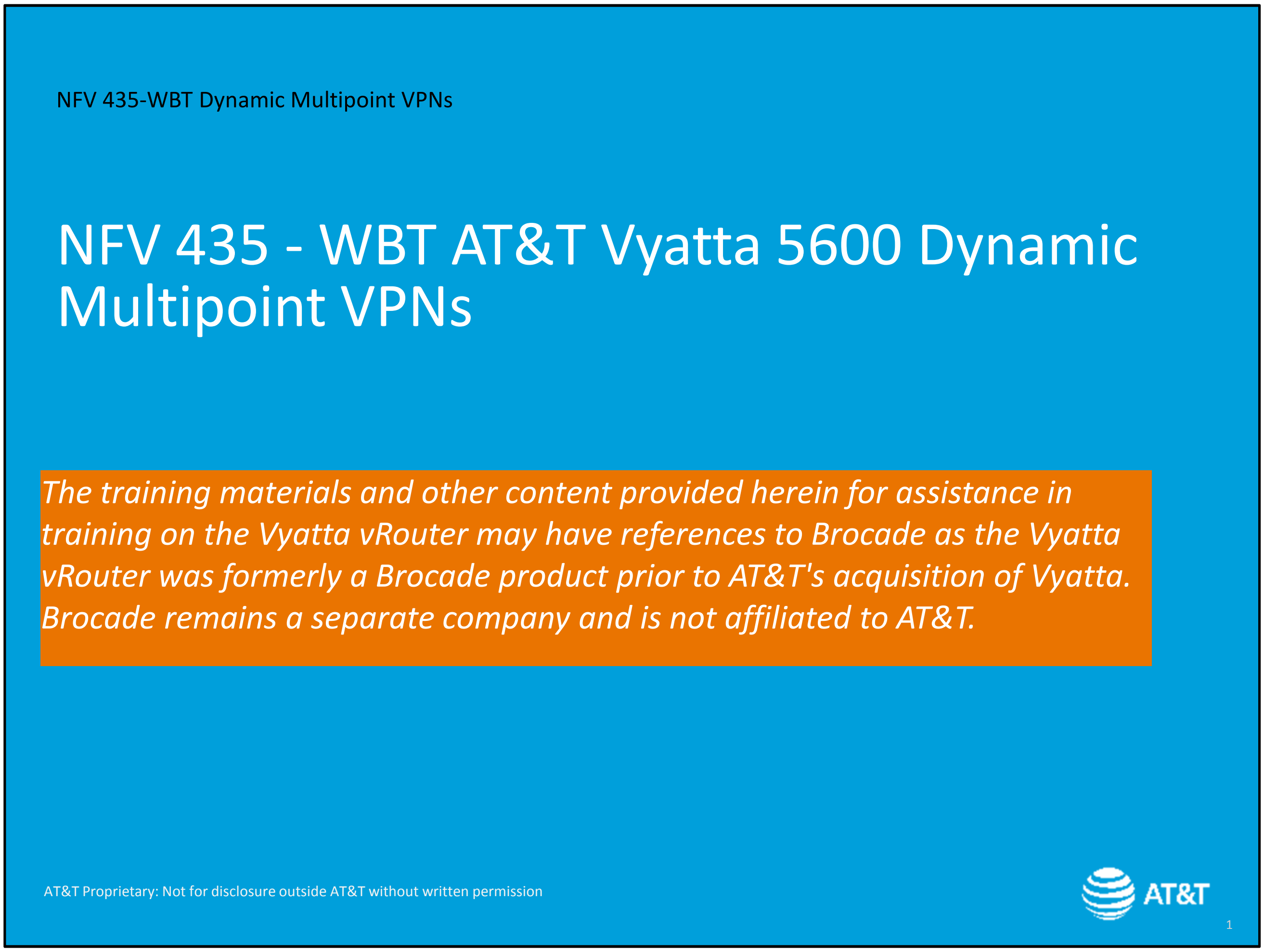


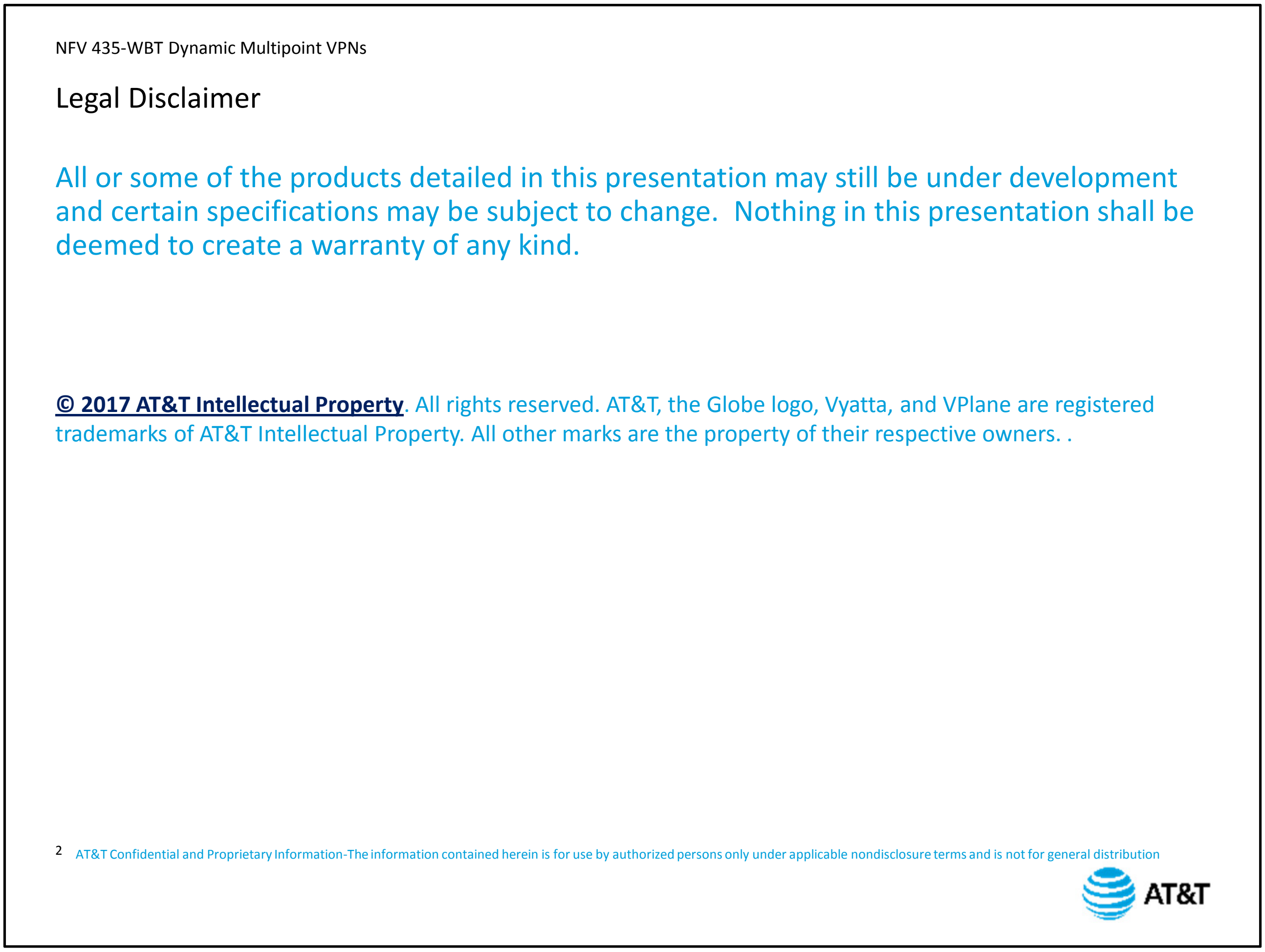
NFV 435-WBT Dynamic Multipoint VPNs

NFV 435 - WBT AT&T Vyatta 5600 Dynamic Multipoint VPNs

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

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

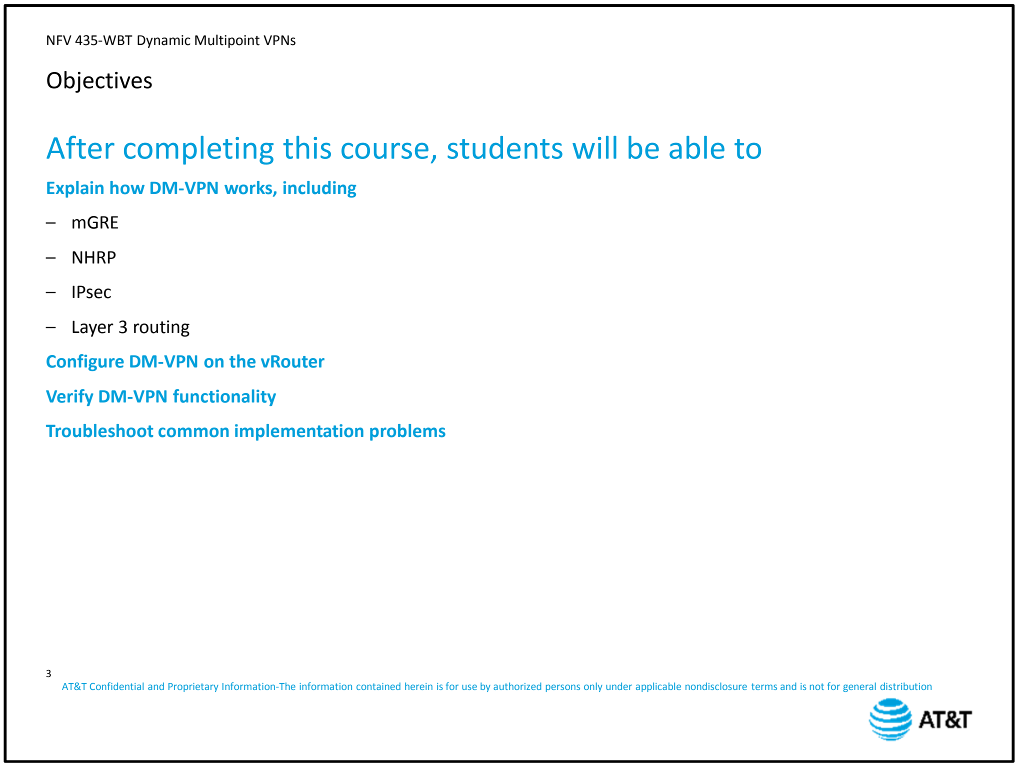


NFV 435-WBT Dynamic Multipoint VPNs

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 435-WBT Dynamic Multipoint VPNs

