Router Redundancy Using XRRP

Contents

Introduction to XRRP ......................................................... 17-2
Terminology ................................................................. 17-2
Overview of XRRP Operation ................................................. 17-3
  XRRP During Normal Router Operation ......................... 17-4
  XRRP Fail-Over Operation ............................................. 17-5
  XRRP Operation Notes ................................................. 17-10
Configuring XRRP ............................................................ 17-12
  Customizing the XRRP Configuration .............................. 17-12
  Enabling and Disabling XRRP ........................................ 17-16
  Configuration Rules ..................................................... 17-16
  Configuration Examples ................................................. 17-17
Displaying XRRP Data ....................................................... 17-19
Comparison Between XRRP and VRRP ............................... 17-22
Introduction to XRRP

XRRP (XL Router Redundancy Protocol) is the feature used by the HP Procurve Series 5300XL switches to provide router redundancy, or fail-over, to a backup router in case one fails. XRRP is similar to the industry standard VRRP (Virtual Router Redundancy Protocol), although the details of the operation are different.

Throughout this discussion, the 5300XL switches are considered as routers and the term “router” is used to identify them.

Terminology

The following terms are used in the description of XRRP:

- **Protection Domain** – A pair of physical routers that are running XRRP and are configured to provide fail-over protection for each other.

- **Virtual Router** – A virtual routing device that provides a router interface to host computers that are accessing it. Each physical router in the Protection Domain can own a virtual router. On fail-over, one physical router may own all the virtual routers in the Protection Domain. Movement of the virtual router responsibility, as part of the XRRP operation, is transparent to the host computers.

- **Master** – The physical router that is currently providing the virtual router interface to the host computers.

- **Owner** – The physical router that is configured with the IP address that is involved in the XRRP operation.

- **Advertisement Interval** – The time interval at which the Master router sends out XRRP packets on each virtual router interface.
Overview of XRRP Operation

XRRP allows you to configure pairs of HP 5300XL switches to behave as backup routers for each other. Each pair of routers configured to operate this way is defined as a Protection Domain. If either router in the Protection Domain fails for whatever reason, the other router will automatically take over the routing function of the failed router. This transfer of the routing function is transparent to the host computers that are using the routers.

To accomplish this transfer, both routers in the Protection Domain must have identical network access so that each can get to all the same subnets and the same end nodes without going through each other.

Figure 17-1 shows an example of a Protection Domain being used to provide redundant connectivity between some clients and the network servers that the hosts need to access. As part of the XRRP configuration, you define the identity of the Protection Domain. In figure 1, it is Domain 2. See “Configuring XRRP” on page 17-12 for information on how to configure XRRP.

Figure 17-1. XRRP Protection Domain

The clients are connected to the routers through a Layer 2 switch (in this case an HP Procurve Switch 4100GL).
XRRP During Normal Router Operation

For each router, XRRP defines a virtual router, using the IP address that you have configured on the router interface, and for which XRRP assigns a virtual MAC address based on the Protection Domain ID and the XRRP router number of the router that owns the interface. The configuration is done for each VLAN on which you wish to use XRRP for router redundancy, so the router interfaces for each virtual router must be in the VLAN. Each Protection Domain contains two routers, but within a single VLAN, up to 16 Protection Domains (16 pairs of routers) can be configured.

In the situation in which both routers in the Protection Domain are operating normally, none of the VLANs are down, each physical router behaves as the Master of all of its XRRP virtual router interfaces. The Master and Owner of each interface is the same.

In the example shown in figure 17-2, the XRRP configuration is done in VLAN 5. For Domain 2, Router-1 is given the IP address of 10.1.1.1 and Router-2 is given the address 10.1.1.2. XRRP assigns MAC addresses MAC-A to Router-1 and MAC-B to Router-2. Note that the clients in figure 2 use both of the virtual router as their default gateways. Client 10.1.1.48 is configured to use virtual router 10.1.1.1 as its default gateway, and client 10.1.1.49 is configured to use virtual router 10.1.1.2. In this way XRRP can be used to provide load balancing as long as both virtual routers are operating normally. The virtual routers will route packets passed to them, respond to IP ARP requests and PING packets, and perform the other router functions.

