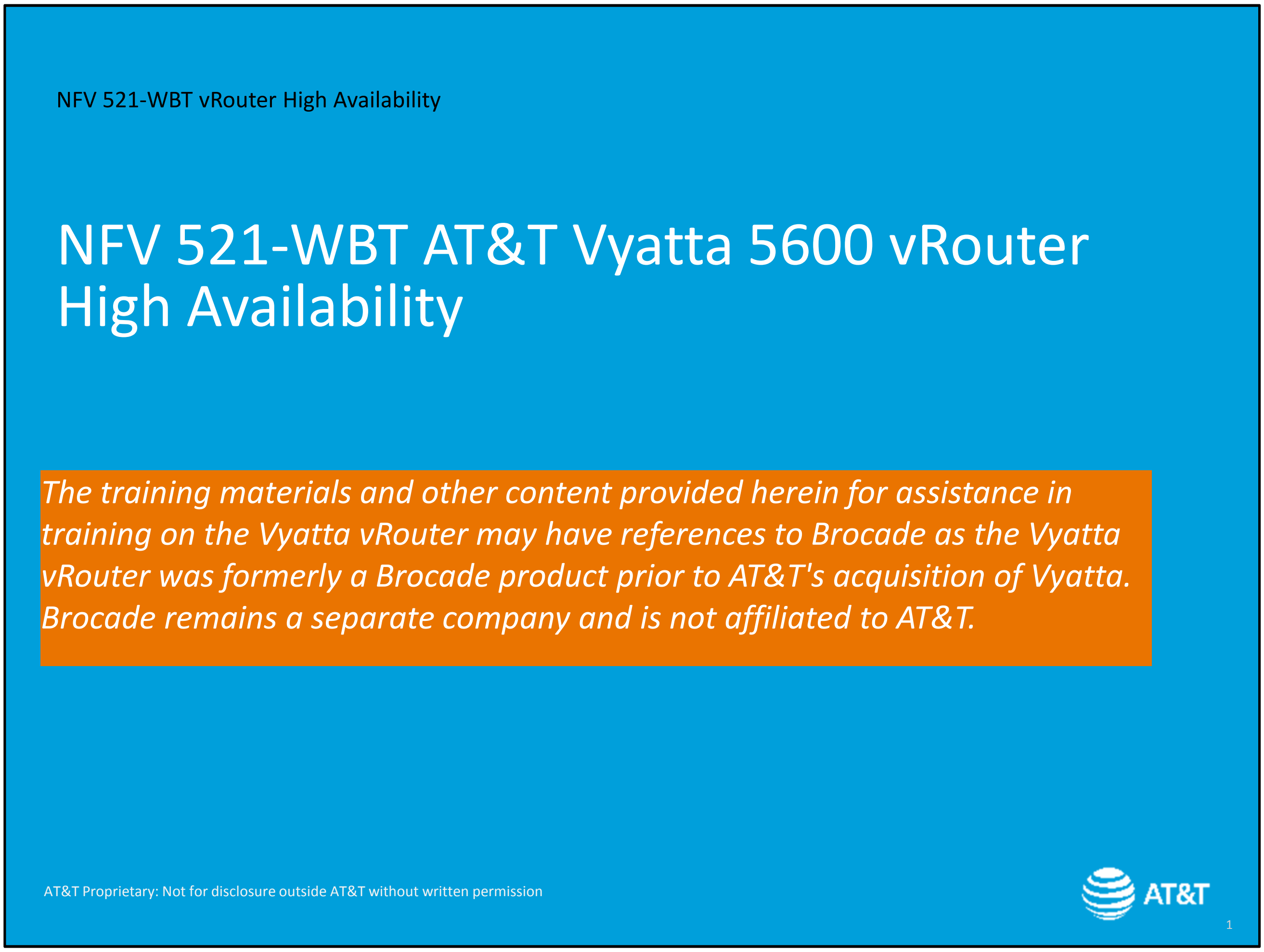


NFV 521-WBT vRouter High Availability

NFV 521-WBT AT&T Vyatta 5600 vRouter High Availability

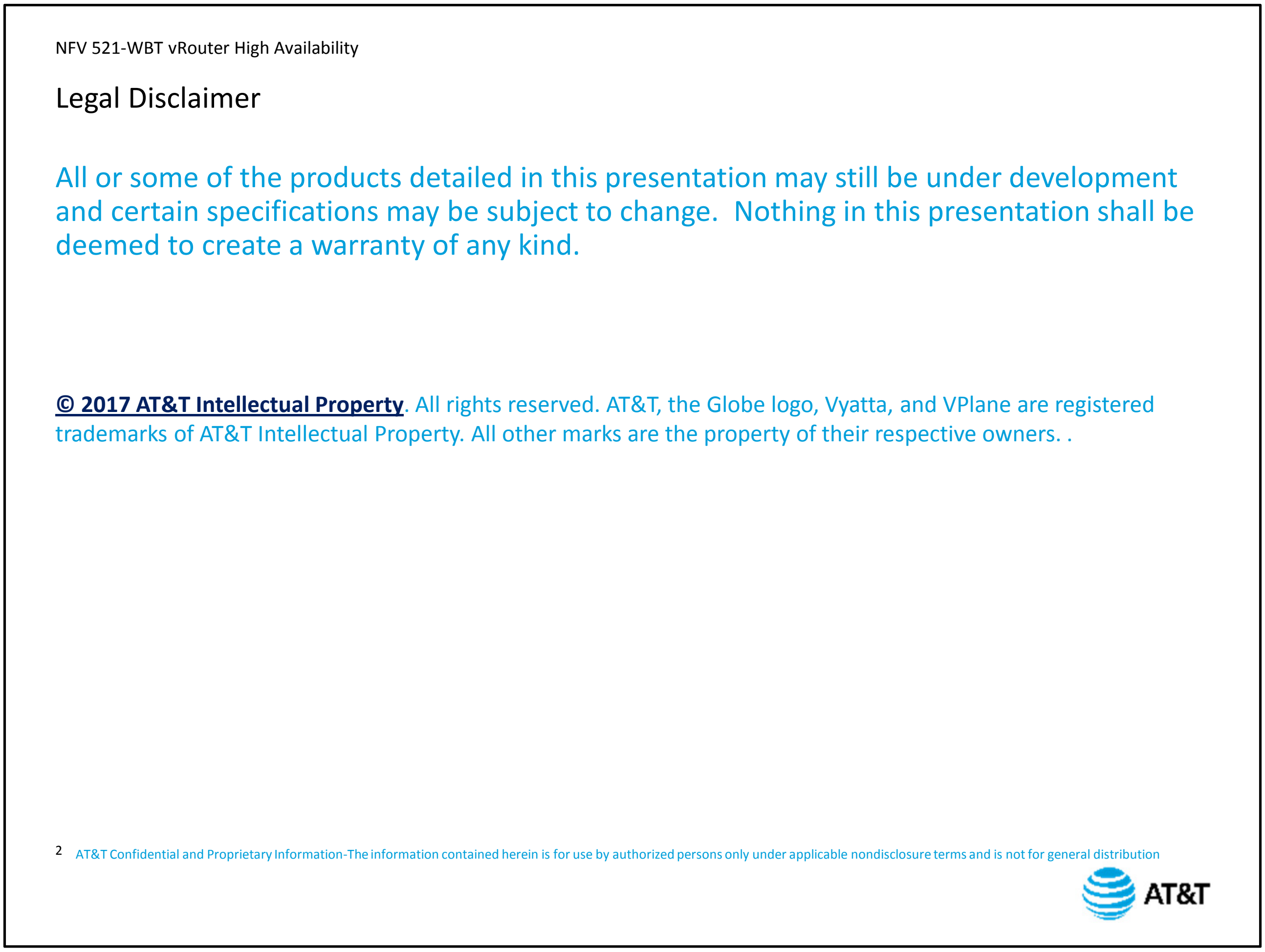
The training materials and other content provided herein for assistance in training on the Vyatta vRouter may have references to Brocade as the Vyatta vRouter was formerly a Brocade product prior to AT&T's acquisition of Vyatta. Brocade remains a separate company and is not affiliated to AT&T.

AT&T Proprietary: Not for disclosure outside AT&T without written permission

AT&T

1

Welcome to the AT&T vRouter Dynamic Multipoint VPN course.

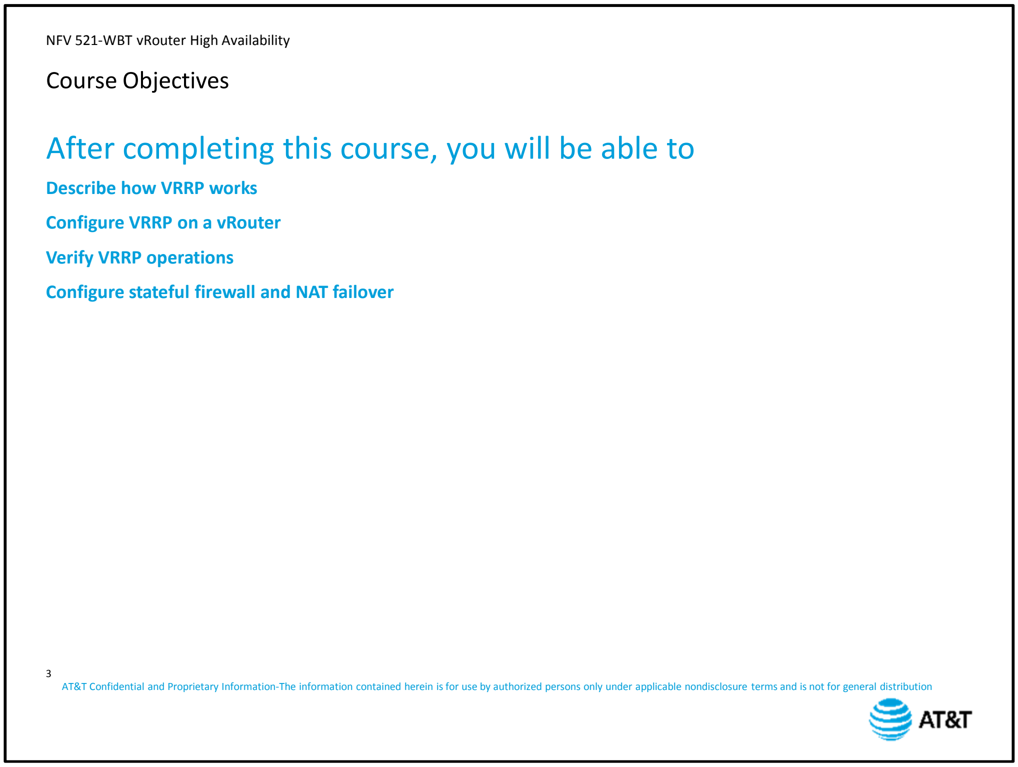


NFV 521-WBT vRouter High Availability

Legal Disclaimer

All or some of the products detailed in this presentation may still be under development and certain specifications may be subject to change. Nothing in this presentation shall be deemed to create a warranty of any kind.

Before we begin the course, please take a moment to read our legal disclaimer.



NFV 521-WBT vRouter High Availability

Course Objectives

After completing this course, you will be able to

Describe how VRRP works

Configure VRRP on a vRouter

Verify VRRP operations

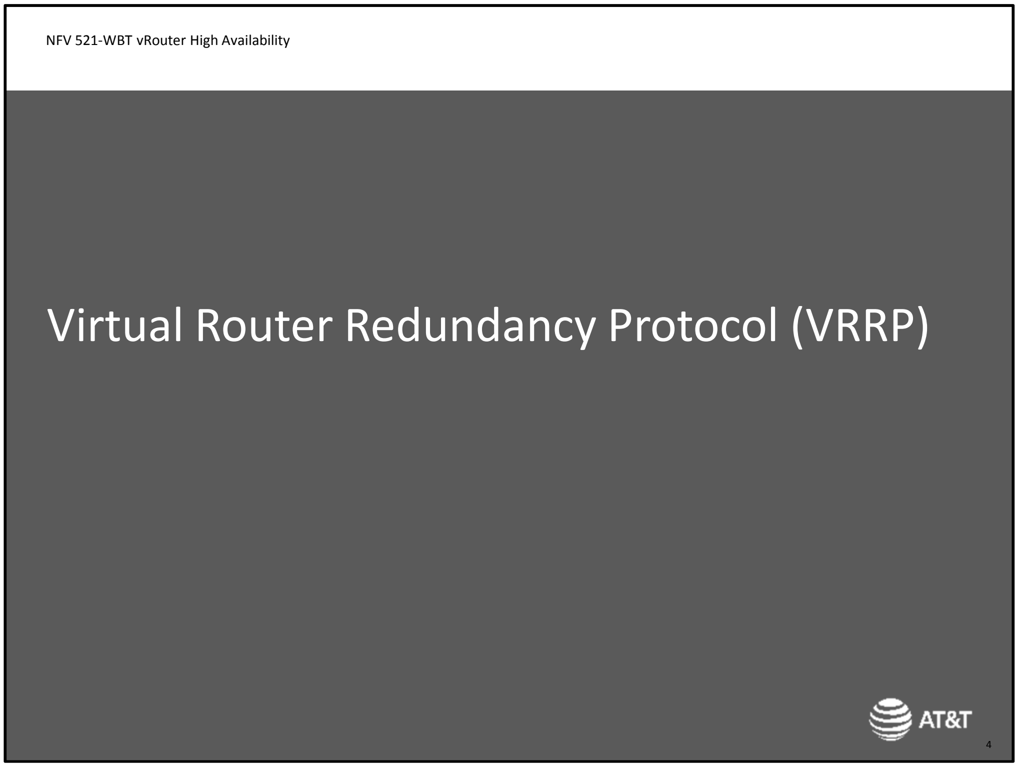
Configure stateful firewall and NAT failover

3

AT&T Confidential and Proprietary Information-The information contained herein is for use by authorized persons only under applicable nondisclosure terms and is not for general distribution