Objectives

After completing this course, students will be able to

Explain how DM-VPN works, including

– mGRE

– NHRP

– IPsec

– Layer 3 routing

Configure DM-VPN on the vRouter

Verify DM-VPN functionality

Troubleshoot common implementation problems

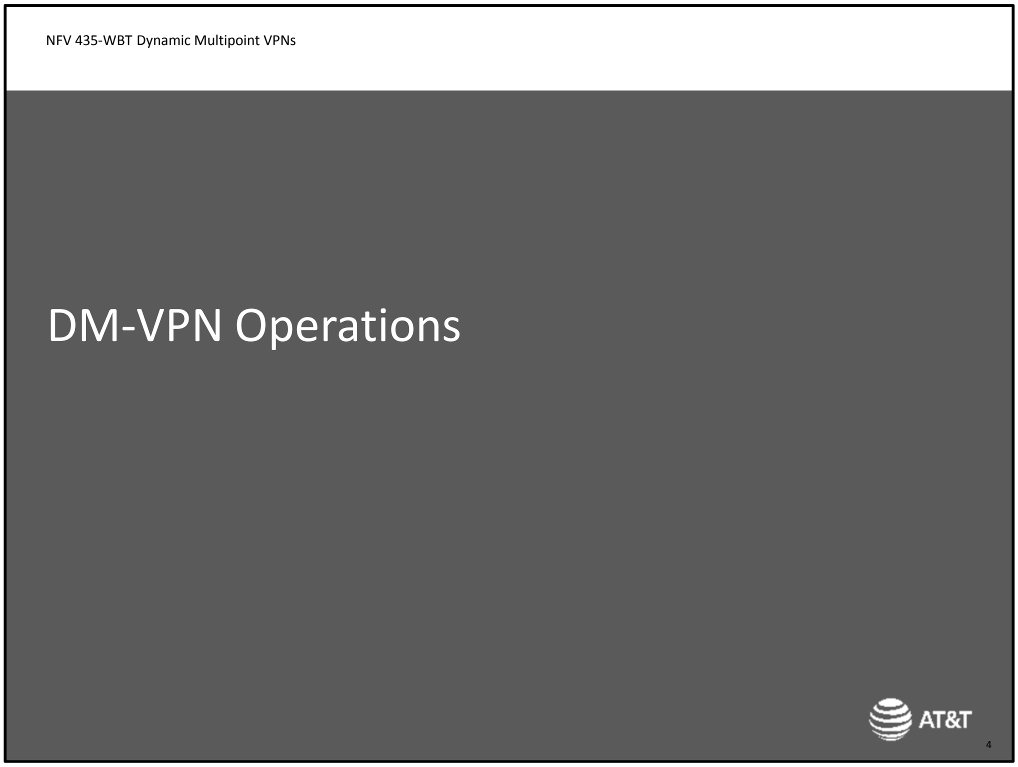
3

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

AT&T

After completing this course, students will be able to:

- Explain how Dynamic Multipoint VPNs (DM-VPN) incorporate the following protocols: Multipoint GRE, NHRP, IPsec, and Layer 3 routing.
- Configure DM-VPNs on the vRouter
- Verify DM-VPN functionality
- Troubleshoot common implementation problems

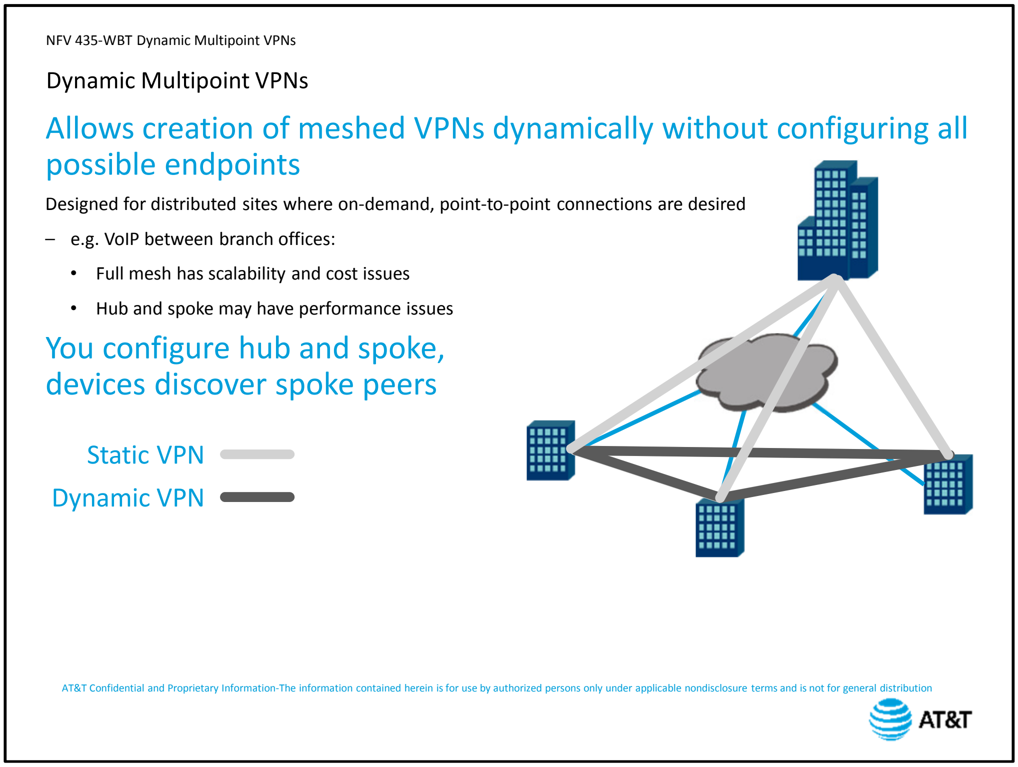


NFV 435-WBT Dynamic Multipoint VPNs

DM-VPN Operations

4

We’ll begin with an overview of Dynamic Multipoint VPN operations.



NFV 435-WBT Dynamic Multipoint VPNs

Dynamic Multipoint VPNs

Allows creation of meshed VPNs dynamically without configuring all possible endpoints

Designed for distributed sites where on-demand, point-to-point connections are desired

– e.g. VoIP between branch offices:
  - Full mesh has scalability and cost issues
  - Hub and spoke may have performance issues

You configure hub and spoke, devices discover spoke peers

Static VPN ▬

Dynamic VPN ▬

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

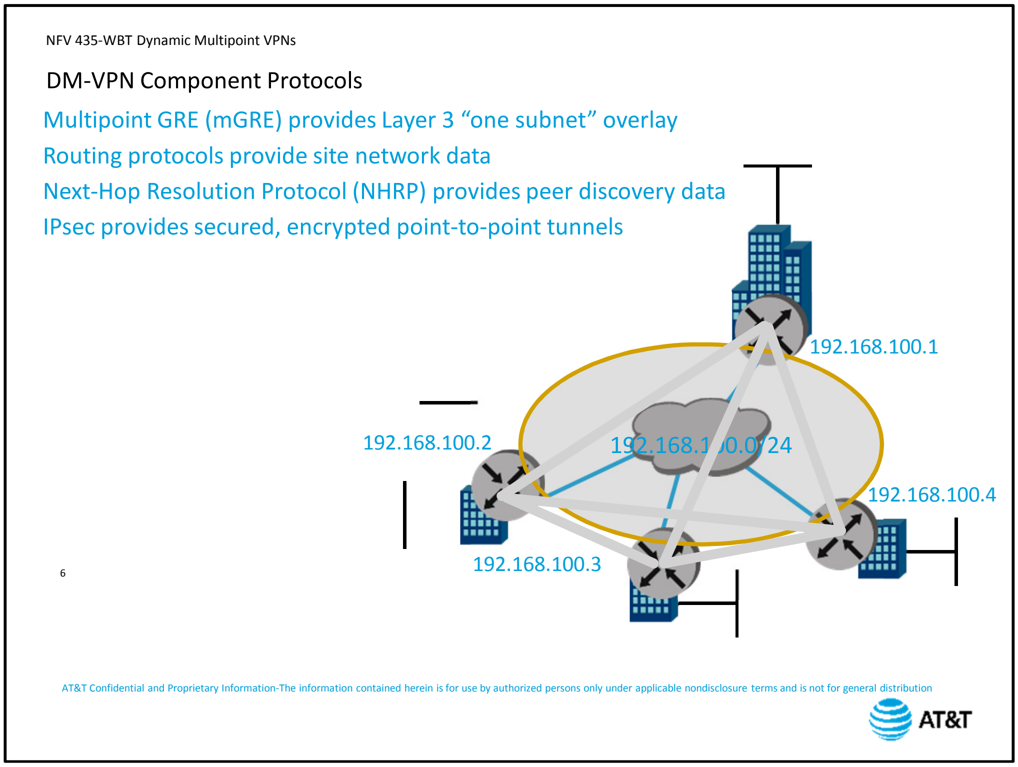
Dynamic multipoint VPNs allow the creation of meshed VPNs to be created on an on-demand basis, without requiring the configuration of a full mesh of all possible endpoints. The technology is designed for distributed sites where on-demand point-to-point VPN tunnels are desired.

For example, we have an enterprise with several branch offices, and we have deployed Voice over IP for our phone system.

We could configure a static mesh of VPNs to allow for secured site-to-site IP connections, but this presents challenges. A full mesh of connections presents scalability issues in configuration, management, and network device capacity. There is also the cost of maintaining the VPNs, especially if you are paying for your connectivity based on total data usage.

A hub and spoke configuration can eliminate much of the complexity, but introduces latency into exchanges between branch offices. If you are using Voice over IP or other delay-sensitive applications, this is not an ideal solution.

What DM-VPN does is combine the best of both. You configure the hub and spoke network, and the branch peers use that connectivity to discover each other, then establish site-to-site VPNs as traffic demands the connections.