Figure 17-2. XRRP During Normal Router Operation
XRRP Fail-Over Operation

If all access to a VLAN from one of the routers in the Protection Domain fails, the routing function of that router is automatically transferred to the other router in the Protection Domain. The master of the virtual router in the Protection Domain sends out multicast advertisements at the XRRP advertisement interval (every 5 seconds by default). If the other router in the Protection Domain does not hear an advertisement packet within 3 advertisement intervals, this other router will become the master router, and it takes control of the IP address and the MAC address of the failed router.

Single VLAN Operation

In figure 17-3, the link between the layer-2 switch and Router-2 fails. As a result, Router-2 no longer hears any link signals on VLAN 5 and the communication between Router-2 and Router-1 is disabled. Router-1, after not hearing XRRP packets from Router-2, will take over the IP addresses from Router-2 for the VLAN 5 interfaces and it will take over the XRRP MAC address for Router-2. Now Router-1 is the Master for its own IP addresses and the IP addresses for Router-2 for VLAN 5, and it is the Master of its own XRRP MAC address and the XRRP MAC address for Router-2. As far as the clients are concerned, the transfer of router functionality is transparent – they can still get to the servers using the same IP addresses and MAC addresses as before.

Figure 17-3. XRRP Fail-Over Example
Figure 17-3 shows a single interface on VLAN 5, but multiple interfaces could exist. For the fail-over to occur, Router-2 must have lost communication on all the VLAN 5 interfaces.

When the fail-over occurs, Router-1 would take over as the Master of the IP address for Router-2 on VLAN 5. If Router-2 has multiple IP addresses on VLAN 5, a multinet situation, Router-1 takes over all the IP addresses for Router-2 on VLAN 5.

### Multiple VLAN Operation

If a router has XRRP interfaces in multiple VLANs, there are some additional details in the way that XRRP operates. For each VLAN on which you wish to run XRRP, a virtual router interface is created.

**Total Router Fail-Over.** In the multiple VLAN case, fail-over again occurs when XRRP packets are not heard on at least one of the VLANs from the other virtual router in the Protection Domain. Even if one or more VLANs are still operating correctly, when one VLAN fails (a link signal is no longer detected by the router from any device in the VLAN), the router with the failed VLAN will stop its operation as the Master of its owned virtual router interfaces. The fail over is a “total router” fail over. The router with the failed VLAN stops routing on all of its XRRP virtual interfaces and the other router in the Protection Domain takes control of all the XRRP IP and MAC addresses.

Depending on whether the routers can maintain communication through at least one or the XRRP VLANs (the VLAN continues to operate correctly for both routers in the Protection Domain), the type of fail-over varies:

- If communication is maintained, the router with the failed VLAN can execute what is called a “fast fail-over”. This situation is depicted in figure 17-4.

- If *all* XRRP communication is lost between the routers in the Protection Domain, the normal fail-over occurs after 3 advertisement intervals, as shown in figure 17-5.
**Fast Fail-Over.** As shown in figure 17-4, if the same link goes down as was shown in figure 17-3, the standard fail-over does not occur. As soon as Router-2 detects the loss of link signal from any device in VLAN 5, it immediately requests, through VLAN 6, that Router-1 to take over all of its virtual router resources. This function is referred to as “fast fail-over”. Because it occurs as soon as link signal is lost, the fail-over can take as little as one second to complete.