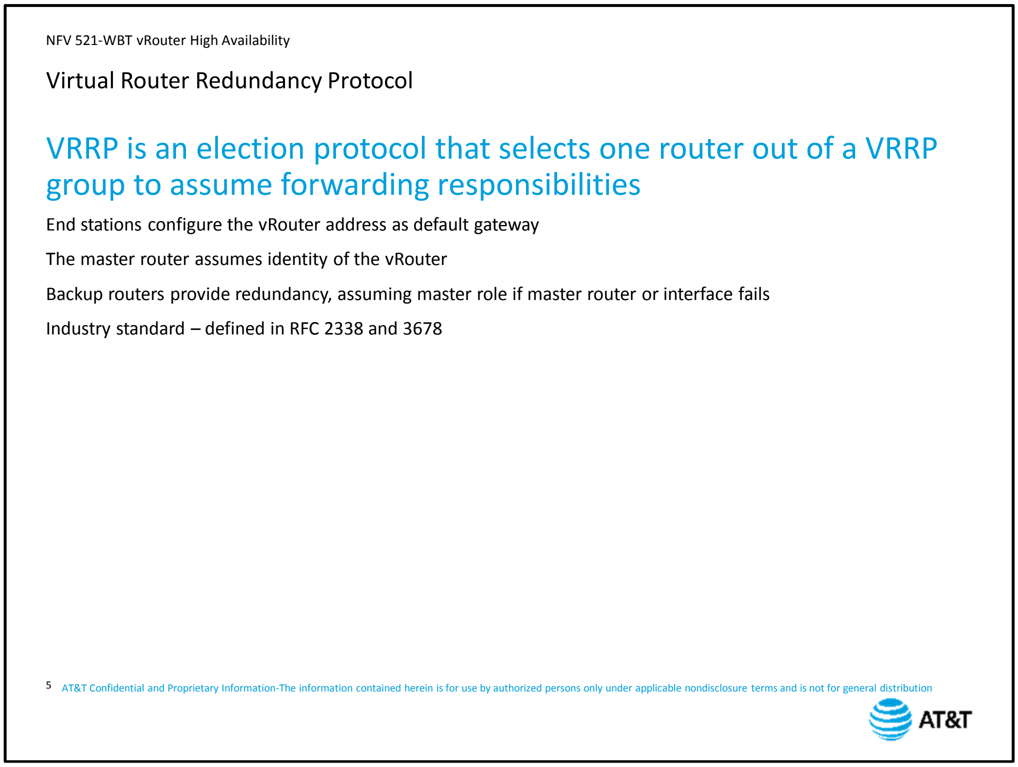
Welcome to the AT&T vRouter High Availability Features course.
After completing this course, you will be able to:

- Describe how VRRP works
- Configure VRRP on a vRouter
- Verify VRRP operations
- Configure stateful firewall and NAT failover



Virtual Router Redundancy Protocol (VRRP)

Let’s start out with a discussion of VRRP



NFV 521-WBT vRouter High Availability

Virtual Router Redundancy Protocol

VRRP is an election protocol that selects one router out of a VRRP group to assume forwarding responsibilities

End stations configure the vRouter address as default gateway

The master router assumes identity of the vRouter

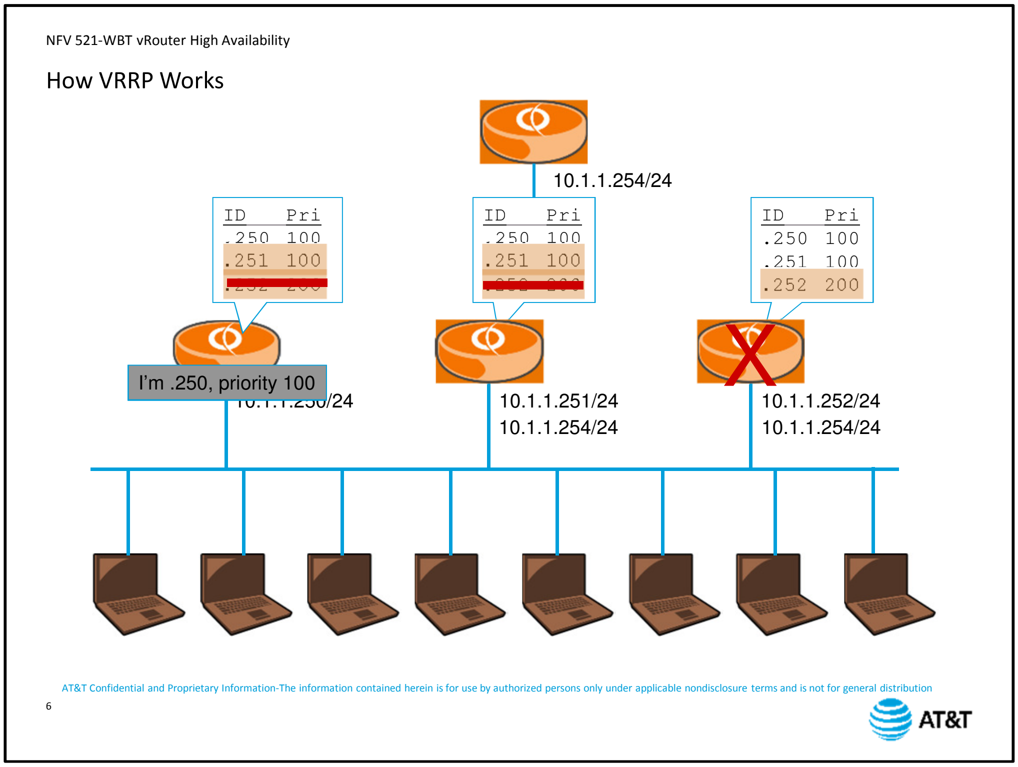
Backup routers provide redundancy, assuming master role if master router or interface fails

Industry standard – defined in RFC 2338 and 3678

5 AT&T Confidential and Proprietary Information-The information contained herein is for use by authorized persons only under applicable nondisclosure terms and is not for general distribution

AT&T

VRRP is an election protocol that selects one router out of a VRRP group to assume forwarding responsibilities. In other words, it is a protocol that allows multiple physical routers to share a single identity for traffic forwarding purposes.
End stations on the segment use this single identity, known as a Virtual Router, as their default gateway IP address.
The active router on the segment, also called the master, acts on packets sent to the IP address of the virtual router in addition to its own local IP address.
The other routers on the segment are not actively forwarding traffic for the virtual IP, but wait in backup mode. If the master fails, one of the backup routers will assume the forwarding responsibilities for the virtual router IP address.
VRRP is an industry standard redundancy protocol, defined in RFCs 2338 and 3678.



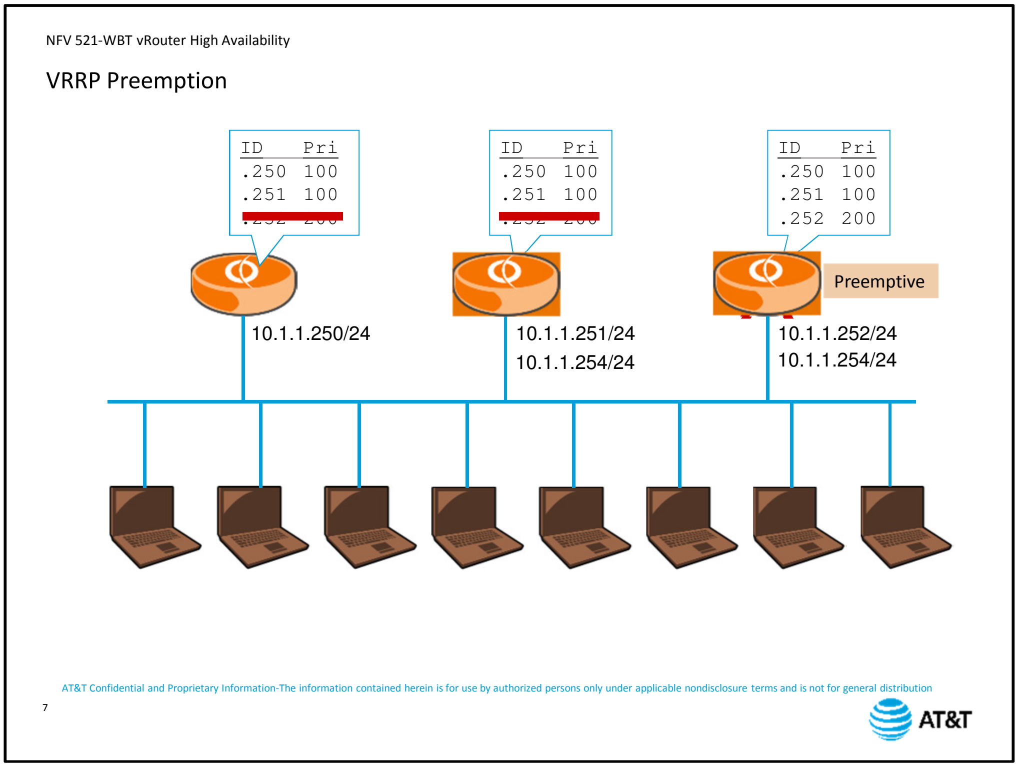
How VRRP Works

ID	Pri
.250	100
.251	100
~~.252~~	~~200~~

ID	Pri
.250	100
.251	100
~~.252~~	~~200~~

ID	Pri
.250	100
.251	100
.252	200

Let's look at an example of VRRP. In this network, we have three routers connected to the same network segment, and we want the three routers to provide redundancy for connectivity on this segment. We will make all three routers members of a VRRP group.
Next, we create a virtual router identity. This virtual router has its own IP address on the same subnet.
The routers then begin negotiating to determine which physical router is going to assume the virtual router identity. Each device sends a multicast VRRP packet containing its IP address and priority.
Each device builds a table of its VRRP neighbors and their priority.
The device with the highest priority becomes the master router,
and assumes the identity of the virtual router. All VRRP peers continue to send VRRP multicasts as keep-alives every second by default. As long as the master continues to send out VRRP packets, the other devices on the segment stay in backup mode, although they will handle traffic sent to their physical addresses.
If the master device stops sending VRRP packets for whatever reason – the device fails, the interface fails, or the configuration is removed
The remaining routers look for the next highest priority in the table.
If priority is equal, then the device with the highest IP address becomes the new master and takes over the virtual router functionality..



NFV 521-WBT vRouter High Availability

VRRP Preemption

ID	Pri
.250	100
.251	100
~~.252~~	~~200~~

ID	Pri
.250	100
.251	100
~~.252~~	~~200~~

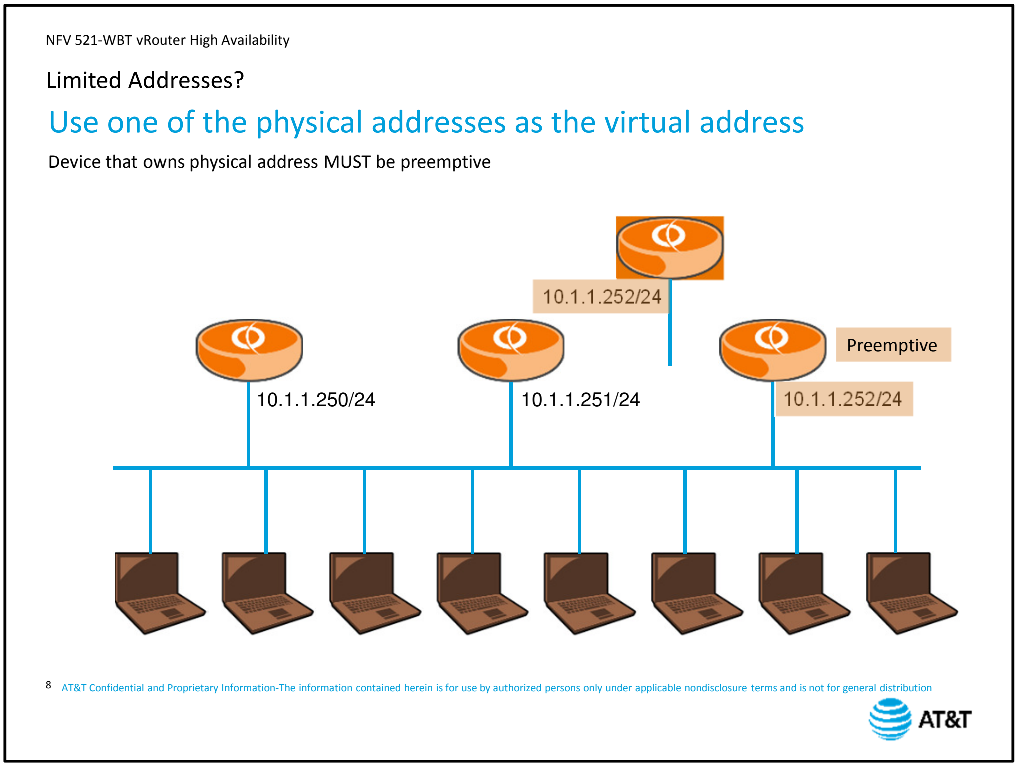
ID	Pri
.250	100
.251	100
.252	200

AT&T Confidential and Proprietary Information-The information contained herein is for use by authorized persons only under applicable nondisclosure terms and is not for general distribution

7

AT&T

By default, if a device is master, it will remain master,
even if a device with a higher priority appears, or in this case, re-appears on the network.
The high-priority device will only take over if the current master fails.
You can override this if you configure a device to be pre-emptive..
Now, when the router comes back online,
it will resume the master role. You may want to do this if the high-priority router has better performance than the other devices on the segment.



NFV 521-WBT vRouter High Availability

Limited Addresses?

