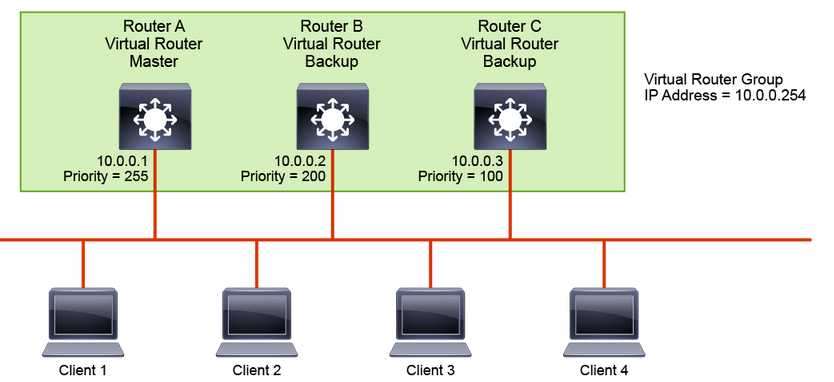
**Discovery 13: Configure VRRP**

**Overview**

**VRRP**

VRRP is an open standard alternative to HSRP.



VRRP is similar to HSRP, both in operation and configuration. The VRRP master is analogous to the HSRP active gateway, while the VRRP backup is analogous to the HSRP standby gateway. A VRRP group has one master device and one or multiple backup devices. A device with the highest priority is the elected master. The priority can be a number between 0 and 255. The priority value 0 has a special meaning—it indicates that the current master has stopped participating in VRRP. This setting is used to trigger backup devices to quickly transition to master without having to wait for the current master to time out.

VRRP differs from HSRP in that it allows you to use an address of one of the physical VRRP group members as a virtual IP address. In this case, the device with the used physical address is a VRRP master whenever it is available.

The master is the only device that sends advertisements (analogous to HSRP hellos). Advertisements are sent to the 224.0.0.18 multicast address, with the protocol number 112. The default advertisement interval is 1 second. The default holdtime is 3 seconds. HSRP, in comparison, has the default hello timer set to 3 seconds and the hold timer to 10 seconds.

Although the VRRP protocol as per RFC 3768 does not support millisecond timers, Cisco devices allow you to configure millisecond timers. You need to manually configure the millisecond timer values on both the master and the backup devices. Use the millisecond timers only when absolutely necessary and with careful consideration and testing. Millisecond values work only under favorable circumstances, and you must be aware that the use of the millisecond timer values restricts VRRP operation to Cisco devices only.

**Note**

When you use millisecond values, the master advertisement value that is displayed by the show vrrp command output on the backup routers is always 1 second, even though the actual value may differ.

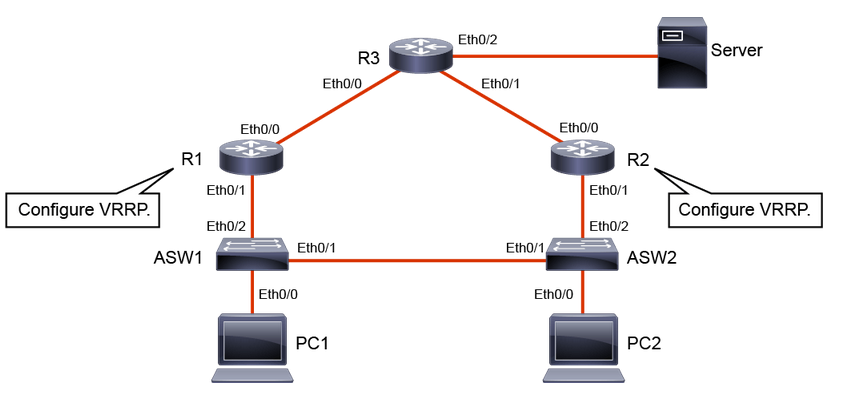
In the example, the Layer 3 switches A, B, and C are configured as VRRP virtual routers and are members of the same VRRP group. Because switch A has the highest priority, it is elected as the master for this VRRP group—end-user devices will use it as their default gateway. The Layer 3 switches B and C function as virtual router backups. If the master fails, the device with the highest configured priority will become the master and provide uninterrupted service for the LAN hosts. When switch A recovers and the pre-emption is enabled, switch A becomes the master again. Contrary to HSRP, pre-emption is enabled by default with VRRP.

Load sharing is also available with VRRP and, like with HSRP, multiple virtual router groups can be configured. For instance, you could configure clients 3 and 4 to use a different default gateway than clients 1 and 2 do. Then you would configure the three Layer 3 switches with another VRRP group and designate switch B to be the master VRRP device for the second group.

In this discovery, you will learn how to configure VRRP and the differences between VRRP and HSRP.

Your configuration task is as follows:

* Configure and verify VRRP
* Configure authentication for VRRP



**Task 1: Configure VRRP on Routers**

**Activity**

**Step 1:** Configure GigabitEthernet 0/1 on R1 with the IP address 192.168.1.3 and the VRRP virtual IP address 192.168.1.1.

On R1, enter the following commands:

R1(config)# interface GigabitEthernet 0/1

R1(config-if)# ip address 192.168.1.3 255.255.255.0

R1(config-if)# vrrp 1 ip 192.168.1.1



Like HSRP, VRRP uses the concept of the virtual IP address to provide the end-user devices with redundant first-hop connectivity. The virtual IP address is configured by using the vrrp group\_number ip virtual\_ip interface configuration command.