![Diagram of Fast Fail-Over with Partial VLAN Failure](image)

*Figure 17-4. Fast Fail-Over with Partial VLAN Failure*

When Router-2 makes the fast fail-over request, if Router-1 has no failed VLANs, then it will take control of Router-2’s virtual interfaces. If Router-1 also has one or more failed VLANs, then it will not take control and both routers will continue to control only their owned IP addresses.
**Standard Fail-Over.** In the multiple-VLAN situation in which all communication between the routers in the Protection Domain is lost, the standard XRRP fail-over occurs. As shown in figure 6, Router-2 has lost communications on all of its XRRP virtual router interfaces. In this case, Router-1 will no longer hear XRRP packets coming from Router-2. If that condition persists for 3 advertisement intervals, Router-1 then takes over all of the virtual routers from Router-2.

![Diagram showing standard XRRP fail-over with total VLAN failure]

**Figure 17-5. Standard XRRP Fail-Over with Total VLAN Failure**

If the cause of the total VLAN access failure, as shown in figure 17-5, is because of a complete router failure (due to building power loss, for example), the router that remains active will wait for the three XRRP advertisement intervals and will then take control of the failed router’s IP and MAC addresses. If both routers are still active but the all network connections between them have been severed, then both routers will take over for each other. This means that identical IP and MAC addresses will exist on both routers, but in a completely severed network, there will be no duplicated MAC or duplicate IP address errors.
If Communication is Maintained Through Non-XRRP Interfaces. In some cases, it may be possible that all connectivity is lost between the routers on all their XRRP virtual router interfaces, in which case XRRP operates and both routers try to take control of all the virtual routers in the Protection Domain, but if connectivity still exists on non-XRRP VLANs, a situation could occur in which both routers allow and use the same MAC addresses on the non-XRRP VLAN(s). This could create a situation in which a switch connected between the two routers will see continuous move interrupts and potential duplication of inbound packets if that switch floods. To prevent this condition, a simple XRRP protocol packet is exchanged between the two routers on the non-XRRP VLAN to inform each other of their uses of the MAC addresses. This exchange prevents the routers from taking over each other’s MAC addresses. Note that this protocol is used only when one router attempts to take over control of the other routers virtual router interfaces.
XRRP Operation Notes

■ **Reserved Multicast MAC Address** – XRRP uses the following multicast MAC address for its protocol packets:

  0101-E794-0640

■ **Use of Proxy ARP on non-XRRP VLANs** – Although it is not disallowed, you should not configure Proxy ARP on non-XRRP VLANs on a router running XRRP. To do so will potentially cause loss connectivity on those non-XRRP VLANs should the router fail-over to the other router in the Protection Domain.

The non-XRRP VLANs will not fail-over, however the XRRP-assigned MAC address, which were used while the router was operating as an XRRP router, were used on all the router interfaces, XRRP and non-XRRP. When the router fails-over its XRRP interfaces, it stops operating as an XRRP router and reverts back to using the default factory-assigned MAC address on all the interfaces. Any hosts that rely on proxy ARP will only receive updated ARPs for the router MAC address not for all the possible IP addresses that the router had previously responded too as a proxy ARP interface. Note: this is not a problem on the XRRP interfaces because the XRRP-assigned MAC address will have moved over to the other router and proxy ARP learned routes will still be valid. (See also “Router connectivity” on the next page).

■ **Static and Default route usage** – You should never set up a default or static route that points to the peer XRRP router as the path. Should fail-over occur, this path is no longer valid and connectivity on that path will be lost.

■ **Router connectivity** – In general peer routers using XRRP must have identical connectivity. That is, they must have the same access to all remote subnets, and the route costs of the access must be the same. This will prevent the routing protocols from using the peer XRRP router as the best path to get to a given subnet.

If this is not done, then fail-over may have to wait until the routing protocols converge before full connectivity is restored. Should one router have exclusive access to a given subnet, (that is, the only way one of the XRRP routers can get to a given subnet is though its peer) connectivity to those exclusive subnets may be lost when fail-over occurs.