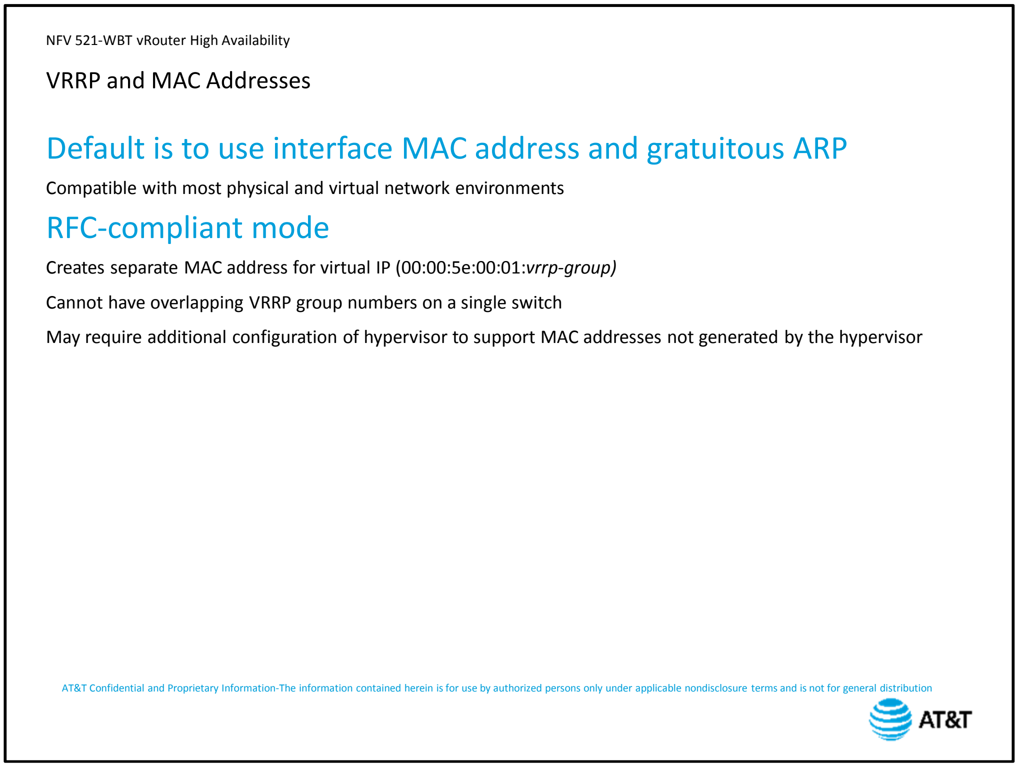
Use one of the physical addresses as the virtual address

Device that owns physical address MUST be preemptive

8 AT&T Confidential and Proprietary Information-The information contained herein is for use by authorized persons only under applicable nondisclosure terms and is not for general distribution

AT&T

If you have limited availability of addresses on a segment, you can configure the virtual router to use the same IP address as one of the physical routers on the segment.
If you do this, then the device that owns the physical address MUST be configured to be pre-emptive. Otherwise, you will wind up with an address conflict on the segment.



NFV 521-WBT vRouter High Availability

VRRP and MAC Addresses

Default is to use interface MAC address and gratuitous ARP

Compatible with most physical and virtual network environments

RFC-compliant mode

Creates separate MAC address for virtual IP (00:00:5e:00:01:*vrrp-group)*

Cannot have overlapping VRRP group numbers on a single switch

May require additional configuration of hypervisor to support MAC addresses not generated by the hypervisor

AT&T Confidential and Proprietary Information-The information contained herein is for use by authorized persons only under applicable nondisclosure terms and is not for general distribution

AT&T

By default, a vRouter uses its own MAC address in association with the virtual IP address for the VRRP group. Devices on the segment learn this MAC address through a gratuitous ARP process, which we will discuss on the next slide.

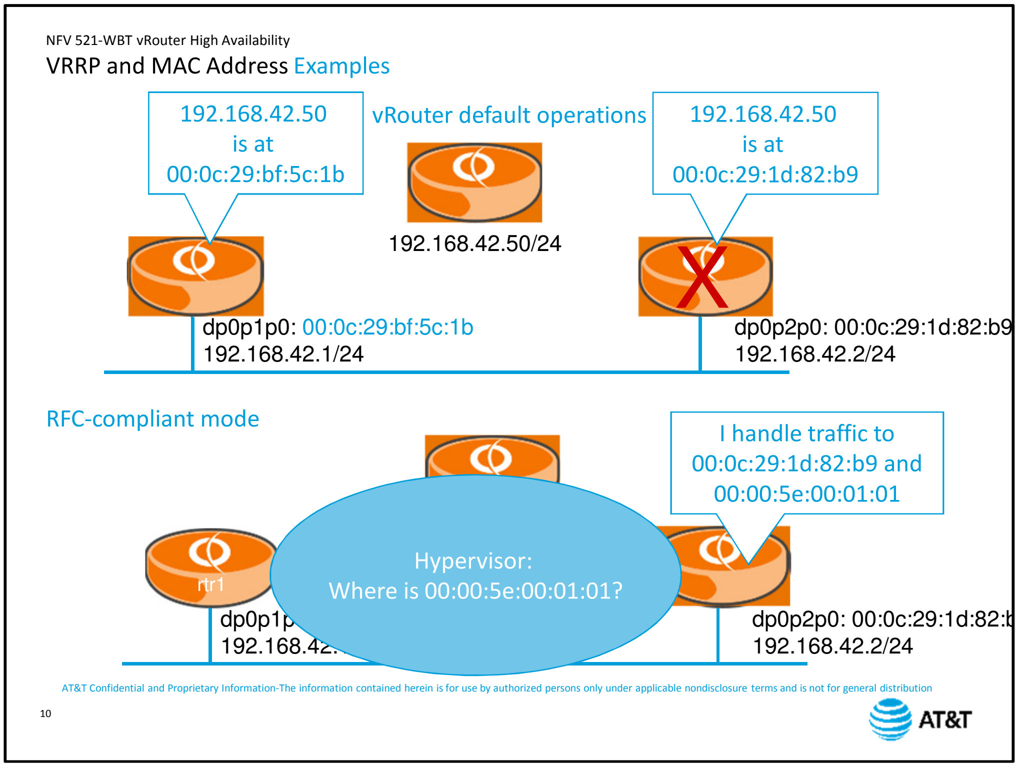
This operational mode is compatible with most physical and virtual network environments, but may cause some issues when used in conjunction with non-vRouter physical routers.

You can configure the vRouter to operate in RFC-compliant mode.

RFC 3768 defines a virtual MAC address to be used with VRRP. It always begins with 00:00:5E:00:01. The last octet is the VRRP group number, allowing for 255 separate VRRP groups on a single network segment.

Note that if you are using a shared switched environment, you need to plan your VRRP group numbers so that the same group number does not appear simultaneously on multiple switch ports.

While this mode allows for interoperation in multi-vendor router environments, it may cause problems in a virtual environment, depending on how your hypervisor learns MAC addresses.



NFV 521-WBT vRouter High Availability

VRRP and MAC Address Examples

AT&T Confidential and Proprietary Information-The information contained herein is for use by authorized persons only under applicable nondisclosure terms and is not for general distribution

10

AT&T

In default mode, the master router for the VRRP group sends out an ARP response message when it assumes the master role. This is called a gratuitous arp because we're sending a response even though we have not received an ARP request.

This ARP response says that the MAC address for the virtual IP is the MAC address of the vRouter itself.

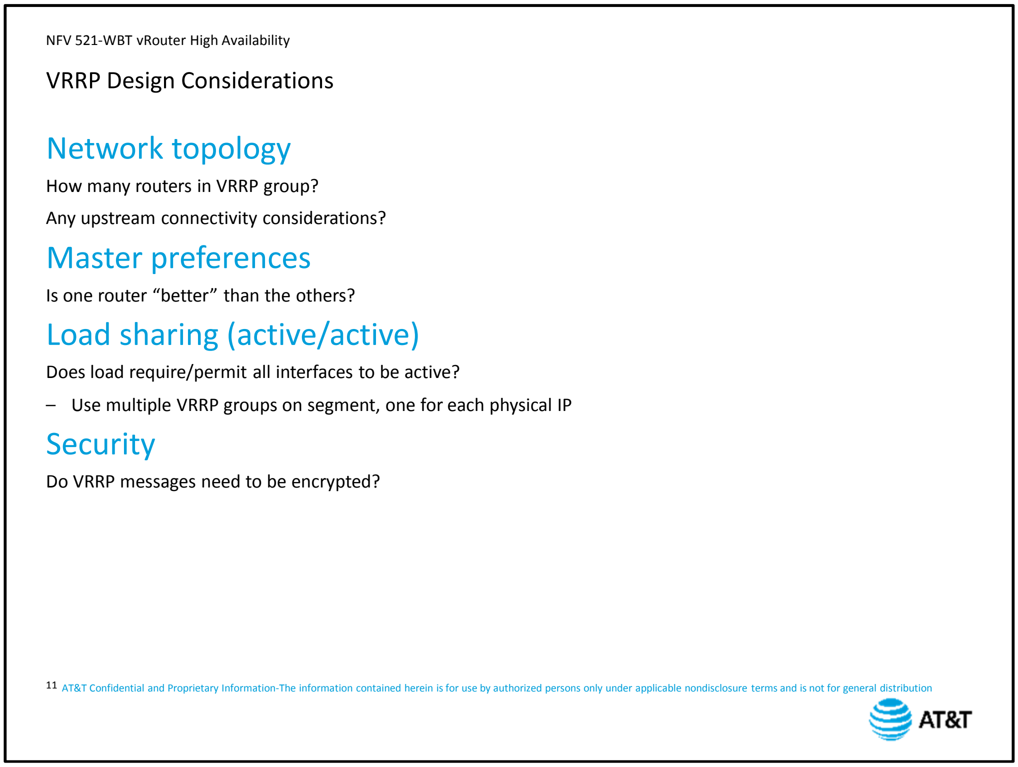
If the device fails, the new master takes over and sends out its own ARP response. Under normal IP operations, all devices on the segment are always listening for ARP responses in order to build their local ARP tables, so all devices will automatically update their own tables with the new MAC address.

In RFC compliant mode,

the virtual router has its own MAC address.

The master router will respond to traffic sent to both its locally-configured MAC address and the virtual MAC address for the VRRP group.

The problem in a virtual environment is that the underlying hypervisor software does not know what virtual machine is associated with the VRRP MAC address. It cannot process traffic to that MAC address, so it ignores it. If this problem occurs in your hypervisor, you will need to consult the hypervisor documentation for guidance on how to address this problem. The vRouter Knowledge Base can also provide information on specific hypervisor versions.



NFV 521-WBT vRouter High Availability

VRRP Design Considerations

Network topology

How many routers in VRRP group?

Any upstream connectivity considerations?

Master preferences

Is one router “better” than the others?

Load sharing (active/active)

Does load require/permit all interfaces to be active?

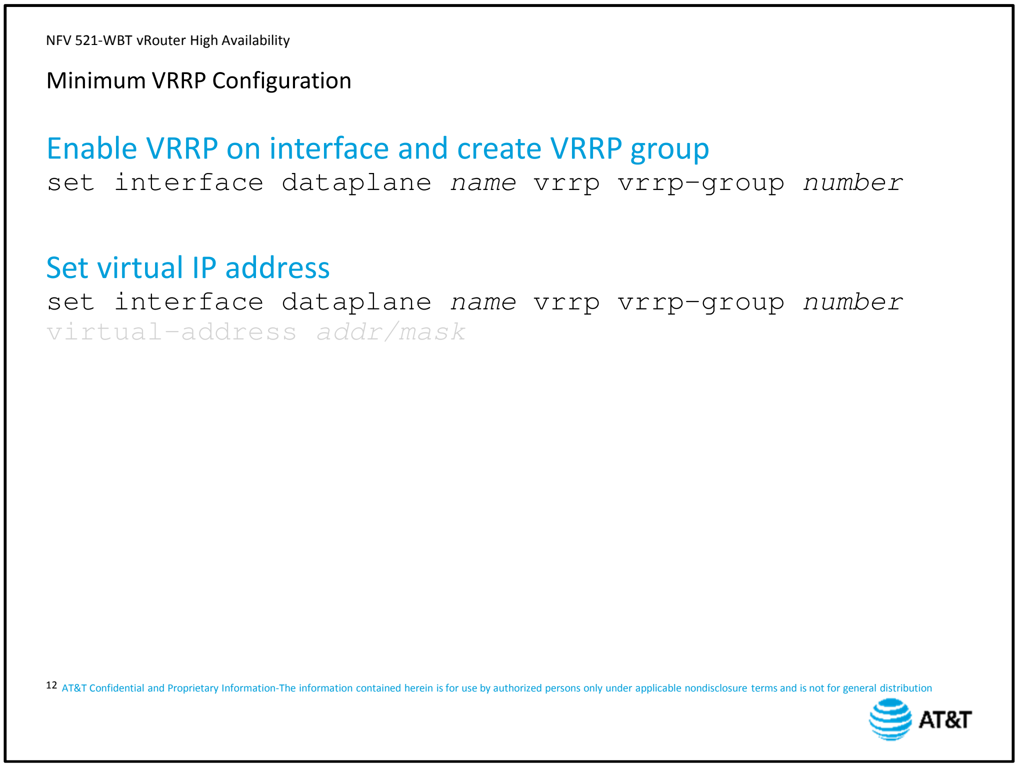
– Use multiple VRRP groups on segment, one for each physical IP

Security

Do VRRP messages need to be encrypted?

11 AT&T Confidential and Proprietary Information-The information contained herein is for use by authorized persons only under applicable nondisclosure terms and is not for general distribution

When you are planning your VRRP deployment, keep in mind the following:
First, consider your network topology.
How many routers are in your VRRP group? Remember, you have to explicitly configure VRRP on all routers.
Think about your upstream connectivity.
Next, think about whether you want to select one router to be master rather than leaving it to the VRRP protocol.
Is one router 'better' than another? Think about device performance as well as upstream bandwidth. You also need to decide whether you want to enable preemption so that the preferred device is the master whenever it's available.
Another consideration is whether or not you want load sharing, also known as an active/active configuration. By default, a VRRP group only has one active device per group.
Do you want to take advantage of all the available interfaces and use all of them under normal operations?
If so, you will need to configure multiple VRRP groups, one for each physical IP address. We will look at an example of this later.
Finally, consider security. VRRP messages are multicasts, which means any device on the segment can intercept the messages. Do you need to encrypt these messages in order to meet your network security requirements?