NFV 435-WBT Dynamic Multipoint VPNs

DM-VPN Component Protocols

Multipoint GRE (mGRE) provides Layer 3 “one subnet” overlay

Routing protocols provide site network data

Next-Hop Resolution Protocol (NHRP) provides peer discovery data

IPsec provides secured, encrypted point-to-point tunnels

6

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

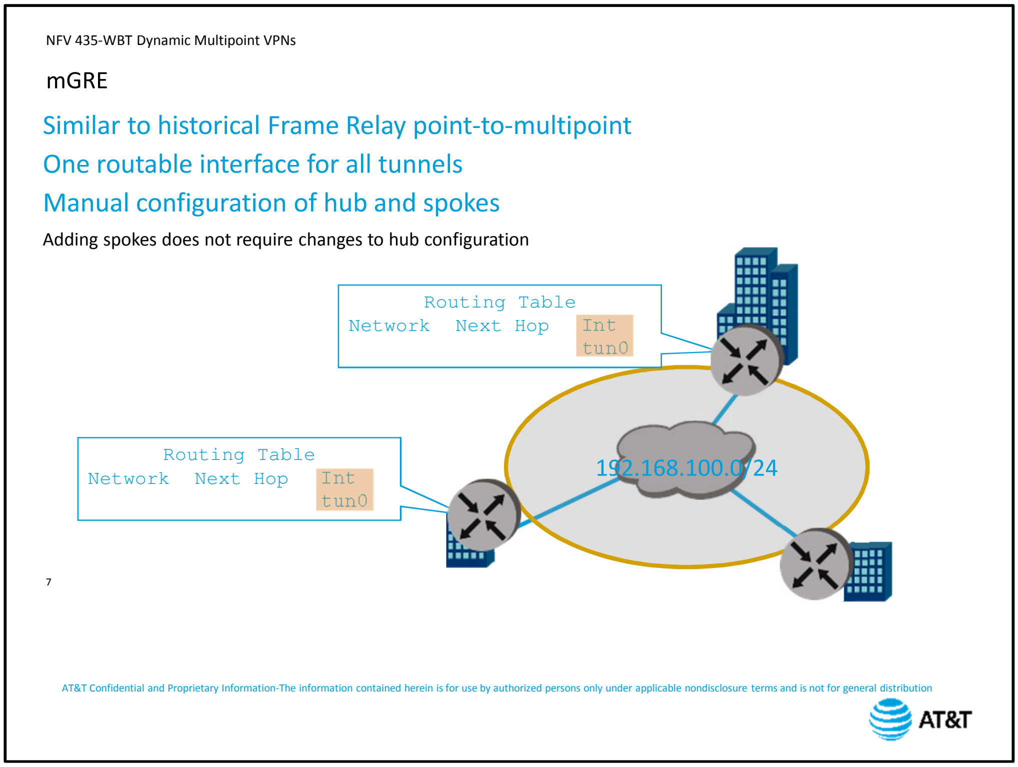
DM-VPN uses several different protocols.

The first, Multipoint GRE (mGRE), provides a Layer 3 single subnet overlay for the entire VPN mesh. This preserves addressing space as well as simplifying routing – the entire inter-site network appears as a single subnet in routing tables.

The second is your routing protocol. You can use OSPF, or you can statically configure routing information, to build the table of networks reachable over the multipoint GRE subnet.

The third, Next-hop Resolution Protocol (NHRP), allows devices to learn each others specific IP addresses on the shared subnet. The addresses learned via NHRP populate the next-hop information in the routing tables.

Finally, the tunnels themselves can use IPsec for security and encryption.



NFV 435-WBT Dynamic Multipoint VPNs

mGRE

Similar to historical Frame Relay point-to-multipoint

One routable interface for all tunnels

Manual configuration of hub and spokes

Adding spokes does not require changes to hub configuration

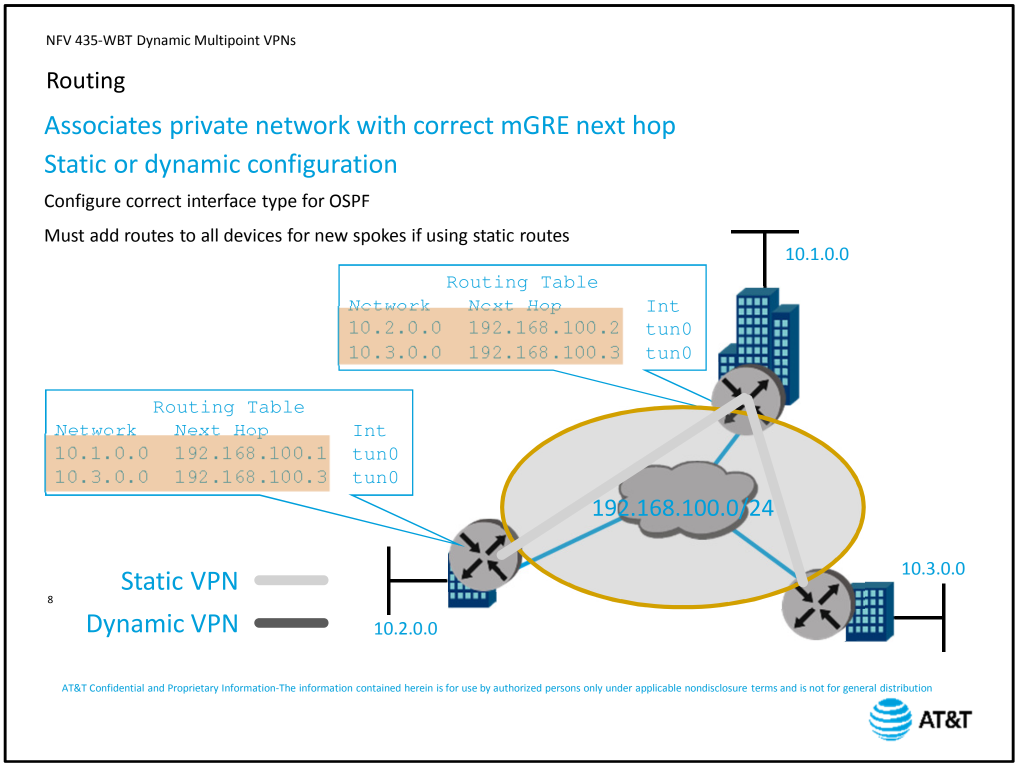
```
      Routing Table
Network   Next Hop   Int
                     tun0
```

```
      Routing Table
Network   Next Hop   Int
                     tun0
```

7

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 said on the previous slide, Multipoint GRE provides a Layer 3 overlay that allows you to treat the entire VPN network as a single subnet for routing purposes.
If you ever worked with Frame Relay point-to-multipoint networks in the past, the concept is the same.
You configure a single routeable tunnel interface for all of your VPN connections. You assign this interface an IP address from the subnet you have assigned to your DM-VPN network.
This manual configuration needs to be done once at the hub, and once on every spoke in the VPN mesh.
Because each new device is also part of the same subnet, you do not need to modify the configuration of the hub when you add new spokes.



NFV 435-WBT Dynamic Multipoint VPNs

Routing

Associates private network with correct mGRE next hop

Static or dynamic configuration

Configure correct interface type for OSPF

Must add routes to all devices for new spokes if using static routes

Routing Table

Network	Next Hop	Int
10.2.0.0	192.168.100.2	tun0
10.3.0.0	192.168.100.3	tun0

Routing Table

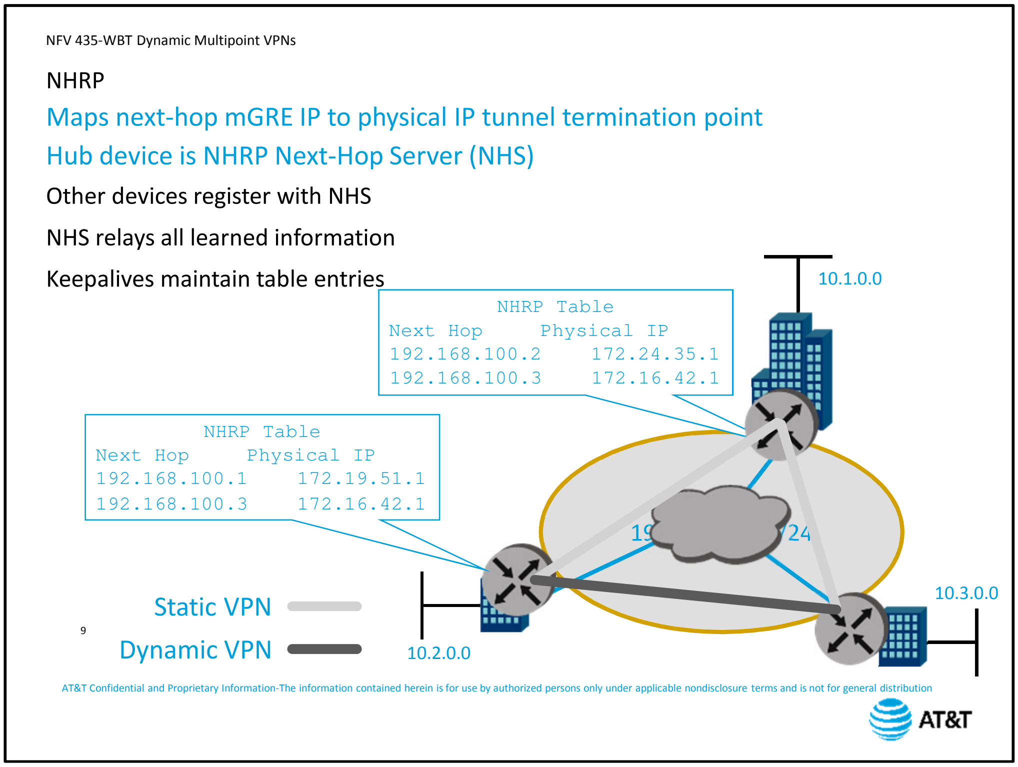
Network	Next Hop	Int
10.1.0.0	192.168.100.1	tun0
10.3.0.0	192.168.100.3	tun0

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

The next component maps the remote private networks and associate them with the correct next-hop address in the mGRE network. In other words, building the routing table. You can do this either by configuring manual static routes, or you can configure OSPF to run over the tunnel interface.

If you do use OSPF, make sure to configure the correct OSPF interface type on the tunnel interface on each node.

If you use static routes, you will have to manually configure routing entries on each spoke and on the hub for all spokes in the network. If you add a new spoke, you will need to add the route to all other devices.