■ **SNMP Requests** – SNMP requests on an XRRP router interface will follow the virtual interface, which may be different from the physical interface in a fail-over situation. Alternately, you can make sure that the SNMP requests are made on the management VLAN or other non-XRRP interface.
Multiple VLAN Considerations – When using multiple VLANs, some consideration must be given to whether the router interfaces on the Series 5300XL are connected to devices that have a multiple forwarding database (a MAC address table for each VLAN):

- If the switch at the other end of a router interface connection has a multiple forwarding database, you can use a separate interface for each VLAN. Since the switch at the other end has a separate MAC address table for each VLAN, the fact that the Series 5300XL Switches uses the same MAC address on all interfaces causes no problems.

![Diagram of valid topology](image)

**Figure 17-6. Example of a Valid Topology for Devices Having Multiple Forwarding Databases in a Multiple VLAN Environment**

As of this printing, the HP Procurve switches that have a multiple forwarding database include the Series 5300XL switches, the Series 4100GL Switches, the Switch 2650, and the Switch 6108.

- If the switch at the other end of the router interface connection does not have a multiple forwarding database, you can use only a single interface for the connection. For multiple VLANs, use VLAN tagging. To increase the network bandwidth of the connection between the router and the switch, use a trunk of multiple physical links rather than a single physical link.
Router Redundancy Using XRRP

Configuring XRRP

Figure 17-7. Example of a Solution for Single-Forwarding to Multiple-Forwarding Database Devices in a Multiple VLAN Environment

As of this printing, the HP Procurve switches that do not have a multiple forwarding database include the Switches 1600M, 2400M, 2424M, Series 2500, 4000M, and 8000M. Some older HP AdvanceStack switches also do not have a multiple forwarding database.

For more information, refer to “Multiple VLAN Considerations” on page 11-10.

Configuring XRRP

Configuring XRRP is performed through the switch console CLI at the global configuration level by using the xrrp command. Use the xrrp ? command to see a list of possible options. You define which VLANs have XRRP configured through the xrrp instance command described on page 17-14.

You should first customize the XRRP configuration, as described below, and then enable XRRP, as described on page 17-16. Some of the configuration parameters cannot be changed while XRRP is operational. These are identified in the parameter descriptions below.

Customizing the XRRP Configuration

To customize the XRRP configuration, use any of the following XRRP command options at the CLI global configuration level:

**Syntax.**  
[no] xrrp [domain <1-16> |
    router <1-2> |
    failback <10-999> |
Router Redundancy Using XRRP
Configuring XRRP

`xrrp domain <1-16>`

This command sets the XRRP Protection Domain that the router is in. The router can be in only one domain. The default value is 1.

This value cannot be changed if there is at least one virtual router instance running on the router. To change the value after XRRP is operating, you must first disable XRRP (use the `no xrrp` command).

`xrrp router <1-2>`

This command sets the unique number for the router within a given Protection Domain. No two routers in the same Protection Domain can have the same router number. The default value is 1.

This value cannot be changed if there is at least one virtual router instance running on the router. To change the value after XRRP is operating, you must first disable XRRP (use the `no xrrp` command).
**xrrp failback <10-999>**

This command sets the XRRP fail back time in seconds. The fail back time is the delay that a router will wait before trying to take back control of all the XRRP virtual routers it owns after its VLANs come back up. The default time is 10 seconds.

**[no] xrrp trap <trap-name | all>**

This command enables or disables the generation of SNMP traps for XRRP events on the router. The following trap names are available:

- **state-change** – signifies that the router has a experienced a state change. The trap sent would contain the domain-number, router-number, and state information.

- **master-transition** – signifies that the router state has changed specifically to the master state. The trap sent would contain the domain-number, router-number, and state information.

- **authentication-failure** – signifies that the virtual router instance has received an XRRP packet with an authentication mismatch. The trap sent would contain the domain-number, router-number, and virtual router instance ID (virtual router owner number and VLAN ID) of the virtual router that detected the error.

To enable all the traps, use the command `xrrp trap all`.