NFV 521-WBT vRouter High Availability

Minimum VRRP Configuration

Enable VRRP on interface and create VRRP group

```
set interface dataplane name vrrp vrrp-group number
```

Set virtual IP address

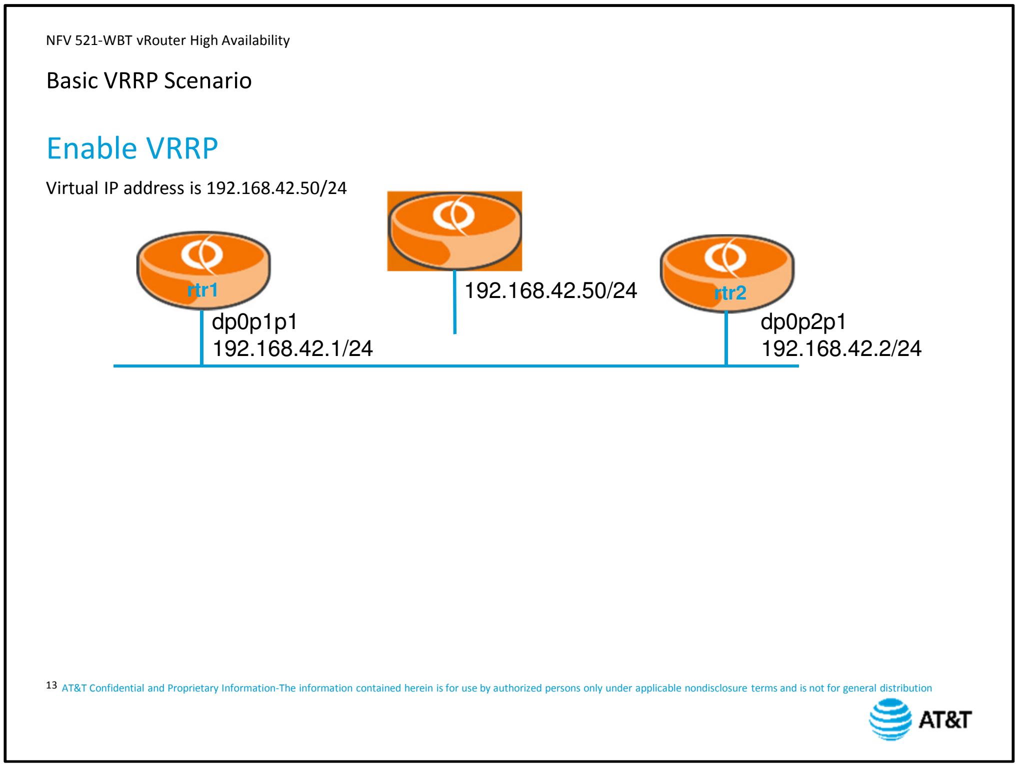
```
set interface dataplane name vrrp vrrp-group number
virtual-address addr/mask
```

12 AT&T Confidential and Proprietary Information-The information contained herein is for use by authorized persons only under applicable nondisclosure terms and is not for general distribution

AT&T

To configure VRRP, you first need to set up the VRRP group on the interface that is participating in VRRP. The group number must be set to the same value across all devices participating in the VRRP group.

Next, specify the virtual IP address. This address must be set to the same value on all members of the VRRP group.



NFV 521-WBT vRouter High Availability

Basic VRRP Scenario

Enable VRRP

Virtual IP address is 192.168.42.50/24

rtr1

dp0p1p1
192.168.42.1/24

192.168.42.50/24

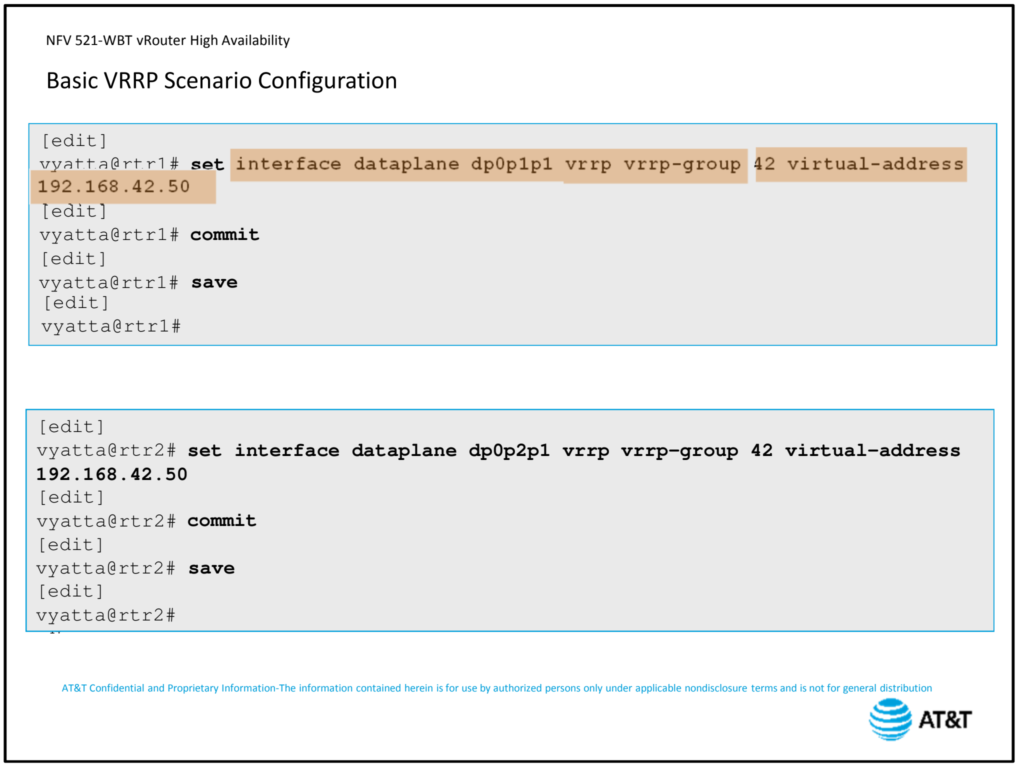
rtr2

dp0p2p1
192.168.42.2/24

13 AT&T Confidential and Proprietary Information-The information contained herein is for use by authorized persons only under applicable nondisclosure terms and is not for general distribution

AT&T

Let’s apply these commands to an example. In this scenario, we will enable VRRP on both routers.
The virtual IP address is 192.168.42.50.



NFV 521-WBT vRouter High Availability

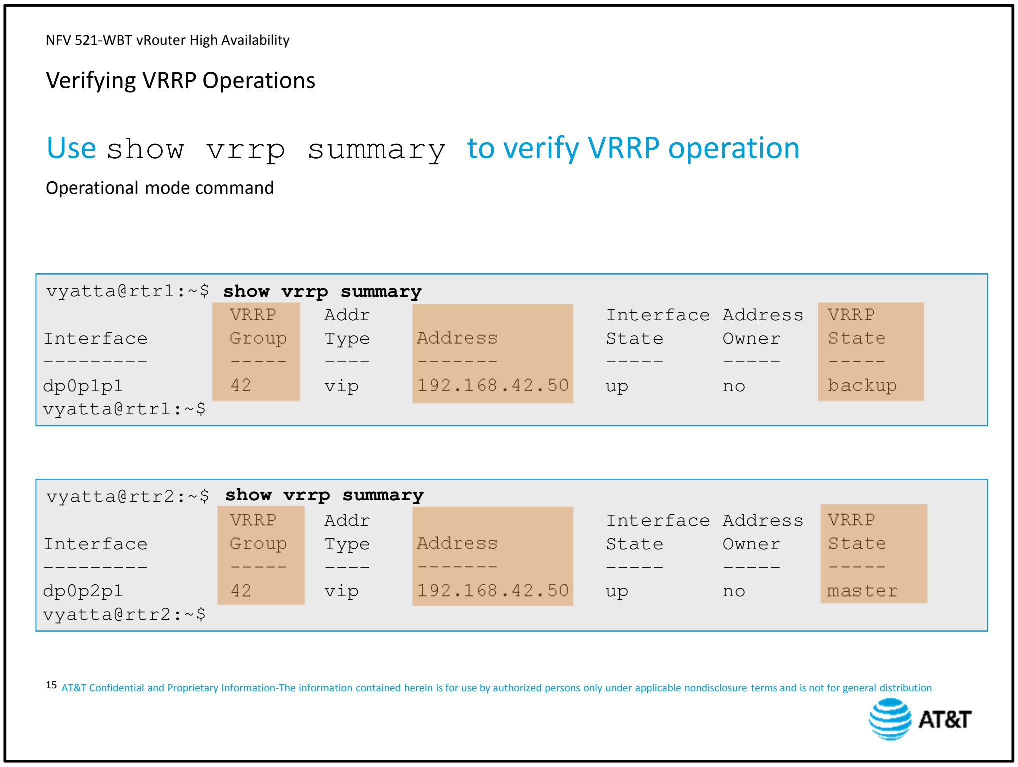
Basic VRRP Scenario Configuration

```
[edit]
vyatta@rtr1# set interface dataplane dp0p1p1 vrrp vrrp-group 42 virtual-address
192.168.42.50
[edit]
vyatta@rtr1# commit
[edit]
vyatta@rtr1# save
[edit]
vyatta@rtr1#
```

```
[edit]
vyatta@rtr2# set interface dataplane dp0p2p1 vrrp vrrp-group 42 virtual-address
192.168.42.50
[edit]
vyatta@rtr2# commit
[edit]
vyatta@rtr2# save
[edit]
vyatta@rtr2#
```

AT&T Confidential and Proprietary Information-The information contained herein is for use by authorized persons only under applicable nondisclosure terms and is not for general distribution

We can actually complete this configuration with a single set command on each device.
On router 1 (rtr1), we enter the `virtual-address` command. This accomplishes three things:
it sets up VRRP on dataplane interface 1,
it creates group 42,
and sets the virtual address for the VRRP group.
Next, we commit our changes to make them take effect, and save them so they become permanent.
We repeat the exact same command on router 2 (rtr2).



NFV 521-WBT vRouter High Availability

Verifying VRRP Operations

Use `show vrrp summary` to verify VRRP operation

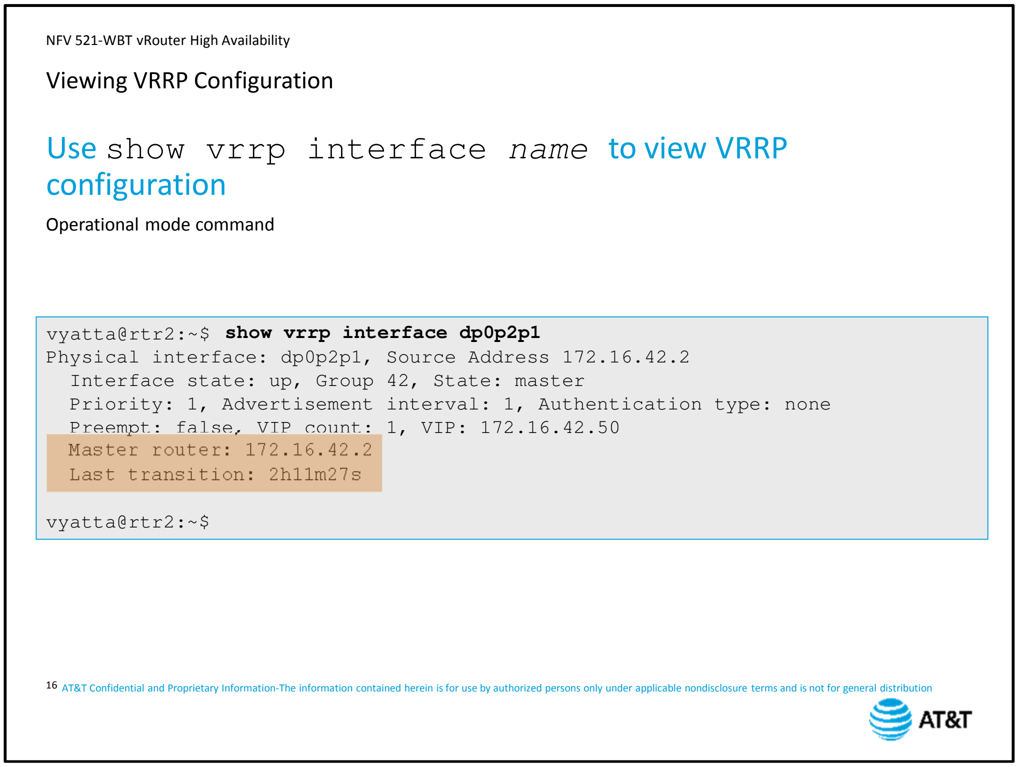
Operational mode command

```
vyatta@rtr1:~$ show vrrp summary
                VRRP    Addr                      Interface  Address  VRRP
Interface       Group   Type    Address           State      Owner    State
---------       -----   ----    -------           -----      -----    -----
dp0p1p1         42      vip     192.168.42.50     up         no       backup
vyatta@rtr1:~$
```

```
vyatta@rtr2:~$ show vrrp summary
                VRRP    Addr                      Interface  Address  VRRP
Interface       Group   Type    Address           State      Owner    State
---------       -----   ----    -------           -----      -----    -----
dp0p2p1         42      vip     192.168.42.50     up         no       master
vyatta@rtr2:~$
```

15 AT&T Confidential and Proprietary Information-The information contained herein is for use by authorized persons only under applicable nondisclosure terms and is not for general distribution

To verify that VRRP is working, use the command `show vrrp summary`.
We run this command on both rtr1
and rtr2.
We can see the VRRP group number,
the virtual address,
and the device state. In this case, rtr2 is the master. Because we did not set a priority, the device with the highest IP address became the master. If you refer back to the diagram, you will see that rtr2's address is higher than rtr1.