You can use one of the "real" IP addresses from physical routers as the virtual IP address. In this example you could, for instance, use 192.168.1.3 as the virtual IP address.

Observe the console message and notice that since there is not another active VRRP router in the broadcast domain R1 transitions to the Master state.

**Step 2:** Configure GigabitEthernet 0/1 on R2 with the IP address of 192.168.1.2 and the VRRP virtual IP address of 192.168.1.1.

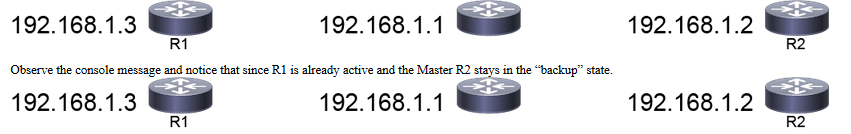
On R2, enter the following commands:

R2(config)# interface GigabitEthernet 0/1

R2(config-if)# ip address 192.168.1.2 255.255.255.0

R2(config-if)# vrrp 1 ip 192.168.1.1





With HSRP, you could leave out the group number when performing the configuration and it will default to group 0. With VRRP, there is no such default. You need to specify a group number, which can be anything between 1 and 255.

**Step 3:** Configure GigabitEthernet 0/1 on R2 with a VRRP priority of 110.

On R2, enter the following command:

R2(config-if)# vrrp 1 priority 110



Go to R1 and find below message



In the CLIs of the routers, you observed console messages that showed that R2 has now transitioned to the master state and R1 to the backup state.

A higher priority is configured on a device that should be the master of the VRRP group. In this example, you configured R2 with a priority of 110. R1 is left with the default priority of 100.

However, if you use one of the router IP addresses as the virtual IP address, priorities are ignored for electing the master. The router that has the IP address that matches the virtual IP address will become the master.

VRRP has pre-emption enabled by default, compared to HSRP having pre-emption disabled by default.

**Step 4:** On VRRP-enabled devices, verify the VRRP status.

On R1 and R2, enter the following commands:

R1# show vrrp



R2# show vrrp



In the output of R1, you can see the MAC address of the virtual router. The MAC address has the following form: 0000.5e00.01XX, where XX is the two-digit hexadecimal group number.

R2# show vrrp brief

Interface Grp Pri Time Own Pre State Master addr Group addr Et0/1 1 110 3570 Y Master 192.168.1.2 192.168.1.1

To verify VRRP status, use the show vrrp command. If you append the brief keyword, you will get a more condensed view.

**Task 2: Configure Authentication for VRRP**

**Activity**

**VRRP and Authentication**

The VRRP standard that is used to specify plaintext and MD5 authentication, which was later revoked. However, Cisco IOS devices still support authentication mechanisms.

* VRRP used plaintext and MD5 authentication with RFC 2338.
* RFC 3768 and RFC 5798 remove authentication support for VRRP.
* Cisco IOS Software still supports the RFC 2338 authentication mechanisms.

R1(config-if)# vrrp group\_number authentication text key\_string

* Configures plaintext authentication

R1(config-if)# vrrp group\_number authentication md5 key-string key\_string

* Configures MD5 authentication

According to RFC 5798, operational experience and further analysis determined that VRRP authentication did not provide sufficient security to overcome the vulnerability of misconfigured secrets, causing multiple masters to be elected. Due to the nature of the VRRP protocol, even if VRRP messages are cryptographically protected, it does not prevent hostile nodes from behaving as if they are the VRRP master, creating multiple masters. Authentication of VRRP messages could have prevented a hostile node from causing all properly functioning routers from going into the backup state. However, having multiple masters can cause as much disruption as no routers, which authentication cannot prevent. Also, even if a hostile node could not disrupt VRRP, it can disrupt ARP and create the same effect as having all routers go into the backup state.

Independent of any authentication type, VRRP includes a mechanism (setting Time to Live [TTL] = 255, checking on receipt) that protects against VRRP packets being injected from another remote network. This setting limits most vulnerability to local attacks.

With Cisco IOS devices, the default VRRP authentication is plaintext. MD5 authentication can be configured by specifying a key string or, like with HSRP, reference to a key chain.

**Step 1:** Configure MD5 authentication for VRRP on the GigabitEthernet 0/1 interface of R1.

On R1, enter the following commands:

R1(config)# interface GigabitEthernet 0/1

R1(config-if)# vrrp 1 authentication md5 key-string MyVRRP



In the CLI output of R1, notice the "bad authentication" message. R1 is currently configured with the MD5 authentication while R2 has no VRRP authentication configured. As a consequence, the routers do not consider each other as members of the same group. If you verify the VRRP status on both devices, you will see that both consider themselves to be the master for VRRP group 1.



**Step 2:** Configure MD5 authentication for VRRP on the GigabitEthernet 0/1 interface of R2.

On R2, enter the following commands:

R2(config)# interface GigabitEthernet 0/1

R2(config-if)# vrrp 1 authentication md5 key-string MyVRRP



Notice that now that you have configured matching MD5 VRRP authentications, you get a message in the CLI output of R1 that says that R1 is transitioning to the backup state.

On R1 find below message.



**Step 3:** Verify the VRRP states and authentication method or R1 and R2.

On R1 and R2, enter the following commands:

R1# show vrrp



R2# show vrrp



Verify that R1 is in the “Backup” state and using “MD5, key-string” as the authentication method, and R2 is in the “Master” state and also using “MD5, key-string” as the authentication method.