NFV 435-WBT Dynamic Multipoint VPNs

NHRP

Maps next-hop mGRE IP to physical IP tunnel termination point

Hub device is NHRP Next-Hop Server (NHS)

Other devices register with NHS

NHS relays all learned information

Keepalives maintain table entries

NHRP Table

Next Hop	Physical IP
192.168.100.2	172.24.35.1
192.168.100.3	172.16.42.1

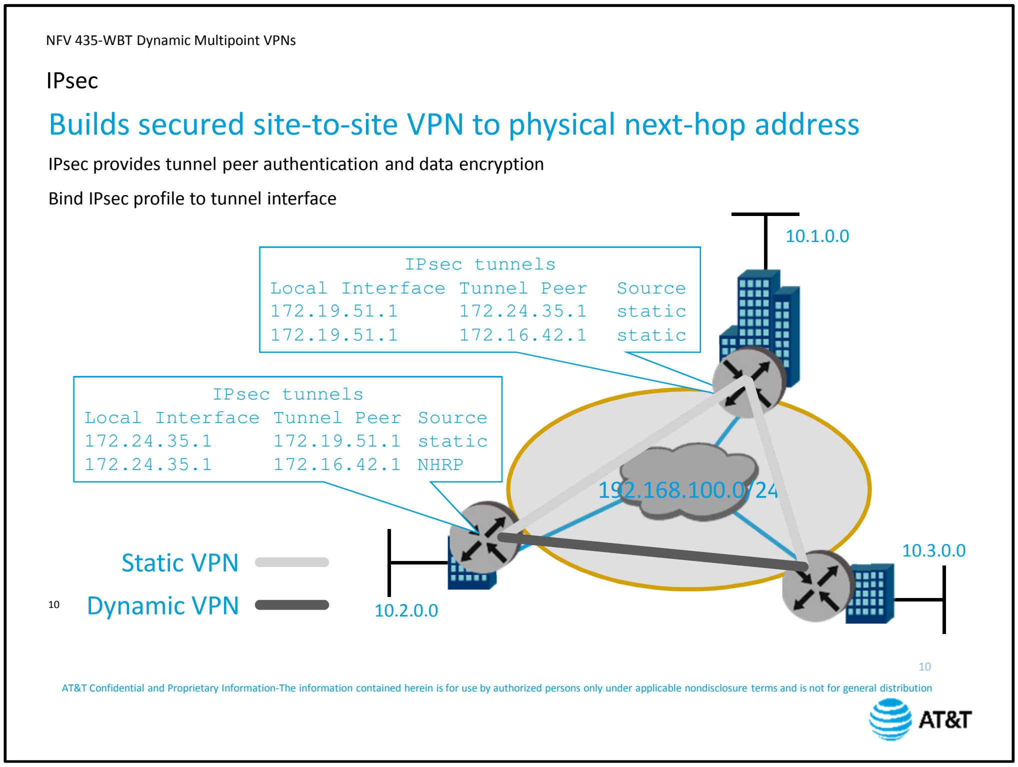
NHRP Table

Next Hop	Physical IP
192.168.100.1	172.19.51.1
192.168.100.3	172.16.42.1

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 order to know which specific tunnel to use, the next-hop IP address needs to be mapped to the correct physical tunnel termination point. This is the job of NHRP.
NHRP is a client-server protocol. The hub device is the NHRP next hop server.
You configure each spoke device with the mGRE tunnel address and the physical address of the next-hop server.
The spokes then register with the next-hop server, providing the mGRE tunnel address that goes with its physical address.
The server then relays all learned information to all registered clients.
NHRP uses keepalives to maintain the tables and keep the information current.
Now that the spokes have a physical address for each other, they can use GRE to encapsulate data and send it directly between the two sites. At this point, you have a full tunnel mesh using GRE encapsulation, but none of the tunnels are secured.



NFV 435-WBT Dynamic Multipoint VPNs

IPsec

Builds secured site-to-site VPN to physical next-hop address

IPsec provides tunnel peer authentication and data encryption

Bind IPsec profile to tunnel interface

IPsec tunnels

Local Interface	Tunnel Peer	Source
172.19.51.1	172.24.35.1	static
172.19.51.1	172.16.42.1	static

IPsec tunnels

Local Interface	Tunnel Peer	Source
172.24.35.1	172.19.51.1	static
172.24.35.1	172.16.42.1	NHRP

10

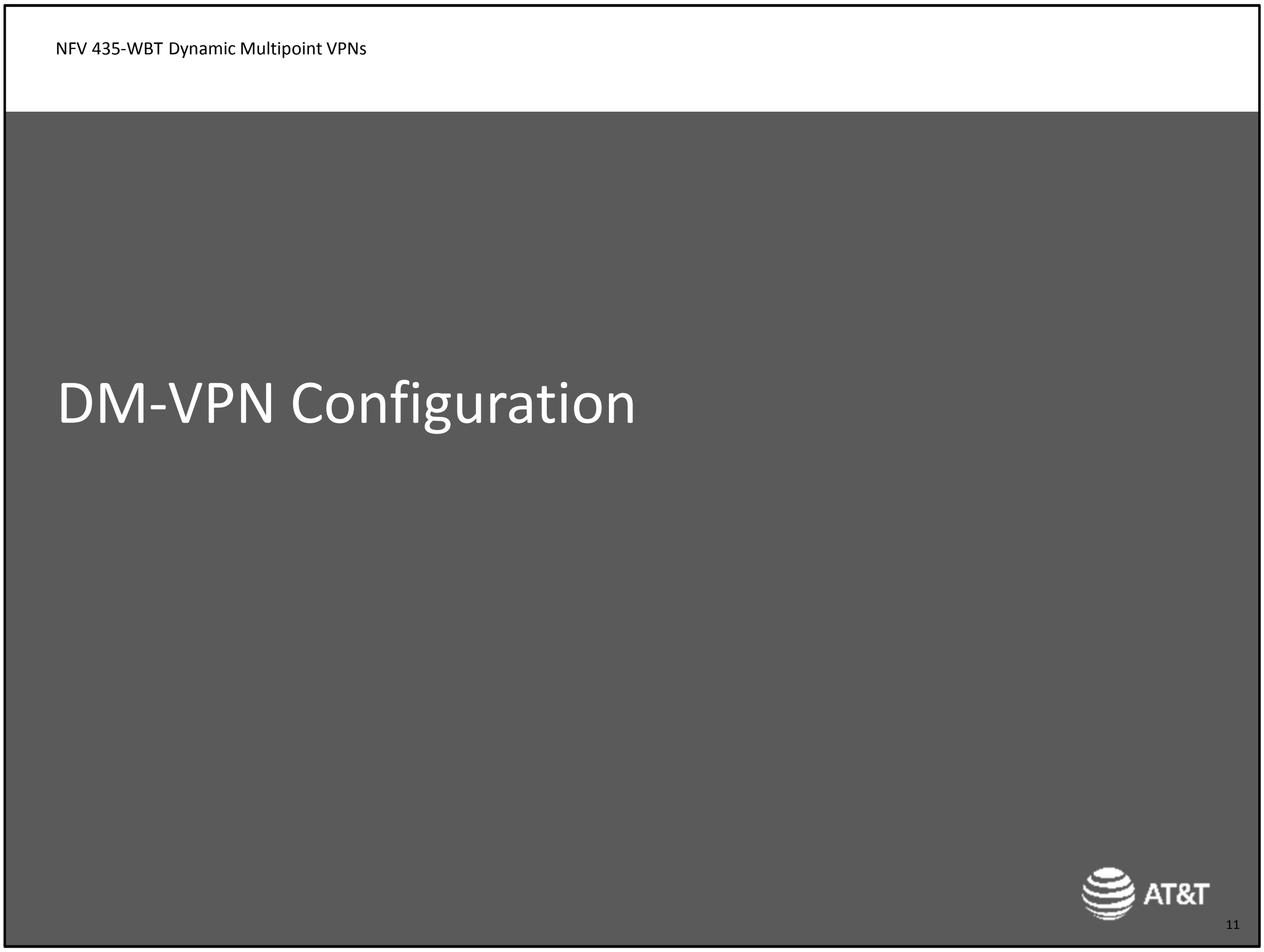
AT&T Confidential and Proprietary Information-The information contained herein is for use by authorized persons only under applicable nondisclosure terms and is not for general distribution

AT&T

IPsec provides the security you want for transmitting traffic across the public network. The IPsec tunnels use the same physical addressing as the GRE tunnels. The IPsec peer addresses are configured statically for links between the hub and individual spokes, and are learned dynamically via NHRP for spoke-to-spoke tunnel negotiation.

IPsec provides both tunnel peer authentication and user data encryption. Before any user data is transmitted, the tunnel peers verify that they are allowed to connect to each other and can secure the user data. Once that verification is complete, all transmissions over the tunnel are encrypted.

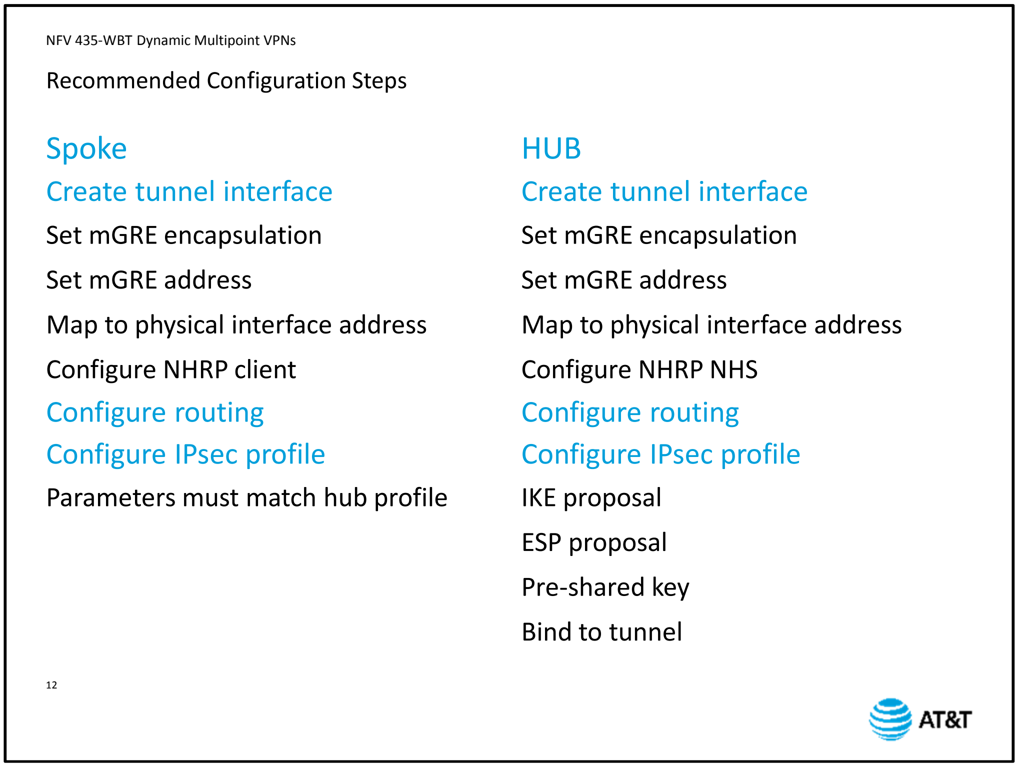
Instead of configuring individual site-to-site connections, you will configure a VPN profile on each device, then bind that profile to the tunnel interface. Of course, a with any IPsec configuration, the profile parameters must match between sites or the IPsec negotiations will fail.



NFV 435-WBT Dynamic Multipoint VPNs

DM-VPN Configuration

Next, we’ll discuss IGMP and how multicast sources and clients use it to join and leave multicast groups.