NFV 521-WBT vRouter High Availability

Viewing VRRP Configuration

Use `show vrrp interface` *`name`* to view VRRP configuration

Operational mode command

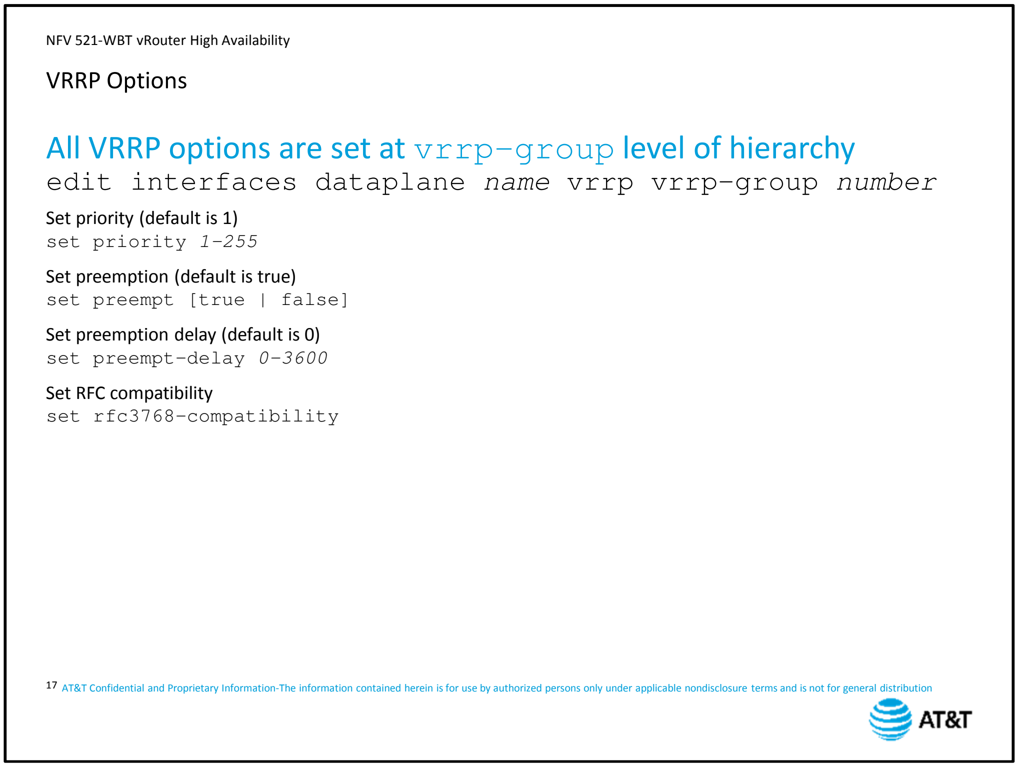
```
vyatta@rtr2:~$ show vrrp interface dp0p2p1
Physical interface: dp0p2p1, Source Address 172.16.42.2
  Interface state: up, Group 42, State: master
  Priority: 1, Advertisement interval: 1, Authentication type: none
  Preempt: false, VIP count: 1, VIP: 172.16.42.50
  Master router: 172.16.42.2
  Last transition: 2h11m27s

vyatta@rtr2:~$
```

16 AT&T Confidential and Proprietary Information-The information contained herein is for use by authorized persons only under applicable nondisclosure terms and is not for general distribution

If you do not have access to Configuration mode, you can still view the settings for VRRP with the command. `show vrrp interfaces dpxpypz.`

The output shows all the configuration settings, including options we will discuss on the next screen.

The last two lines of the output show you which device is the master router, and how long it has been since the last device failover.



NFV 521-WBT vRouter High Availability

VRRP Options

All VRRP options are set at `vrrp-group` level of hierarchy

```
edit interfaces dataplane name vrrp vrrp-group number
```

Set priority (default is 1)

```
set priority 1-255
```

Set preemption (default is true)

```
set preempt [true | false]
```

Set preemption delay (default is 0)

```
set preempt-delay 0-3600
```

Set RFC compatibility

```
set rfc3768-compatibility
```

17 AT&T Confidential and Proprietary Information-The information contained herein is for use by authorized persons only under applicable nondisclosure terms and is not for general distribution

AT&T

We have a few options we can set with VRRP that relate to preemption and failover.

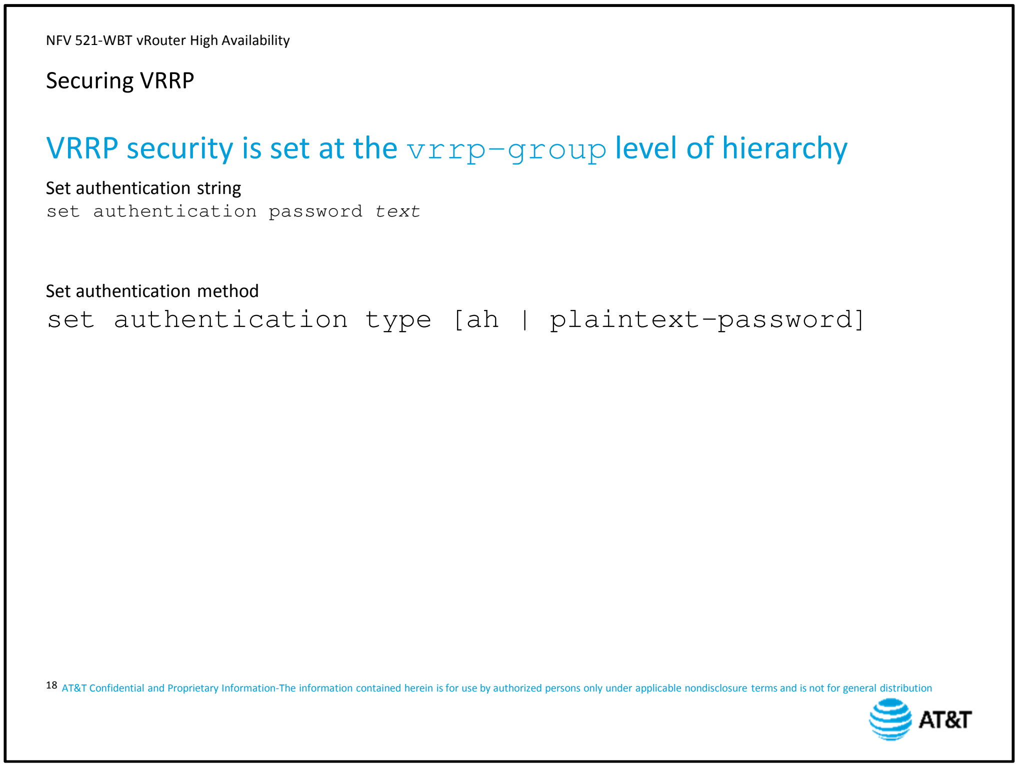
All of these options are set at the VRRP group level. In order to save some typing – and to prevent typing mistakes – we recommend using the `edit` command to move within the configuration hierarchy. The following commands assume that you are using the `edit` command.

To set the device priority, use the `set priority` command. Supported values for priority is 1 to 255. The higher the number, the more likely a device is going to be the master. The default priority on all vRouters is 1.

To enable preemption, configure `set preempt true`. The default is true. However, preempt requires that the priority be higher than the other devices in the VRRP group, so for preempt to be effective, you need to set the priority accordingly.

You can set a preemption delay, which can prevent flapping in an unstable environment. The interval is in seconds, and the default is 0. Setting an interval means the preempting router will wait for the configured interval before assuming the master role again.

You can also enable RFC compatibility mode.



NFV 521-WBT vRouter High Availability

Securing VRRP

VRRP security is set at the `vrrp-group` level of hierarchy

Set authentication string

```
set authentication password text
```

Set authentication method

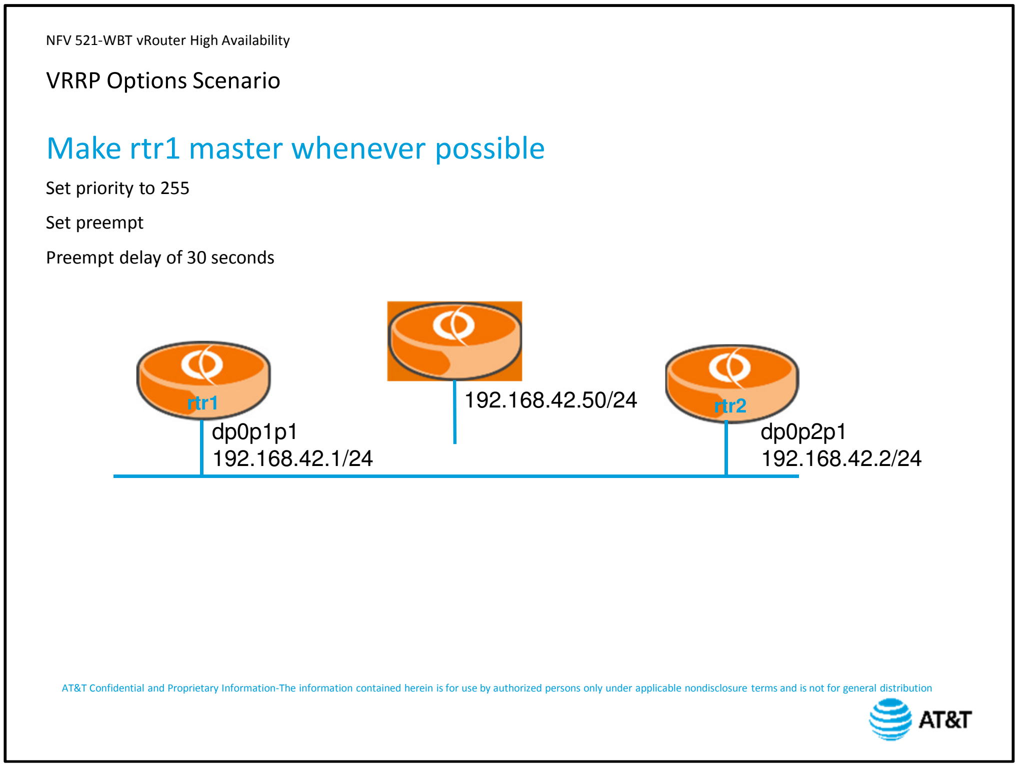
```
set authentication type [ah | plaintext-password]
```

18 AT&T Confidential and Proprietary Information-The information contained herein is for use by authorized persons only under applicable nondisclosure terms and is not for general distribution

You can secure VRRP exchanges by encrypting the VRRP messages. Again, these commands are set at the VRRP group level.

First, set the authentication string. This string must be configured on all devices in the group, and must be identical. The string is stored in clear-text in the configuration file, so is easily verified or recovered as needed.

Next, set the authentication method. AH uses the authentication header format as described in the IPsec standards. Simple uses the plain-text password rather than an encrypted string password.



NFV 521-WBT vRouter High Availability

VRRP Options Scenario

Make rtr1 master whenever possible

Set priority to 255

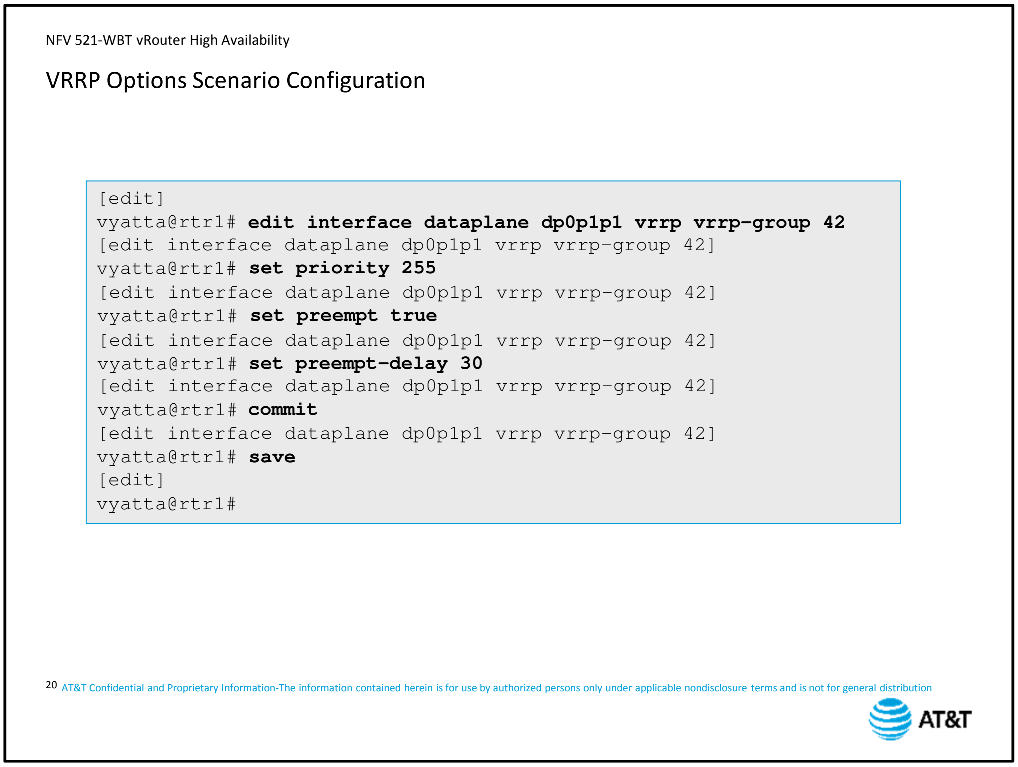
Set preempt

Preempt delay of 30 seconds

AT&T Confidential and Proprietary Information-The information contained herein is for use by authorized persons only under applicable nondisclosure terms and is not for general distribution

AT&T

Let’s add to our existing scenario and make rtr1 the master whenever possible – that is, whenever it is available.
We do this by adding to rtr1’s configuration, setting the priority to 255
and enabling preempt.
The default for preempt delay is 0 seconds; that is, the device becomes master as soon as it is available. To prevent flapping between rtr1 and rtr2 in an unstable environment, we set the preempt delay to 30 seconds.