To disable the traps, use the `no` form of the command, with the trap name to disable a specific trap or with `all` to disable all the traps. By default, all the traps are disabled.

**[no] xrrp instance <owner-router-number> <vlan-id>**

This command configures the virtual router interface on the router. The virtual router interface (XRRP instance) is identified by the **owner-router-number** and the **vlan-id**. The **owner-router-number** is the XRRP router number of the router that owns the IP address(es). The **vlan-id** identifies the VLAN on which the XRRP instance is running.

**Required Parameters** – For each router in the Protection Domain, an **xrrp instance** command must be entered for each of the following:

- To create each virtual router interface for the physical router being configured, you would enter an **xrrp instance** command with the router number and the VLAN ID for that interface. For example, to create a virtual router interface in VLAN 5 for the router that has the XRRP router number 1, you would enter the following command:
  
  `xrrp instance 1 5`
• To specifically identify the virtual router interfaces on the other router in the Protection Domain, you would enter an `xrrp instance` command with the `ip` parameter. For example, on Router-1 in VLAN 5, to identify the virtual router interface on Router-2 that has the IP address 10.1.1.2 and mask length 24, you would enter the following command:

```
xrrp instance 2 5 ip 10.1.1.2/24
```

For the instance command that creates the virtual router interface on the router being configured, the `ip` parameter must *not* be specified. These XRRP instances, which are being configured on the router that owns the IP address, automatically use the IP address of the VLAN on the router being configured.

Please see the configuration examples on page 17-17 to help clarify these concepts.

• If a VLAN has multiple IP addresses (a multinet situation), an individual IP address can be removed from the XRRP configuration. To remove an IP address from fail-over protection by the router being configured, use the `no` version of the instance command. For example, to remove the virtual interface in the above example from the fail-over protection provided by Router-1, you would enter the following command:

```
no xrrp instance 2 5 ip 10.1.1.2/24
```

You cannot remove an individual IP address if it is the only IP address associated with the backup router.

**Variable Parameters** – In addition, the following variable parameters can be specified by the `xrrp instance` command:

- `advertise <1-60>` – this parameter specifies the frequency, in seconds, that the XRRP Master sends out XRRP advertisement packets. The default is 5 indicating that the Master sends out a packet every 5 seconds.

- `authentication <auth-string>` – this parameter sets the string that is used by the virtual router instance for the authentication of the received XRRP packets. The string can be up to 8 characters long. This same string must be configured on all the virtual routers in the Protection Domain that wish to use authentication.

By default, there is no authentication. Use the `no` version of the command to disable the authentication that was previously enabled on the virtual router interface.

**Note**

For every VLAN on which you wish to run XRRP, you must first configure the VLAN with an IP address.
Enabling and Disabling XRRP

Syntax:  [no] xrrp

Once you have completed the XRRP customization, as described in the previous section, use the xrrp command by itself to enable XRRP operation on the switch for all VLANs on which XRRP has been configured. Use the no xrrp command to disable all XRRP operation on the switch.

Configuration Rules

- XRRP can be configured only on statically configured IP VLANs. VLANs automatically created by GVRP cannot be used.

- XRRP cannot be configured on the management VLAN or on any VLAN that gets its IP address through DHCP or Bootp.

- XRRP must be disabled before the Protection Domain number or the router number configuration can be changed. Use the no xrrp command to disable XRRP.

- **Dynamic reconfiguration** – You should be aware that although XRRP can be reconfigured while it is running, dynamic configurations can lead to inconsistency between the two routers while the configuration changes are in progress. This will potentially result in error log messages until the configurations are consistent (for example, matched IP addresses for primary on one side and secondary on the other). To avoid these logs, disable XRRP while changing its configuration.

  Use the no xrrp command to disable XRRP.
**Configuration Examples**

The following configuration examples create the XRRP setups in the single VLAN and multiple VLAN environments shown in the figures earlier in this chapter.

**Configuration for Figure 17-2 – Single VLAN Example**

See the figure on page 17-4.