NFV 435-WBT Dynamic Multipoint VPNs

Recommended Configuration Steps

Spoke

Create tunnel interface

Set mGRE encapsulation

Set mGRE address

Map to physical interface address

Configure NHRP client

Configure routing

Configure IPsec profile

Parameters must match hub profile

HUB

Create tunnel interface

Set mGRE encapsulation

Set mGRE address

Map to physical interface address

Configure NHRP NHS

Configure routing

Configure IPsec profile

IKE proposal

ESP proposal

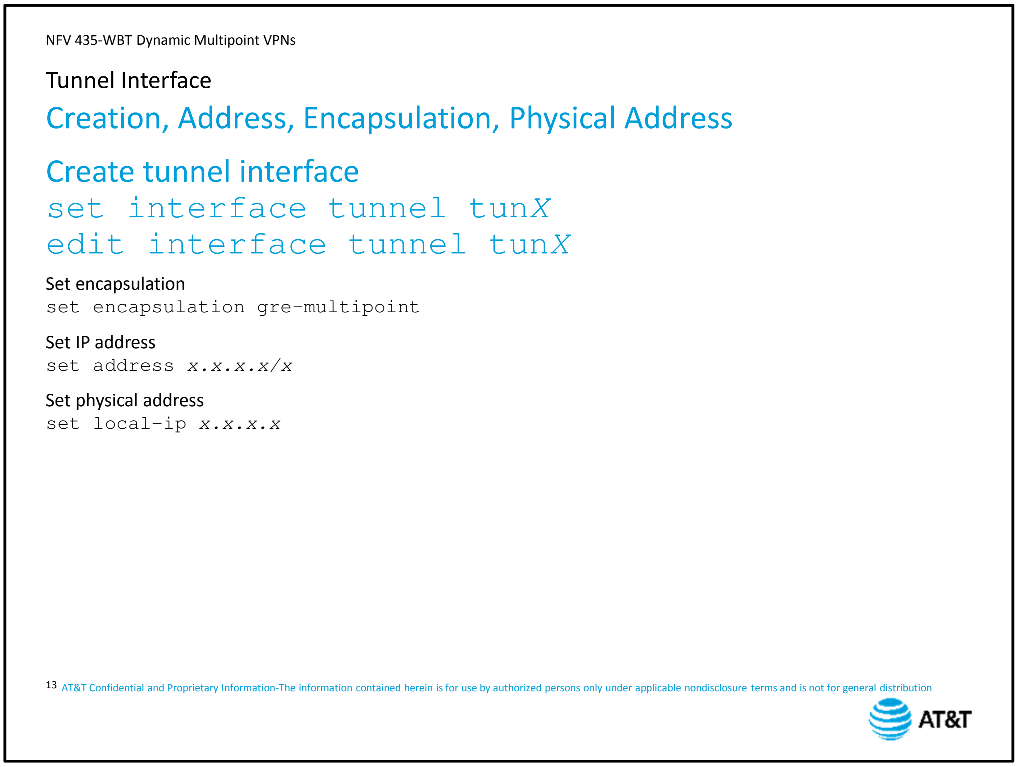
Pre-shared key

Bind to tunnel

12

AT&T

As you already know, DM-VPN has several different protocols, so you can expect the configuration to have several different components. On the hub device,
You begin by creating the tunnel interface and configuring the mGRE and NHRP operations.
Next, you set up your routing, either static routes or OSPF.
You finish with creating an IPsec profile and binding it to the tunnel interface.
On the spokes, you create a tunnel interface as well. The difference here is that you configure NHRP as a client, not as the next-hop server.
You then set up your routing,
and your IPsec profile just as you did on the hub.
The next slides will focus on the commands specific to DM-VPN. If you have not already done so, you should view the vRouter courses on static routing, OSPF, and IPsec for a complete understanding of the configuration of these protocols.



Tunnel Interface

Creation, Address, Encapsulation, Physical Address

Create tunnel interface

```
set interface tunnel tunX
edit interface tunnel tunX
```

Set encapsulation

```
set encapsulation gre-multipoint
```

Set IP address

```
set address x.x.x.x/x
```

Set physical address

```
set local-ip x.x.x.x
```

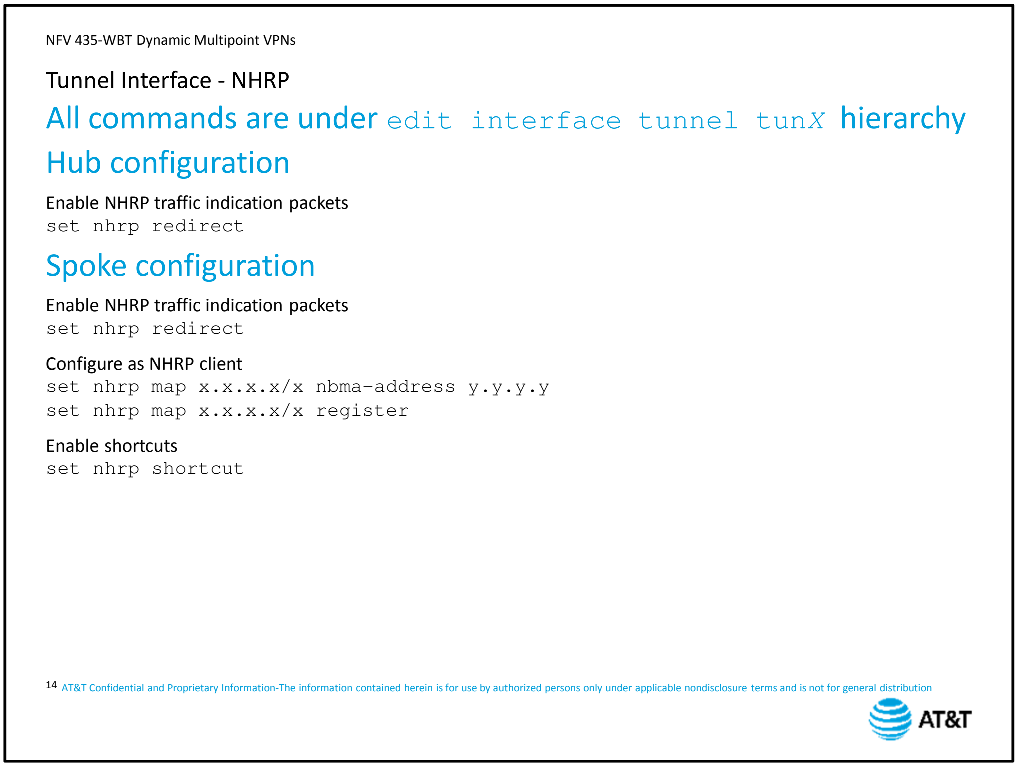
To begin your configuration, you create a tunnel interface. You can number the tunnel interfaces using any non-negative integer.

Because you will be setting several parameters under the tunnel interface, we recommend using the `edit` command. This will save you some typing, and ensure that all your parameters are associated with the correct interface.

Set the encapsulation on the tunnel interface to *gre-multipoint*. This enables mGRE and indicates that this is not a point-to-point tunnel.

The address is the IP address from the mGRE subnet.

The local IP is the address of the interface that physically connects to the network, usually the interface connected to the Internet.



NFV 435-WBT Dynamic Multipoint VPNs

Tunnel Interface - NHRP

All commands are under `edit interface tunnel tunX` hierarchy

Hub configuration

Enable NHRP traffic indication packets

```
set nhrp redirect
```

Spoke configuration

Enable NHRP traffic indication packets

```
set nhrp redirect
```

Configure as NHRP client

```
set nhrp map x.x.x.x/x nbma-address y.y.y.y
set nhrp map x.x.x.x/x register
```

Enable shortcuts

```
set nhrp shortcut
```

14 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

Next you need to enable NHRP. The NHRP configuration is still under the interface, and is different for hub and spoke devices.

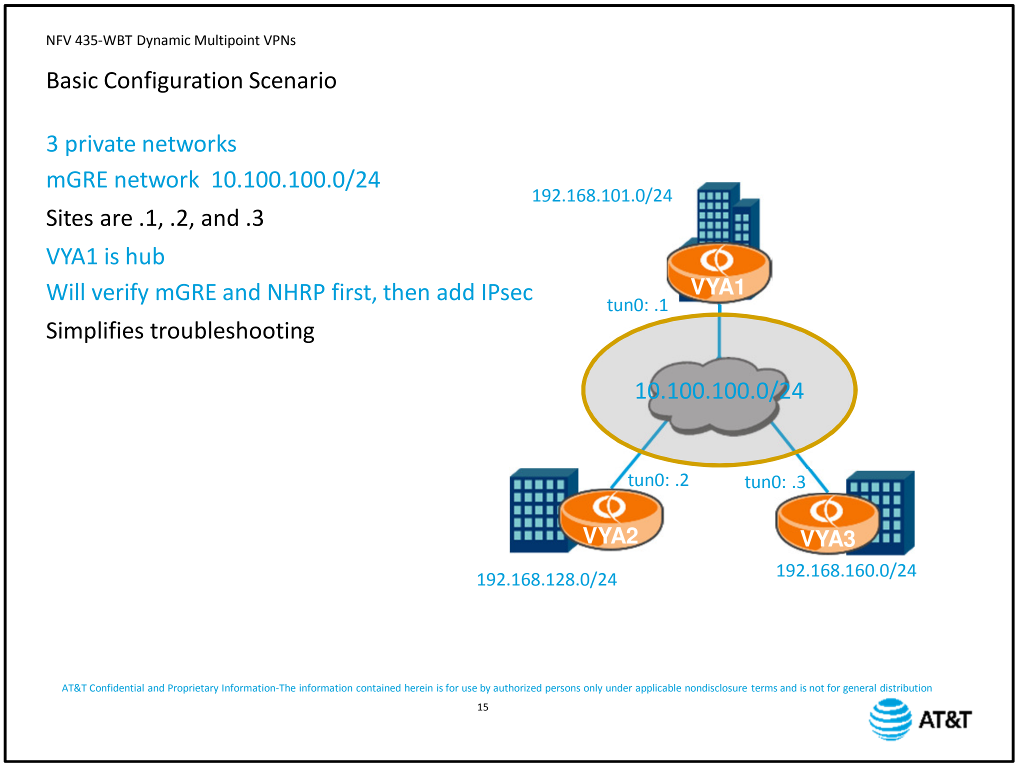
On the hub, all you need to do is enable NHRP traffic indication packets. With no other configuration, the device defaults to operating as the next hop server for the NHRP network.

On the spoke, you also enable NHRP traffic indication.