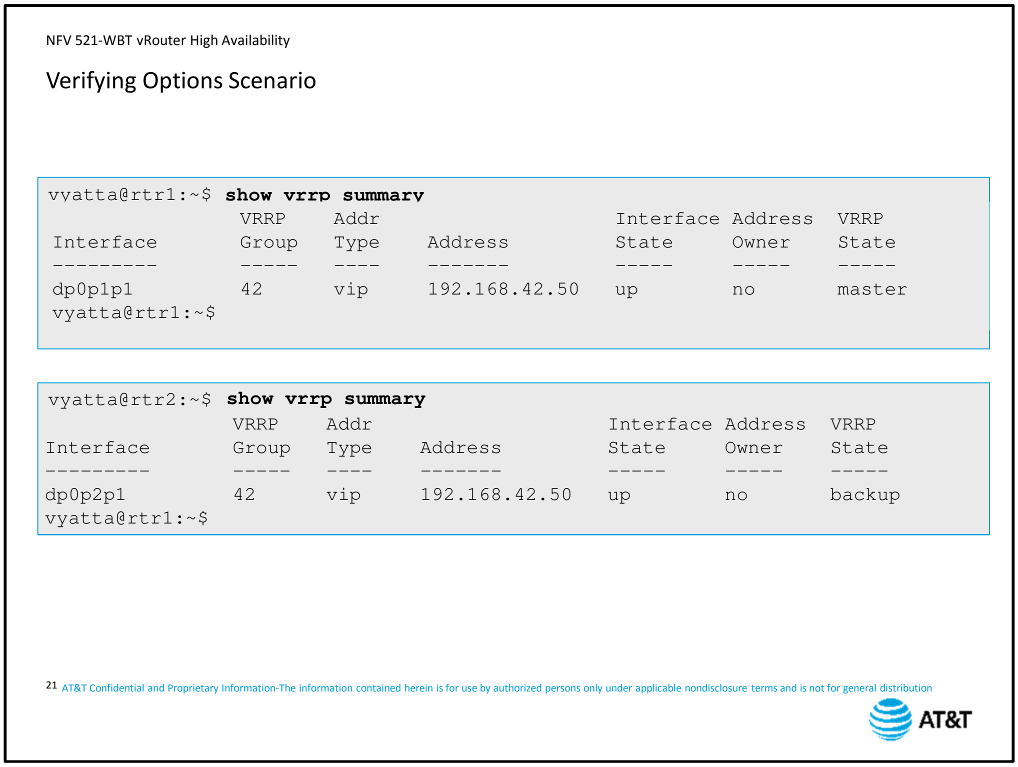
NFV 521-WBT vRouter High Availability

VRRP Options Scenario Configuration

```
[edit]
vyatta@rtr1# edit interface dataplane dp0p1p1 vrrp vrrp-group 42
[edit interface dataplane dp0p1p1 vrrp vrrp-group 42]
vyatta@rtr1# set priority 255
[edit interface dataplane dp0p1p1 vrrp vrrp-group 42]
vyatta@rtr1# set preempt true
[edit interface dataplane dp0p1p1 vrrp vrrp-group 42]
vyatta@rtr1# set preempt-delay 30
[edit interface dataplane dp0p1p1 vrrp vrrp-group 42]
vyatta@rtr1# commit
[edit interface dataplane dp0p1p1 vrrp vrrp-group 42]
vyatta@rtr1# save
[edit]
vyatta@rtr1#
```

20 AT&T Confidential and Proprietary Information-The information contained herein is for use by authorized persons only under applicable nondisclosure terms and is not for general distribution

We use the `edit` command to enter the VRRP group. Note the prompt changes to indicate where we are in the configuration hierarchy.
We set the priority and
set preempt to true
Then we set the preempt delay to 30 seconds.
We commit and save our changes.



NFV 521-WBT vRouter High Availability

Verifying Options Scenario

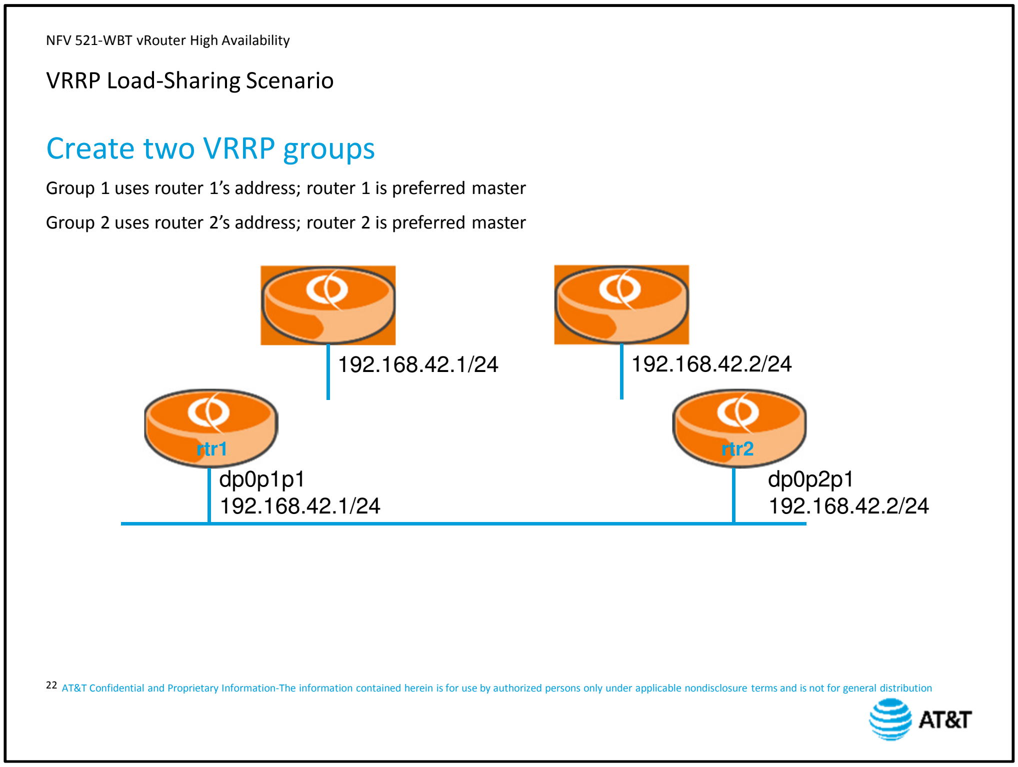
```
vyatta@rtr1:~$ show vrrp summary
                VRRP    Addr                    Interface Address  VRRP
Interface       Group   Type    Address         State     Owner    State
---------       -----   ----    -------         -----     -----    -----
dp0p1p1         42      vip     192.168.42.50   up        no       master
vyatta@rtr1:~$
```

```
vyatta@rtr2:~$ show vrrp summary
                VRRP    Addr                    Interface Address  VRRP
Interface       Group   Type    Address         State     Owner    State
---------       -----   ----    -------         -----     -----    -----
dp0p2p1         42      vip     192.168.42.50   up        no       backup
vyatta@rtr1:~$
```

21 AT&T Confidential and Proprietary Information-The information contained herein is for use by authorized persons only under applicable nondisclosure terms and is not for general distribution

AT&T

When we look at the summary now, we see that rtr1 is now the master.



NFV 521-WBT vRouter High Availability

VRRP Load-Sharing Scenario

Create two VRRP groups

Group 1 uses router 1’s address; router 1 is preferred master

Group 2 uses router 2’s address; router 2 is preferred master

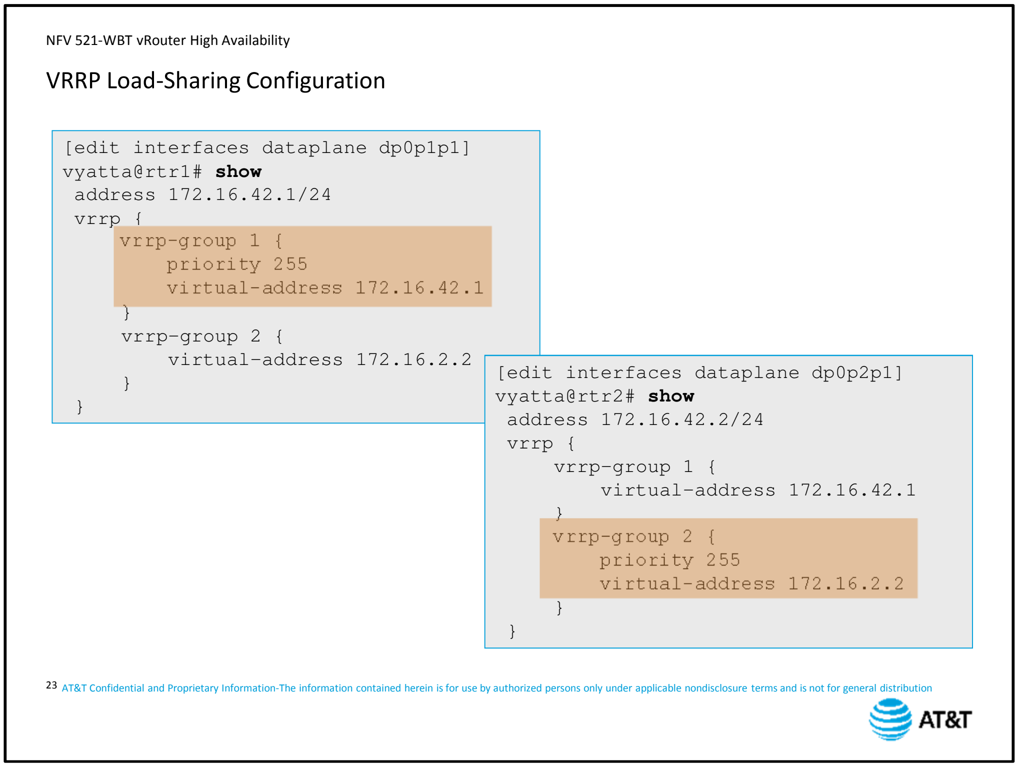
22 AT&T Confidential and Proprietary Information-The information contained herein is for use by authorized persons only under applicable nondisclosure terms and is not for general distribution

As we mentioned earlier, you can set up load sharing, also known as an active/active configuration. Under normal operations, both devices will be operational, but if one fails, the other will take over operations.

To configure load sharing, create two VRRP groups.

Group 1 is configured so that rtr1 is the preferred master and uses rtr1’s physical address

Group 2 is configured so that rtr2 is the preferred master and uses rtr2’s physical address



NFV 521-WBT vRouter High Availability

VRRP Load-Sharing Configuration

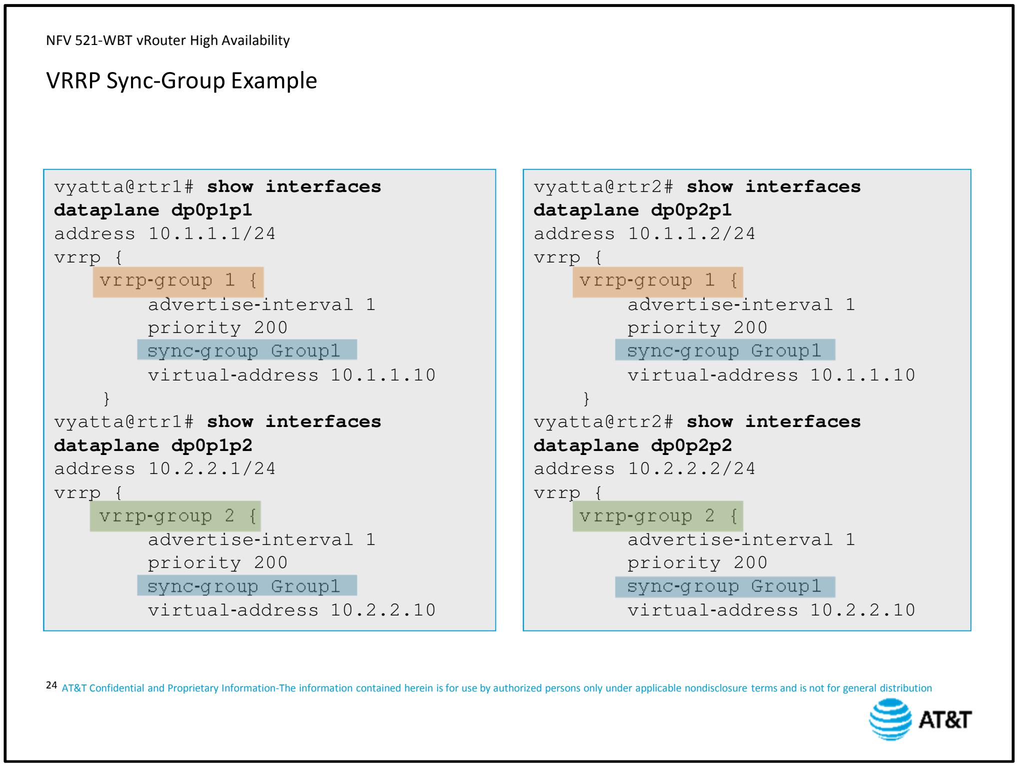
```
[edit interfaces dataplane dp0p1p1]
vyatta@rtr1# show
 address 172.16.42.1/24
 vrrp {
     vrrp-group 1 {
         priority 255
         virtual-address 172.16.42.1
     }
     vrrp-group 2 {
         virtual-address 172.16.2.2
     }
 }
```

```
[edit interfaces dataplane dp0p2p1]
vyatta@rtr2# show
 address 172.16.42.2/24
 vrrp {
     vrrp-group 1 {
         virtual-address 172.16.42.1
     }
     vrrp-group 2 {
         priority 255
         virtual-address 172.16.2.2
     }
 }
```

23 AT&T Confidential and Proprietary Information-The information contained herein is for use by authorized persons only under applicable nondisclosure terms and is not for general distribution

AT&T

When we look at the configurations for both devices,
We see that rtr1 has a higher priority for vrrp-group 1,
and rtr2 has higher priority for vrrp-group 2. Because *preempt true* is the default value, it is not included in the show output.



