipv6 address 2001:db8:20::1/64`	Enter the IPv6 address for the VLAN interface.
`awplus(config-if)#` `router ipv6 vrrp 1 vlan1`	Associate VRRP instance 1 with VLAN1 and enter VRRP config mode.
`awplus(config-router)#` `virtual-ipv6 fe80::2 backup`	Enter the virtual IPv6 address and set the default state to backup.

`awplus(config-router)#` `virtual-ipv6 2001:db8:20::3 backup secondary`	Enter the secondary virtual IPv6 address.
`awplus(config-router)#` `priority 90`	Enter the VRRP priority of this device.
`awplus(config-router)#` `ha associate wan-bypass 1`	Control the HA LED and the bypass on eth1.
`awplus(config-router)#` `enable`	Enable the configured VRRP session so it will participate in virtual routing.
`awplus(config-router)#` `exit`	Revert to Configuration mode.
`awplus(config)#` `exit`	Revert to Privileged Executive mode.
`awplus#` `show vrrp`	Check your configuration.

Step 2. **Configure router 2**	
awplus# configure terminal	Enter Configuration mode.
awplus(config)# interface eth1	Enter the WAN interface.
awplus(config-if)# ipv6 address 2001:db8::2/64	Enter the IPv6 address for the WAN interface.
awplus(config-if)# interface vlan1	Enter the VLAN interface.
awplus(config-if)# ipv6 address 2001:db8:20::2/64	Enter the IPv6 address for the VLAN interface.
awplus(config-if)# router ipv6 vrrp 1 vlan1	Associate the VRRP instance with VLAN1.
awplus(config-router)# virtual-ipv6 fe80::2	Enter the virtual router IPv6 address.
awplus(config-router)# virtual-ipv6 2001:db8:20::3	Enter the secondary virtual router IPv6 address.
awplus(config-router)# priority 150	Enter the backup priority.
awplus(config-router)# ha associate	Control the HA LED only without relay control.
awplus(config-router)# enable	Enable the configured VRRP session so it will participate in virtual routing.
awplus(config-router)# exit	Revert to Configuration mode.
awplus(config)# exit	Revert to Privileged Executive mode.
awplus# show vrrp	Check your configuration.

Verifying the WAN-bypass status

This example shows how to run the **show vrrp** command on the backup router using IPv6. The output is used to check if HA is enabled and displays the WAN-bypass status. In this example VRRP is in HA mode and has control of the WAN-bypass that is in the deactivated state.

Figure 14: Example output from the **show vrrp** command on the backup router

```
awplus# show vrrp
VMAC enabled
Address family IPv6
VRRP Id: 1 on interface: vlan1
  State: AdminUp    - Backup
  Virtual IP address: fe80::2 (Not-owner)
  Secondary Virtual IP address: 2001:db8:20::3 (Not-owner)
  Priority is 90
  Advertisement interval: 100 centiseconds
  Preempt mode: TRUE
  Multicast membership on IPv6 interface  vlan1: JOINED
  Transition mode: FALSE
  Accept mode: TRUE
  Master address: fe80::200:cdff:fe38:c2
  High Availability: enabled
   wan-bypass 1 (eth1) is off
```

This example shows how to run the **show vrrp** command on the master router using IPv6. The output is used to check if HA is enabled and displays the WAN-bypass status.

In this example VRRP is in HA mode and is not controlling a WAN-bypass.

Figure 15: Example output from the **show vrrp** command on the master router

```
awplus# show vrrp
VMAC enabled
Address family IPv6
VRRP Id: 1 on interface: vlan1
 State: AdminUp    - Master
 Virtual IP address: fe80::2 (Not-owner)
 Secondary Virtual IP address: 2001:db8:20::3 (Not-owner)
 Priority is 150
 Advertisement interval: 100 centiseconds
 Preempt mode: TRUE
 Multicast membership on IPv6 interface vlan1: JOINED
 Transition mode: FALSE
 Accept mode: TRUE
 Master address: fe80::200:cdff:fe38:c2
 High Availability: enabled
```