<table>
<thead>
<tr>
<th>Router-1 Configuration</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>HPswitch (vlan-5)# ip address 10.1.1.1/24</td>
<td>Configures the IP address of the router interface in VLAN 5.</td>
</tr>
<tr>
<td>HPswitch (config)# xrrp domain 2</td>
<td>Sets the identity of the Protection Domain.</td>
</tr>
<tr>
<td>HPswitch (config)# xrrp router 1</td>
<td>Sets the XRRP router number.</td>
</tr>
<tr>
<td>HPswitch (config)# xrrp instance 1 5</td>
<td>Creates the XRRP virtual router interface.</td>
</tr>
<tr>
<td>HPswitch (config)# xrrp instance 2 5 ip 10.1.1.2/24</td>
<td>Identifies the virtual router interface on Router-2 for which Router-1 is providing fail-over protection.</td>
</tr>
<tr>
<td>HPswitch (config)# xrrp</td>
<td>Enables XRRP operation on Router-1.</td>
</tr>
<tr>
<td>HPswitch (config)# write memory</td>
<td>Saves this configuration to startup memory.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Router-2 Configuration</th>
<th>(the explanation is the same as for Router-1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>HPswitch (vlan-5)# ip address 10.1.1.2/24</td>
<td></td>
</tr>
<tr>
<td>HPswitch (config)# xrrp domain 2</td>
<td></td>
</tr>
<tr>
<td>HPswitch (config)# xrrp router 2</td>
<td></td>
</tr>
<tr>
<td>HPswitch (config)# xrrp instance 2 5</td>
<td></td>
</tr>
<tr>
<td>HPswitch (config)# xrrp instance 1 5 ip 10.1.1.1/24</td>
<td></td>
</tr>
<tr>
<td>HPswitch (config)# xrrp</td>
<td></td>
</tr>
<tr>
<td>HPswitch (config)# write memory</td>
<td></td>
</tr>
</tbody>
</table>
Configuration for Figure 17-4 – Multiple VLANs

See the figure on page 17-7.

<table>
<thead>
<tr>
<th>Router-1 Configuration</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>HPswitch (vlan-5)# ip address 10.1.1.1/24</td>
<td>Configures the IP address of the router interface in VLAN 5.</td>
</tr>
<tr>
<td>HPswitch (vlan-6)# ip address 10.2.1.1/24</td>
<td>Configures the IP address of the router interface in VLAN 6.</td>
</tr>
<tr>
<td>HPswitch (config)# xrrp domain 2</td>
<td>Sets the identity of the Protection Domain.</td>
</tr>
<tr>
<td>HPswitch (config)# xrrp router 1</td>
<td>Sets the XRRP router number.</td>
</tr>
<tr>
<td>HPswitch (config)# xrrp instance 1 5</td>
<td>Creates the XRRP virtual router interface in VLAN 5.</td>
</tr>
<tr>
<td>HPswitch (config)# xrrp instance 2 5 ip 10.1.1.1/24</td>
<td>Identifies the virtual router interface on Router-2 for which Router-1 is</td>
</tr>
<tr>
<td></td>
<td>providing fail-over protection in VLAN 5.</td>
</tr>
<tr>
<td>HPswitch (config)# xrrp instance 1 6</td>
<td>Creates the XRRP virtual router interface in VLAN 6.</td>
</tr>
<tr>
<td>HPswitch (config)# xrrp instance 2 6 ip 10.2.1.1/24</td>
<td>Identifies the virtual router interface on Router-2 for which Router-1 is</td>
</tr>
<tr>
<td></td>
<td>providing fail-over protection in VLAN 6.</td>
</tr>
<tr>
<td>HPswitch (config)# xrrp</td>
<td>Enables XRRP operation on Router-1.</td>
</tr>
<tr>
<td>HPswitch (config)# write memory</td>
<td>Saves this configuration to startup memory.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Router-2 Configuration</th>
<th>(the explanation is the same as for Router-1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>HPswitch (vlan-5)# ip address 10.1.1.2/24</td>
<td></td>
</tr>
<tr>
<td>HPswitch (vlan-6)# ip address 10.2.1.2/24</td>
<td></td>
</tr>
<tr>
<td>HPswitch (config)# xrrp domain 2</td>
<td></td>
</tr>
<tr>
<td>HPswitch (config)# xrrp router 2</td>
<td></td>
</tr>
<tr>
<td>HPswitch (config)# xrrp instance 2 5</td>
<td></td>
</tr>
<tr>
<td>HPswitch (config)# xrrp instance 1 5 ip 10.1.1.1/24</td>
<td></td>
</tr>
<tr>
<td>HPswitch (config)# xrrp instance 2 6</td>
<td></td>
</tr>
<tr>
<td>HPswitch (config)# xrrp instance 1 6</td>
<td></td>
</tr>
<tr>
<td>HPswitch (config)# xrrp instance 2 6 ip 10.2.1.1/24</td>
<td></td>
</tr>
<tr>
<td>HPswitch (config)# xrrp</td>
<td></td>
</tr>
<tr>
<td>HPswitch (config)# write memory</td>
<td></td>
</tr>
</tbody>
</table>
Displaying XRRP Data