NFV 521-WBT vRouter High Availability

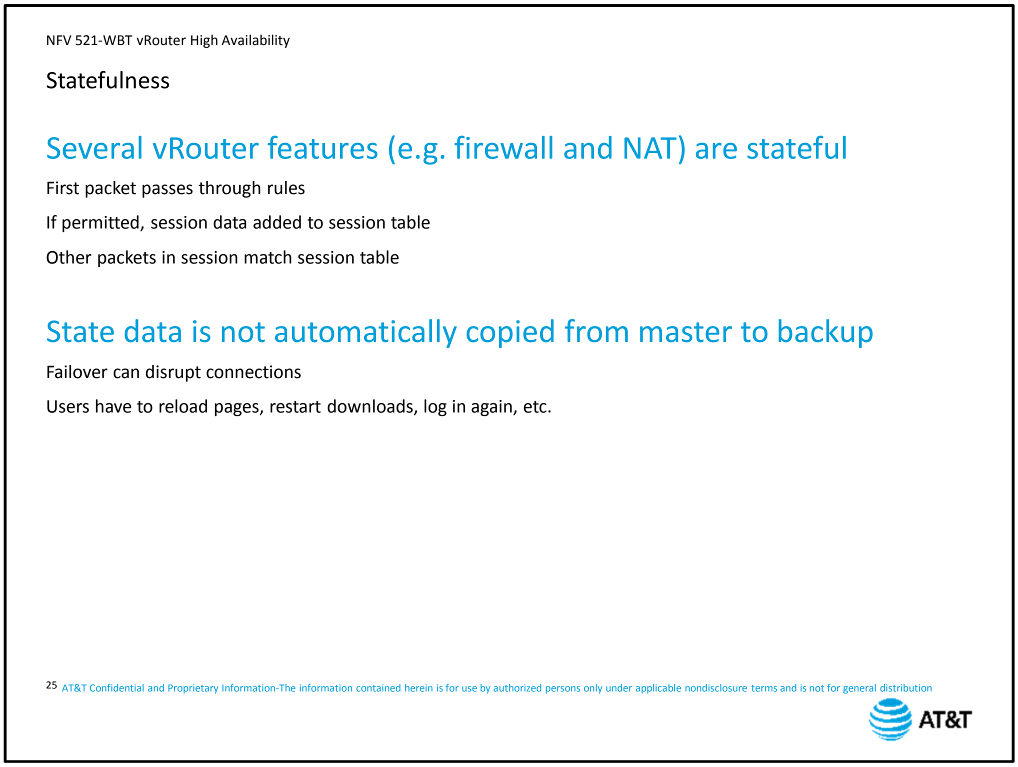
VRRP Sync-Group Example

```
vyatta@rtr1# show interfaces
dataplane dp0p1p1
address 10.1.1.1/24
vrrp {
    vrrp-group 1 {
        advertise-interval 1
        priority 200
        sync-group Group1
        virtual-address 10.1.1.10
    }
vyatta@rtr1# show interfaces
dataplane dp0p1p2
address 10.2.2.1/24
vrrp {
    vrrp-group 2 {
        advertise-interval 1
        priority 200
        sync-group Group1
        virtual-address 10.2.2.10
```

```
vyatta@rtr2# show interfaces
dataplane dp0p2p1
address 10.1.1.2/24
vrrp {
    vrrp-group 1 {
        advertise-interval 1
        priority 200
        sync-group Group1
        virtual-address 10.1.1.10
    }
vyatta@rtr2# show interfaces
dataplane dp0p2p2
address 10.2.2.2/24
vrrp {
    vrrp-group 2 {
        advertise-interval 1
        priority 200
        sync-group Group1
        virtual-address 10.2.2.10
```

24 AT&T Confidential and Proprietary Information-The information contained herein is for use by authorized persons only under applicable nondisclosure terms and is not for general distribution

This slide shows the configuration commands for the scenario shown on the previous screen.
Note that although each interface has its own VRRP group number,
they are both in the same sync group.



NFV 521-WBT vRouter High Availability

Statefulness

Several vRouter features (e.g. firewall and NAT) are stateful

First packet passes through rules

If permitted, session data added to session table

Other packets in session match session table

State data is not automatically copied from master to backup

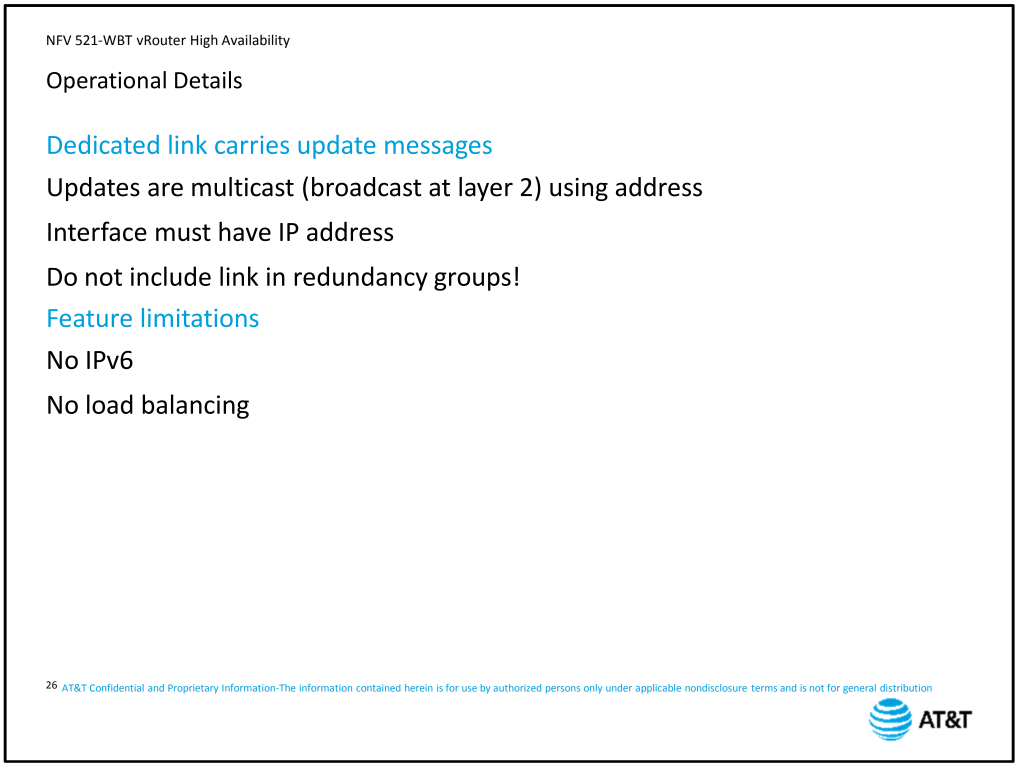
Failover can disrupt connections

Users have to reload pages, restart downloads, log in again, etc.

25 AT&T Confidential and Proprietary Information-The information contained herein is for use by authorized persons only under applicable nondisclosure terms and is not for general distribution

AT&T

vRouter has several features that operate as stateful services. This means that the device tracks information about sessions between devices, and not just individual packets.
In a stateful operation, the first packet in a session passes through the rules associated with the firewall and with NAT.
If the rules permit the traffic, the device not only passes the traffic, but adds information about the session to its session table, including translation data.
All other packets in the session match the entry in the session table and are permitted without having to look at the rules again.
However, statefulness can cause problems in a redundant environment. Session state data is not automatically copied from the master device to the backup device. This means that, although your network itself is redundant,
Individual users may experience connectivity loss if a redundant group fails over.
Users may have to reload pages, restart downloads, or even reinitiate their connections.



NFV 521-WBT vRouter High Availability

Operational Details

Dedicated link carries update messages

Updates are multicast (broadcast at layer 2) using address

Interface must have IP address

Do not include link in redundancy groups!

Feature limitations

No IPv6

No load balancing

26 AT&T Confidential and Proprietary Information-The information contained herein is for use by authorized persons only under applicable nondisclosure terms and is not for general distribution

As we mentioned in the previous slide, stateful redundancy requires a dedicated link between the two vRouters.

The update information is sent between the devices using multicast. One reason to use a dedicated link is that multicasts are Layer 2 broadcasts, and we want to prevent loading the in-band network with administrative overhead.

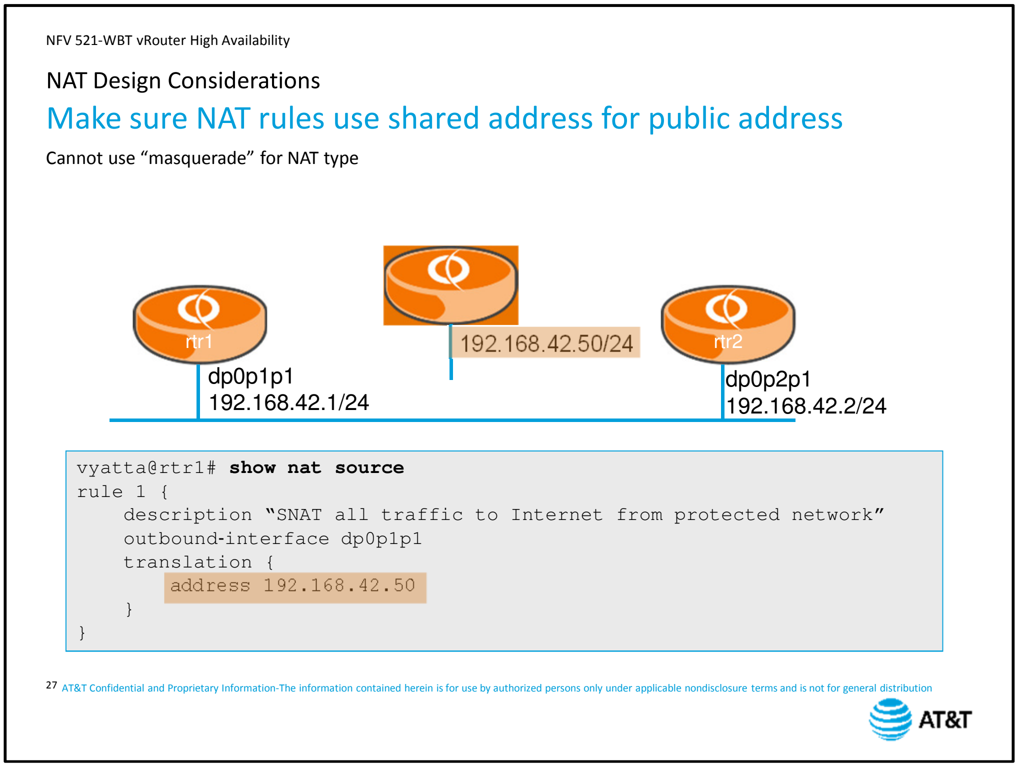
You will have to configure the link with an IP address in order to receive and send the required multicast messages.

Because this link is out-of-band, it should not be included directly in the VRRP configuration. You want your redundancy solution to monitor your in-band networks and not fail over if the out-of-band administrative link fails.

Some stateful features are not supported by Connntrack synchronization.

IP version 6 support is not currently supported.

And load balancing, which uses the Conntrack table to balance load, cannot operate simultaneously with stateful failover.



NFV 521-WBT vRouter High Availability

NAT Design Considerations

Make sure NAT rules use shared address for public address

Cannot use “masquerade” for NAT type

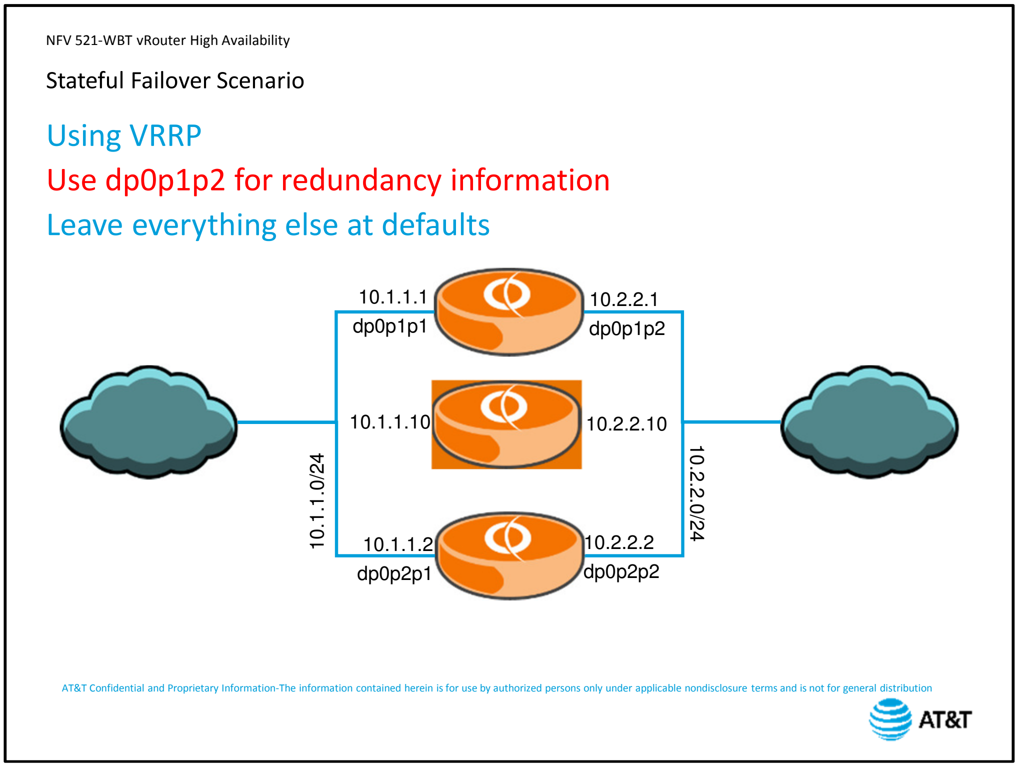
rtr1
dp0p1p1
192.168.42.1/24
192.168.42.50/24
rtr2
dp0p2p1
192.168.42.2/24

```
vyatta@rtr1# show nat source
rule 1 {
    description “SNAT all traffic to Internet from protected network”
    outbound-interface dp0p1p1
    translation {
        address 192.168.42.50
    }
}
```

27 AT&T Confidential and Proprietary Information-The information contained herein is for use by authorized persons only under applicable nondisclosure terms and is not for general distribution

AT&T

If you are using stateful failover with NAT, make sure your NAT configuration uses the shared address for translation, not an individual interface address – unless the interface address IS the shared address.
Also note that you cannot use “masquerade” as the NAT type; you need to specify either source or destination, which requires you to explicitly identify the addresses used in translation.
In this example, the shared address is 192.168.42.50, which is configured as the outside address for source NAT.