Next, you need to set up the NHRP client parameters. First, you map the mGRE address of the hub to the physical address of the hub. Note that the mGRE address, here shown as x.x.x.x, requires the subnet, while the physical address does not.

You then enable the spoke device to register with the hub device. This tells the spoke to send its mGRE and physical address to the hub for learning, and enables the hub to return the complete NHRP table.

Finally, you enable shortcuts. This setting is what allows the spokes to build direct connections to each other and bypass the hub for user traffic forwarding.



NFV 435-WBT Dynamic Multipoint VPNs

Basic Configuration Scenario

3 private networks

mGRE network 10.100.100.0/24

Sites are .1, .2, and .3

VYA1 is hub

Will verify mGRE and NHRP first, then add IPsec

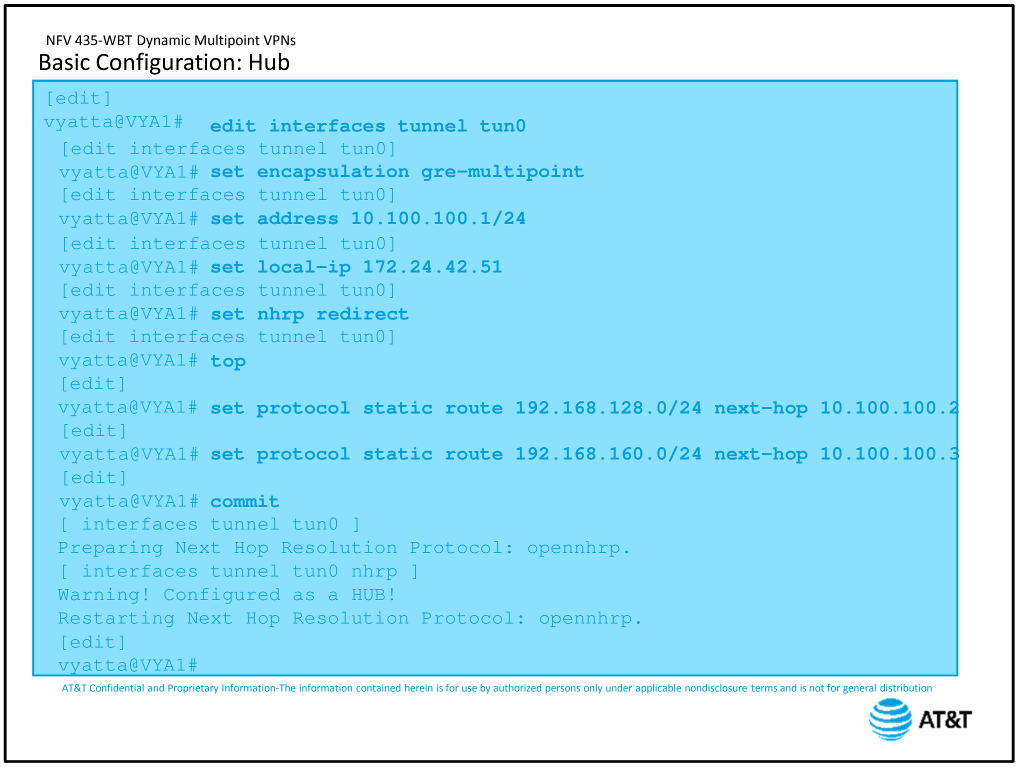
Simplifies troubleshooting

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

15

AT&T

Let’s apply these commands to a simple three-site configuration.
We have three sites, each with a private network in the 192.168. address space.
We will apply an mGRE network overlay, configuring a tunnel interface at each site. Our mGRE subnet is 10.100.100.0.
We will configure vRouter VYA1 as our hub router.
We will set up mGRE, NHRP, and static routing first, then verify that those components are working. We will then go back and add IPsec to secure the tunnels.
We recommend this process to simplify the troubleshooting of your initial configuration. By leaving IPsec out at first, you only have to diagnose mGRE and NHRP if you have connectivity issues. Adding IPsec after you have connectivity isolates any subsequent problems to the IPsec configuration.



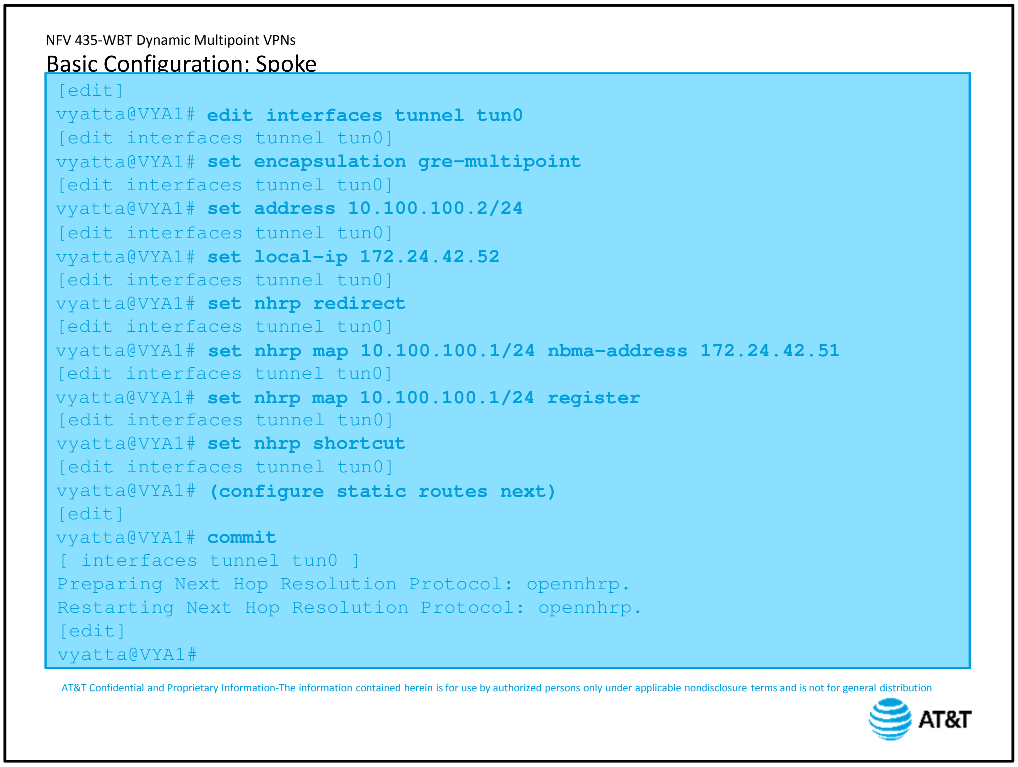
NFV 435-WBT Dynamic Multipoint VPNs

Basic Configuration: Hub

```
[edit]
vyatta@VYA1#  edit interfaces tunnel tun0
 [edit interfaces tunnel tun0]
 vyatta@VYA1# set encapsulation gre-multipoint
 [edit interfaces tunnel tun0]
 vyatta@VYA1# set address 10.100.100.1/24
 [edit interfaces tunnel tun0]
 vyatta@VYA1# set local-ip 172.24.42.51
 [edit interfaces tunnel tun0]
 vyatta@VYA1# set nhrp redirect
 [edit interfaces tunnel tun0]
 vyatta@VYA1# top
 [edit]
 vyatta@VYA1# set protocol static route 192.168.128.0/24 next-hop 10.100.100.2
 [edit]
 vyatta@VYA1# set protocol static route 192.168.160.0/24 next-hop 10.100.100.3
 [edit]
 vyatta@VYA1# commit
 [ interfaces tunnel tun0 ]
 Preparing Next Hop Resolution Protocol: opennhrp.
 [ interfaces tunnel tun0 nhrp ]
 Warning! Configured as a HUB!
 Restarting Next Hop Resolution Protocol: opennhrp.
 [edit]
 vyatta@VYA1#
```

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 configure the hub first.
Using the `edit` command, we create tunnel interface 0 and enter the configuration hierarchy for the interface.
We set the encapsulation to *gre-multipoint*,
Set the tunnel IP address from the mGRE network,
then specify the address of the interface connected to the public network.
Finally, we enable NHRP on the interface.
We go up to the top of the hierarchy using the `top` command.
Then set the static routes, one for the network behind router VYA2,
and one for the network behind router VYA3.
When we commit the configuration, the vRouter provides information about NHRP starting and informs you that the device has been configured as an NHRP hub.



NFV 435-WBT Dynamic Multipoint VPNs

Basic Configuration: Spoke

```
[edit]
vyatta@VYA1# edit interfaces tunnel tun0
[edit interfaces tunnel tun0]
vyatta@VYA1# set encapsulation gre-multipoint
[edit interfaces tunnel tun0]
vyatta@VYA1# set address 10.100.100.2/24
[edit interfaces tunnel tun0]
vyatta@VYA1# set local-ip 172.24.42.52
[edit interfaces tunnel tun0]
vyatta@VYA1# set nhrp redirect
[edit interfaces tunnel tun0]
vyatta@VYA1# set nhrp map 10.100.100.1/24 nbma-address 172.24.42.51
[edit interfaces tunnel tun0]
vyatta@VYA1# set nhrp map 10.100.100.1/24 register
[edit interfaces tunnel tun0]
vyatta@VYA1# set nhrp shortcut
[edit interfaces tunnel tun0]
vyatta@VYA1# (configure static routes next)
[edit]
vyatta@VYA1# commit
[ interfaces tunnel tun0 ]
Preparing Next Hop Resolution Protocol: opennhrp.
Restarting Next Hop Resolution Protocol: opennhrp.
[edit]
vyatta@VYA1#
```

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

Next, we configure the spoke.

Using the `edit` command, we create tunnel interface 0 and enter the configuration hierarchy for the interface.

We set the encapsulation to *gre-multipoint*,

Set the tunnel IP address from the mGRE network

Then specify the address of the interface connected to the public network. So far, these commands are identical to the hub configuration.