To verify XRRP configuration and for XRRP status and statistics information display, use the following CLI `show xrrp` commands at either the Manager level or the global configuration level:

**show xrrp traps**

This command displays the information on the configured XRRP traps.

```
HPswitch(config)# show xrrp traps
Status and Counters - XRRP Traps Information

<table>
<thead>
<tr>
<th>Trap Name</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>state-change</td>
<td>Enabled</td>
</tr>
<tr>
<td>master-transition</td>
<td>Disabled</td>
</tr>
<tr>
<td>authentication-failure</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
```

**show xrrp config [global | instance [<owner-router-num> <vlan-id>]]**

This command displays XRRP configuration information. Invoked without parameters it shows global and virtual routers configuration on the switch.

If the `global` keyword is specified, then the generic configuration information is displayed.

```
HPswitch(config)# show xrrp config global
Status and Counters - XRRP Global Configuration Information

XRRP Enabled : Yes
Domain Number : 2
Router Number : 1
Failback Delay : 11
```

The keyword `instance` can be used to display configuration information for the virtual router instance(s) on the switch. If no parameters are specified after this keyword, the information for all virtual routers is displayed, otherwise...
the information for the particular virtual router is displayed by specifying the `owner-router-number` and the `vlan-id` in the command. In the example below, the configuration information for the virtual router number 1 on VLAN 5 is requested.

```plaintext
HPswitch(config)# show xrrp config instance 1 5
```

Status and Counters - XRRP Virtual Router Configuration Information

```
Owner Router Number : 1
VLAN ID : 5
Authentication Type : Simple Text Password
Authentication Key : password
Advertise Interval : 5
```

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.1.1</td>
<td>255.255.248.0</td>
</tr>
<tr>
<td>10.2.1.1</td>
<td>255.255.248.0</td>
</tr>
</tbody>
</table>

This command displays XRRP status and statistics information.

If the keyword `global` is used, then generic information is displayed as shown in the next example.

```plaintext
HPswitch(config)# show xrrp statistics global
```

Status and Counters - XRRP Global Statistics Information

```
XRRP Enabled : Yes
This Domain Number : 2
This Router Number : 1
XRRP MAC Addr : 0001e7-940601
XRRP AND Mask : fffffffffff
XRRP Up Time : 46 hours
```