NFV 521-WBT vRouter High Availability

Stateful Failover Scenario

Using VRRP

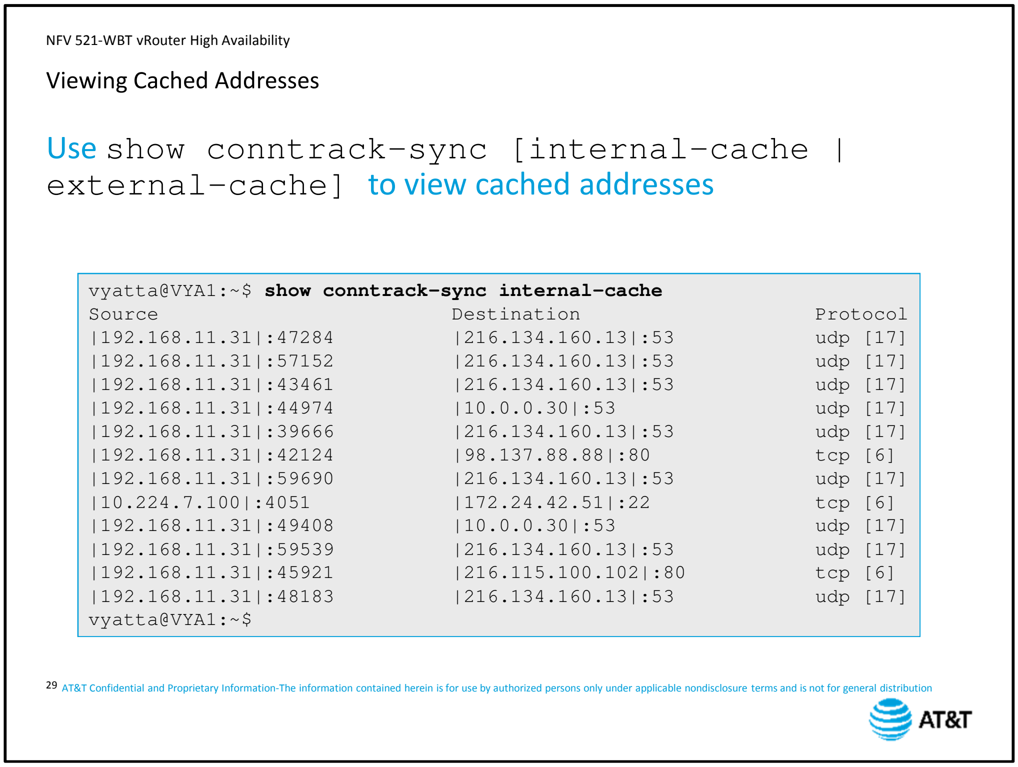
Use dp0p1p2 for redundancy information

Leave everything else at defaults

AT&T Confidential and Proprietary Information-The information contained herein is for use by authorized persons only under applicable nondisclosure terms and is not for general distribution

AT&T

In this scenario, we are expanding on the VRRP multiple interfaces scenario from earlier in the course.
We dedicate dataplane interface 2 for exchanging the redundancy data.
And we will not modify any of the stateful failover defaults



NFV 521-WBT vRouter High Availability

Viewing Cached Addresses

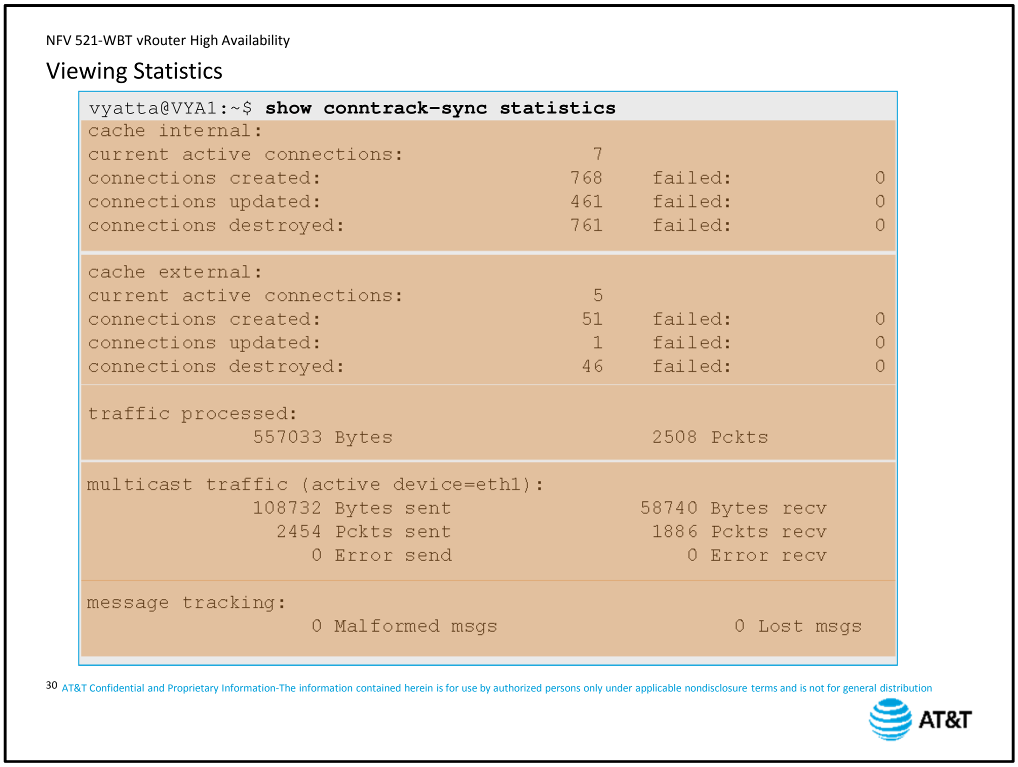
Use `show conntrack-sync [internal-cache | external-cache]` to view cached addresses

```
vyatta@VYA1:~$ show conntrack-sync internal-cache
Source                          Destination                     Protocol
|192.168.11.31|:47284           |216.134.160.13|:53             udp [17]
|192.168.11.31|:57152           |216.134.160.13|:53             udp [17]
|192.168.11.31|:43461           |216.134.160.13|:53             udp [17]
|192.168.11.31|:44974           |10.0.0.30|:53                  udp [17]
|192.168.11.31|:39666           |216.134.160.13|:53             udp [17]
|192.168.11.31|:42124           |98.137.88.88|:80               tcp [6]
|192.168.11.31|:59690           |216.134.160.13|:53             udp [17]
|10.224.7.100|:4051             |172.24.42.51|:22               tcp [6]
|192.168.11.31|:49408           |10.0.0.30|:53                  udp [17]
|192.168.11.31|:59539           |216.134.160.13|:53             udp [17]
|192.168.11.31|:45921           |216.115.100.102|:80            tcp [6]
|192.168.11.31|:48183           |216.134.160.13|:53             udp [17]
vyatta@VYA1:~$
```

29 AT&T Confidential and Proprietary Information-The information contained herein is for use by authorized persons only under applicable nondisclosure terms and is not for general distribution

AT&T

You can view the actual cached entries using the `show conntrack-sync internal-cache` and `external-cache` command. The output displays source and destination address and port, as well as protocol information.



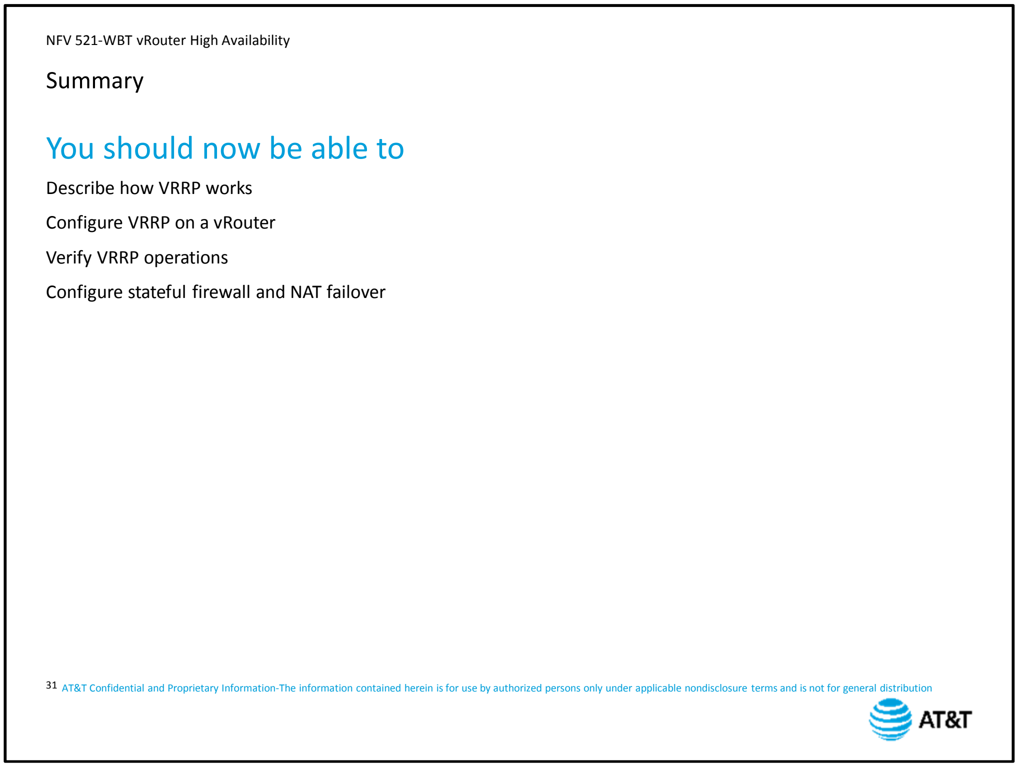
NFV 521-WBT vRouter High Availability

Viewing Statistics

```
vyatta@VYA1:~$ show conntrack-sync statistics
cache internal:
current active connections:                7
connections created:                     768    failed:            0
connections updated:                     461    failed:            0
connections destroyed:                   761    failed:            0

cache external:
current active connections:                5
connections created:                      51    failed:            0
connections updated:                       1    failed:            0
connections destroyed:                    46    failed:            0

traffic processed:
              557033 Bytes                      2508 Pckts

multicast traffic (active device=eth1):
              108732 Bytes sent                58740 Bytes recv
                2454 Pckts sent                 1886 Pckts recv
                   0 Error send                    0 Error recv

message tracking:
                   0 Malformed msgs                     0 Lost msgs
```

30 AT&T Confidential and Proprietary Information-The information contained herein is for use by authorized persons only under applicable nondisclosure terms and is not for general distribution

Finally, you can view detailed statistics using the `show conntrack sync statistics` command.
The output includes
internal cache activity,
external cache activity,
overall throughput,
details on multicast operations for exchanging cache data,
and message tracking counters.



NFV 521-WBT vRouter High Availability

Summary

You should now be able to

Describe how VRRP works

Configure VRRP on a vRouter

Verify VRRP operations

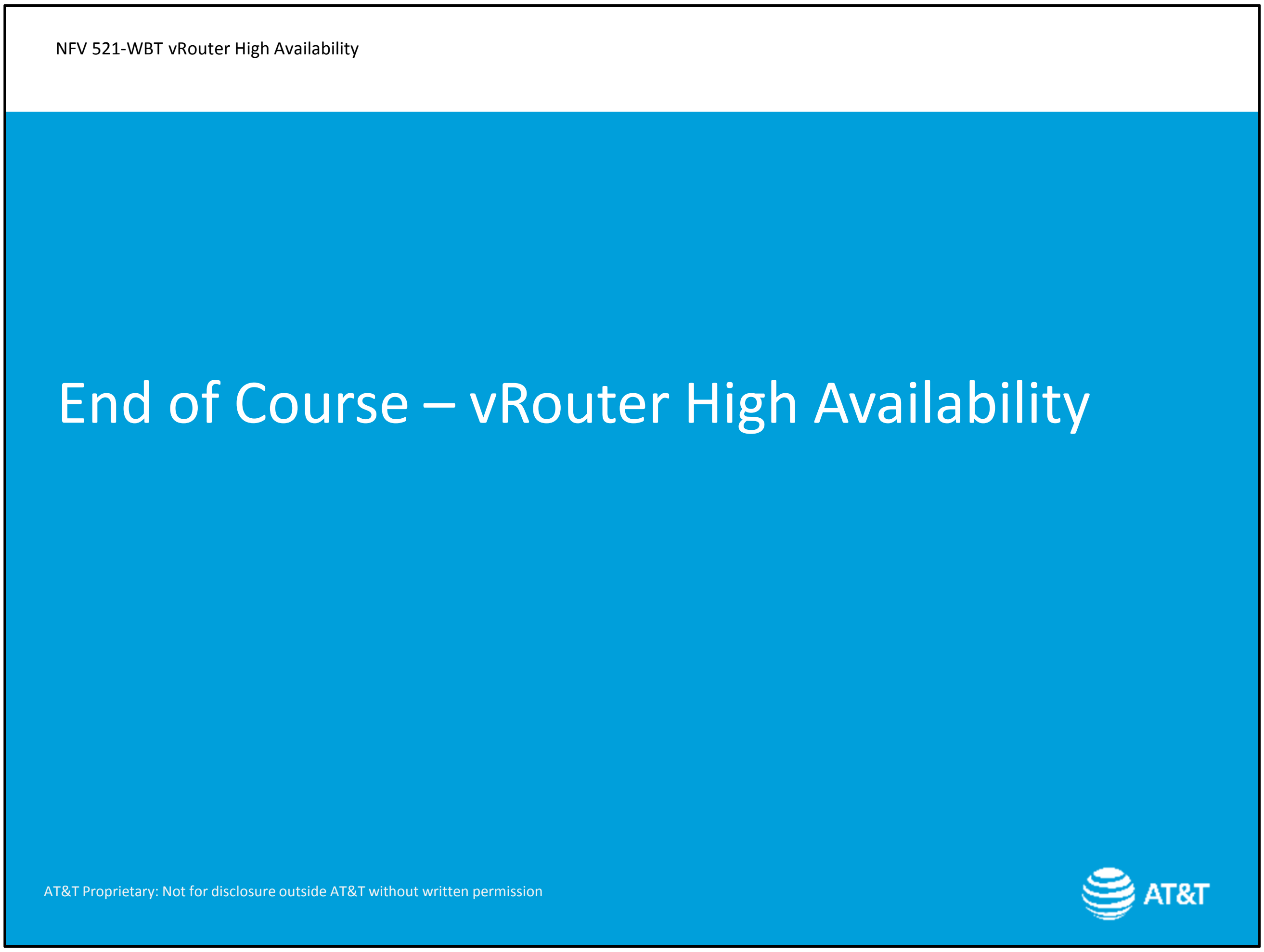
Configure stateful firewall and NAT failover

31 AT&T Confidential and Proprietary Information-The information contained herein is for use by authorized persons only under applicable nondisclosure terms and is not for general distribution

Congratulations! You have completed the AT&T vRouter High Availability course.
You should now be able to:

- Describe how VRRP works
- Configure VRRP on a vRouter
- Verify VRRP operations
- Configure stateful firewall and NAT failover

We hope that this course has been useful, and that you will take additional AT&T University courses in the future.



NFV 521-WBT vRouter High Availability

End of Course – vRouter High Availability

AT&T Proprietary: Not for disclosure outside AT&T without written permission