Next, we configure the NHRP spoke settings. We enable NHRP,

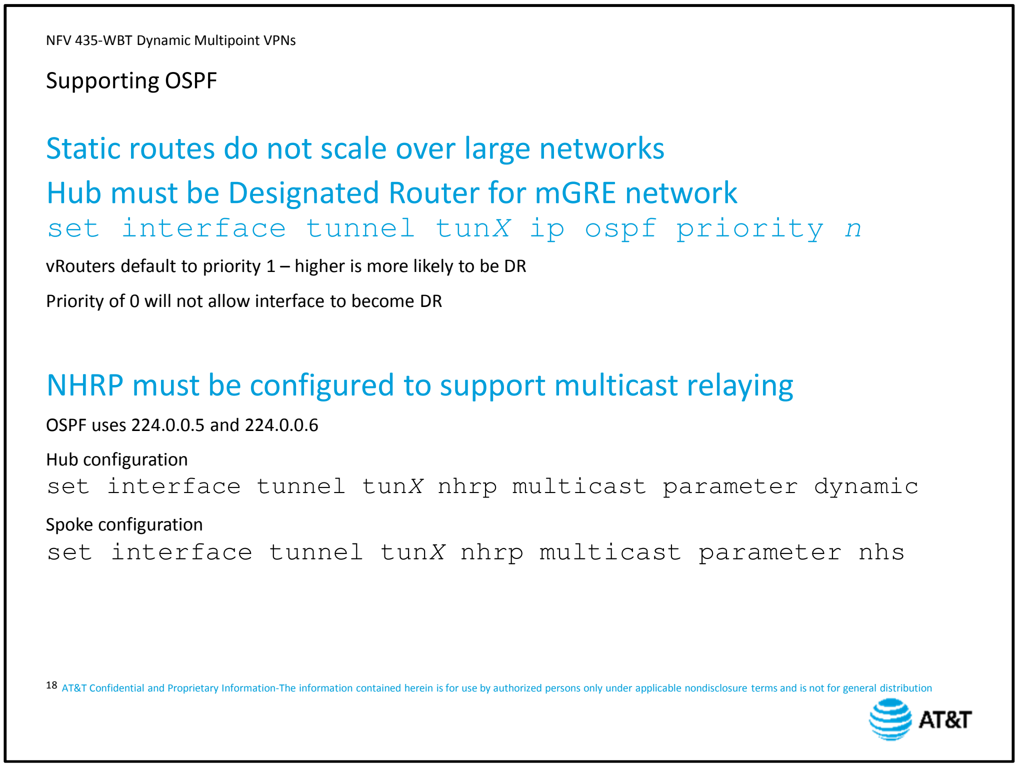
Then map the location of the hub. The first address is the mGRE address for the hub, and the second is the physical address of the hub's connection to the Internetl

We then specify that we need to register our address with the hub.

Finally, we configure NHRP to allow shortcut routes so that spokes can communicate directly with each other.

The next step is to configure the static routes. We'll omit the details in our screen shot here, but the command syntax is the same as on the hub.

When we commit our configuration this time, we see NHRP starting, but do not see any messages about the device being a hub.



NFV 435-WBT Dynamic Multipoint VPNs

Supporting OSPF

Static routes do not scale over large networks

Hub must be Designated Router for mGRE network

```
set interface tunnel tunX ip ospf priority n
```

vRouters default to priority 1 – higher is more likely to be DR

Priority of 0 will not allow interface to become DR

NHRP must be configured to support multicast relaying

OSPF uses 224.0.0.5 and 224.0.0.6

Hub configuration

```
set interface tunnel tunX nhrp multicast parameter dynamic
```

Spoke configuration

```
set interface tunnel tunX nhrp multicast parameter nhs
```

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

AT&T

As you can imagine, setting up static routes in a network with many spokes can be tedious. And adding a spoke means you have to add a route entry on every other spoke as well as the hub. This defeats the purpose of DM-VPN, so we recommend using OSPF in larger networks. However, there are some specific configuration parameters you must set in addition to the standard OSPF configuration.

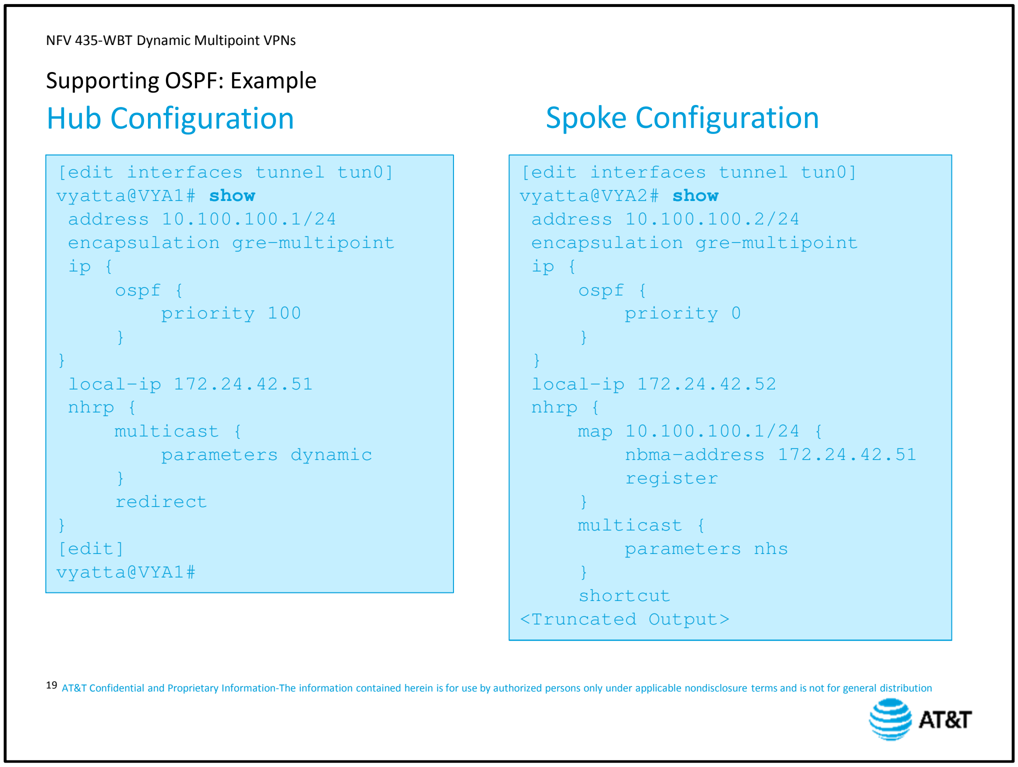
First of all, the hub device must be the Designated Router on the tunnel interface. This ensures that the hub receives advertisements from a spoke, then relays those advertisements to all other spokes in the network.

The higher the priority value, the more likely a device is to become the designated router. On the hub, you should set this value higher than all other devices on the mGRE network. On vRouter spokes, set the priority on the tunnel interface to 0. This ensures that the spoke will not become the DR.

The next setting is to enable NHRP to support learning and relaying multicast addresses. This is required because OSPF uses multicast to send link state advertisements.

On the hub, you configure NHRP for dynamic multicast. This means that the hub will learn and share multicast address information.

On the spokes, you configure NHRP to register needed multicast addresses with the next hop server. When you configure OSPF, the spoke vRouter will register the needed addresses of 224.0.0.5 and 224.0.0.6 at the hub.



NFV 435-WBT Dynamic Multipoint VPNs

Supporting OSPF: Example

Hub Configuration

```
[edit interfaces tunnel tun0]
vyatta@VYA1# show
 address 10.100.100.1/24
 encapsulation gre-multipoint
 ip {
     ospf {
         priority 100
     }
}
 local-ip 172.24.42.51
 nhrp {
     multicast {
         parameters dynamic
     }
     redirect
}
[edit]
vyatta@VYA1#
```

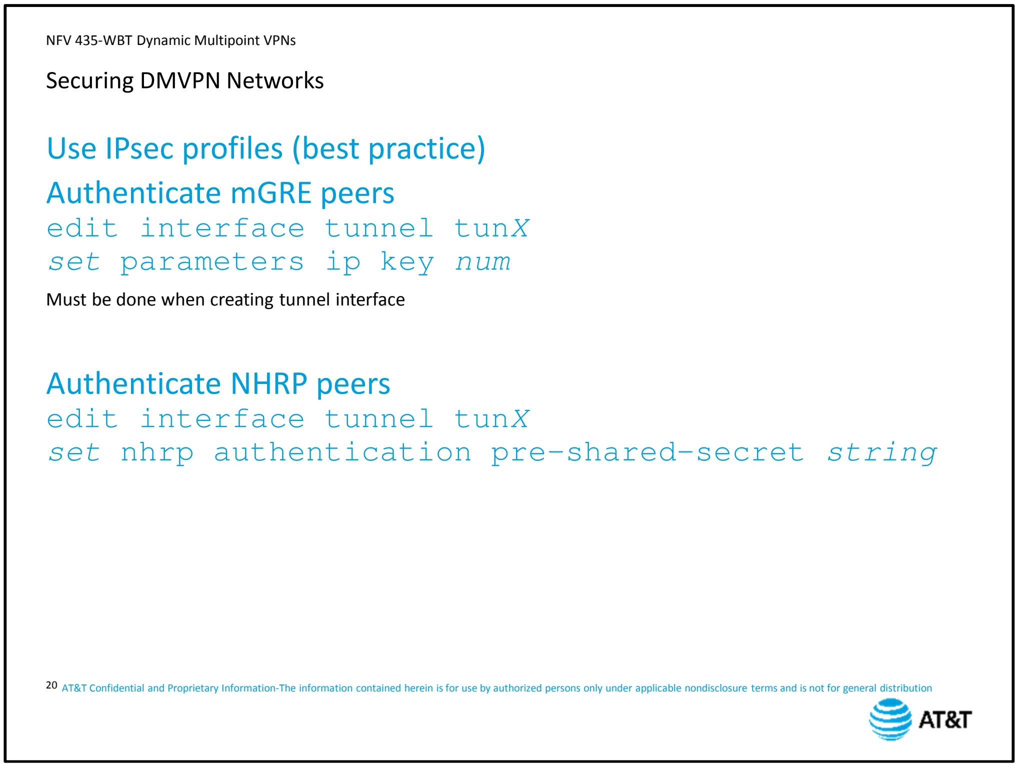
Spoke Configuration

```
[edit interfaces tunnel tun0]
vyatta@VYA2# show
 address 10.100.100.2/24
 encapsulation gre-multipoint
 ip {
     ospf {
         priority 0
     }
 }
 local-ip 172.24.42.52
 nhrp {
     map 10.100.100.1/24 {
         nbma-address 172.24.42.51
         register
     }
     multicast {
         parameters nhs
     }
     shortcut
<Truncated Output>
```

19 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 example,
We can see that the hub has a priority set to 100, and the spokes have a priority of 0. This ensures that the hub will always be the designated router.
We can also see that the hub is set to learn multicast addresses dynamically, and the spokes are configured to register multicast addresses with the NHRP next hop server. As we learned earlier, the next hop server is always the hub in a DM-VPN configuration.
The details of designated router election, OSPF configuration, and protocol verification and troubleshooting are beyond the scope of this course. The *AT&T vRouter OSPF Basics* course covers all these topics in detail.