<table>
<thead>
<tr>
<th>Pkts Rx</th>
<th>Corrupt Pkts</th>
<th>Bad Version</th>
<th>Bad Chksum</th>
<th>Not Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
The keyword `instance` can be used to display statistics information for the virtual router instance(s) on the switch. If no parameters are specified after this keyword, the information for all virtual routers is displayed, otherwise the information for the particular virtual router is displayed by specifying the `owner-router-number` and the `vlan-id` in the command. In the example below, the statistics information for the virtual router number 1 on VLAN 5 is requested.

```plaintext
HPswitch(config)# show xrrp statistics instance 1 5

Status and Counters - XRRP Virtual Router Statistics Information

Owner Router Number : 1
VLAN ID : 5
Operational State : Master
Up Time : 64 mins

Pkts Rx : 0 Pkts Tx : 780
Zero Priority Rx : 0 Zero Priority Tx : 0
Bad Version Pkts : 0 Mismatched Pswd Pkts : 0
Mismatched IP Pkts : 0 Mismatched Interval Pkts : 0
```

The keyword `router` can be used to display statistics information for the specific router coordinator operating in the XRRP domain as shown in the next example.

```plaintext
HPswitch(config)# show xrrp statistics router 2

Status and Counters - XRRP Router Coordinator Statistics Information

Router Number : 2
Become Master : 1
Master Time : 76 mins

Type1 Type1 Type2 Type2 Unknown
Pkts Rx Pkts Tx Pkts Rx Pkts Tx VLAN ID
----------------- ----------------- ----------------- ----------------- ---------------
0 924 0 0 0
```

---

**Router Redundancy Using XRRP**

**Displaying XRRP Data**

The keyword `instance` can be used to display statistics information for the virtual router instance(s) on the switch. If no parameters are specified after this keyword, the information for all virtual routers is displayed, otherwise the information for the particular virtual router is displayed by specifying the `owner-router-number` and the `vlan-id` in the command. In the example below, the statistics information for the virtual router number 1 on VLAN 5 is requested.

```plaintext
HPswitch(config)# show xrrp statistics instance 1 5

Status and Counters - XRRP Virtual Router Statistics Information

Owner Router Number : 1
VLAN ID : 5
Operational State : Master
Up Time : 64 mins

Pkts Rx : 0 Pkts Tx : 780
Zero Priority Rx : 0 Zero Priority Tx : 0
Bad Version Pkts : 0 Mismatched Pswd Pkts : 0
Mismatched IP Pkts : 0 Mismatched Interval Pkts : 0
```

The keyword `router` can be used to display statistics information for the specific router coordinator operating in the XRRP domain as shown in the next example.

```plaintext
HPswitch(config)# show xrrp statistics router 2

Status and Counters - XRRP Router Coordinator Statistics Information

Router Number : 2
Become Master : 1
Master Time : 76 mins

Type1 Type1 Type2 Type2 Unknown
Pkts Rx Pkts Tx Pkts Rx Pkts Tx VLAN ID
----------------- ----------------- ----------------- ----------------- ---------------
0 924 0 0 0
```
Comparison Between XRRP and VRRP

The following information compares the characteristics of XRRP and the industry standard VRRP.

- XRRP will allow a router to respond to SNMP requests on the virtual router IP address even if it is not the owner. VRRP does not. This would allow you to still access the failed router on VLANs that are accessible on that router.
- XRRP uses the same MAC address for each virtual router owned by a given physical router. VRRP uses a separate MAC address per virtual router.
- XRRP uses a fail-over domain concept with up to 2 routers in the fail-over domain and up to 16 domains connected to a given VLAN. VRRP uses a flat space with up to 255 virtual routers in a level 2 switch fabric. However these 255 virtual routers can be used over on every VLAN with VRRP.
- XRRP will warn you of mismatched configurations between the routers but will attempt to use the current master configuration whenever possible when these mismatches occur.
- VRRP fails over at the virtual router level allowing a given physical router to continue to route packets on those virtual routers that it still owns. XRRP will fail-over at the router level. If one of the virtual routers controlled by a physical router fails, then all the virtual routers that it owns will be taken over by the other router in the same XRRP Protection Domain.
- XRRP has fast fail-over. VRRP does not.