NFV 435-WBT Dynamic Multipoint VPNs

Securing DMVPN Networks

Use IPsec profiles (best practice)

Authenticate mGRE peers

```
edit interface tunnel tunX
set parameters ip key num
```

Must be done when creating tunnel interface

Authenticate NHRP peers

```
edit interface tunnel tunX
set nhrp authentication pre-shared-secret string
```

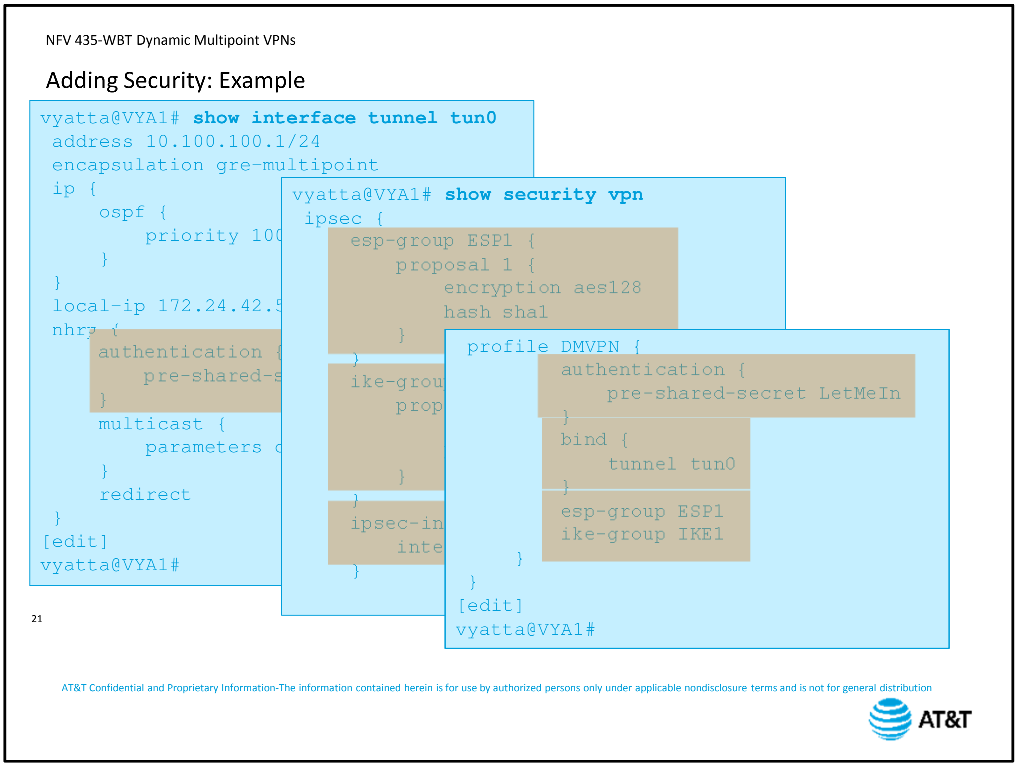
20 AT&T Confidential and Proprietary Information-The information contained herein is for use by authorized persons only under applicable nondisclosure terms and is not for general distribution

As we said earlier, you can use IPsec to provide encryption and authentication between the tunnel peers. Instead of configuring details for each tunnel peer, you create an IPsec profile and bind it to the tunnel interface. All peers on the mGRE network need to have the same IPsec profile settings.

You can also add tunnel peer authentication to the mGRE tunnel itself by setting the IP key value on the tunnel interface. All peers must have the same key value configured. Peers compare key values before establishing the site-to-site GRE tunnel.

If you want to use this security feature, you must configure it when you first create the tunnel interface. You cannot add it later to an existing tunnel interface.

You can also add authentication to NHRP with a pre-shared text string. As with the IP key, the text string must be identical on all tunnel peers.



NFV 435-WBT Dynamic Multipoint VPNs

Adding Security: Example

```
vyatta@VYA1# show interface tunnel tun0
 address 10.100.100.1/24
 encapsulation gre-multipoint
 ip {
     ospf {
         priority 10(
     }
 }
 local-ip 172.24.42.5
 nhrp {
     authentication {
         pre-shared-s
     }
     multicast {
         parameters c
     }
     redirect
 }
[edit]
vyatta@VYA1#
```

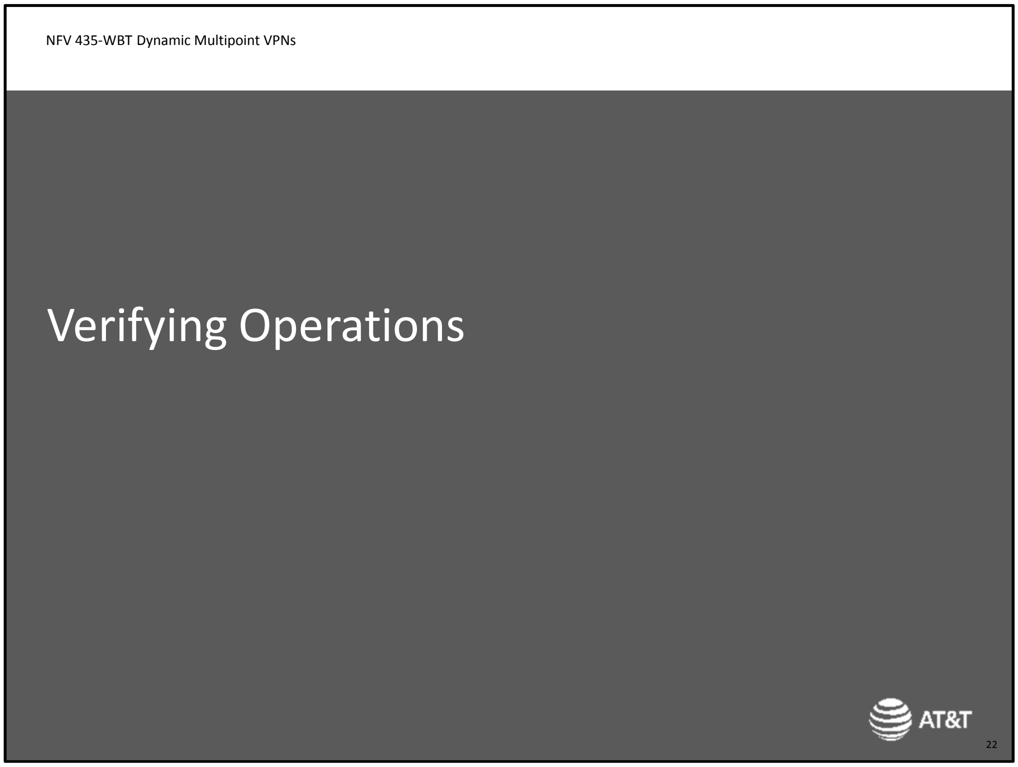
```
vyatta@VYA1# show security vpn
 ipsec {
     esp-group ESP1 {
         proposal 1 {
             encryption aes128
             hash sha1
         }
     }
     ike-grou
         prop

         }
     }
     ipsec-in
         inte
     }
```

```
  profile DMVPN {
         authentication {
             pre-shared-secret LetMeIn
         }
         bind {
             tunnel tun0
         }
         esp-group ESP1
         ike-group IKE1
     }
 }
[edit]
vyatta@VYA1#
```

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

Because our tunnel interface is already up, we cannot add the GRE key.
However, we can add the NHRP preshared secret string in addition to our IPsec profile.
For the IPsec settings, we configure the ESP proposal set,
the IKE proposal set,
enable IPsec on the interface connected to the Internet.
Next, create the DM-VPN profile, which includes
the preshared secret for IKE Phase 1 negotiations,
the binding to the tunnel interface,
and references to the proposal sets. For these security features, there are no differences between hub and spoke configuration. In fact, the configuration parameters must be identical across the mGRE network.
As with OSPF, a detailed discussion of IPsec is beyond the scope of this course. The *AT&T vRouter Site-to-Site VPNs using IPsec* course includes a detailed discussion of IPsec technology, including a breakdown of IKE negotiations; site-to-site VPN configuration, and an extensive verification and troubleshooting section.

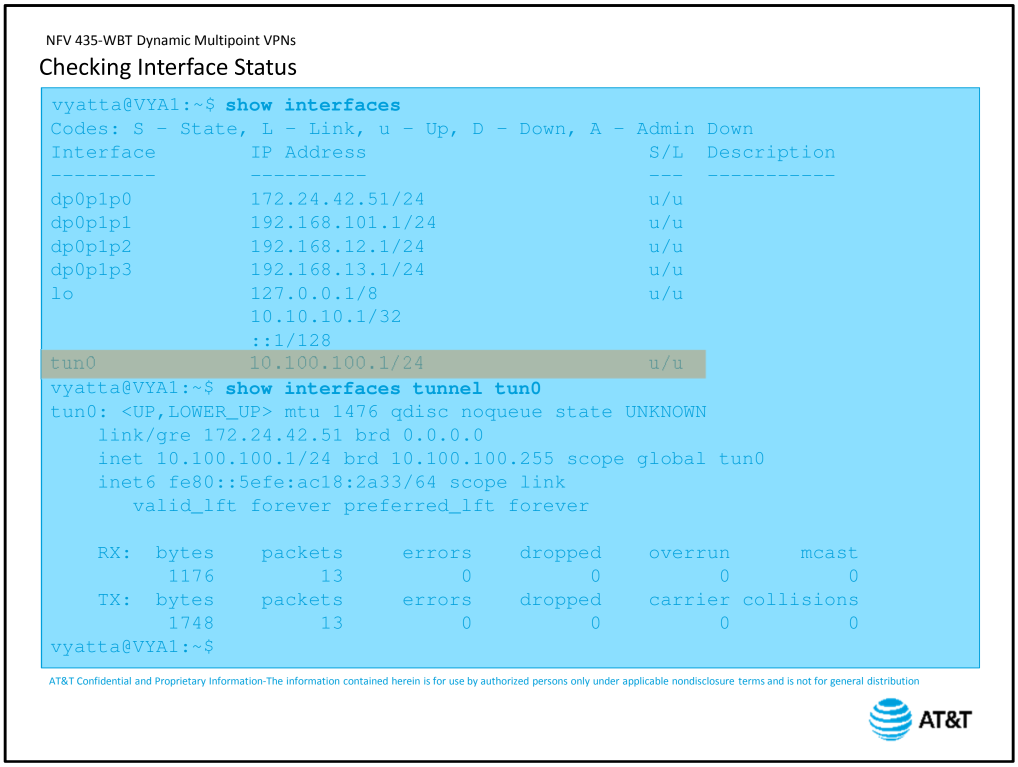


NFV 435-WBT Dynamic Multipoint VPNs

Verifying Operations

22

Next, we’ll discuss IGMP and how multicast sources and clients use it to join and leave multicast groups.



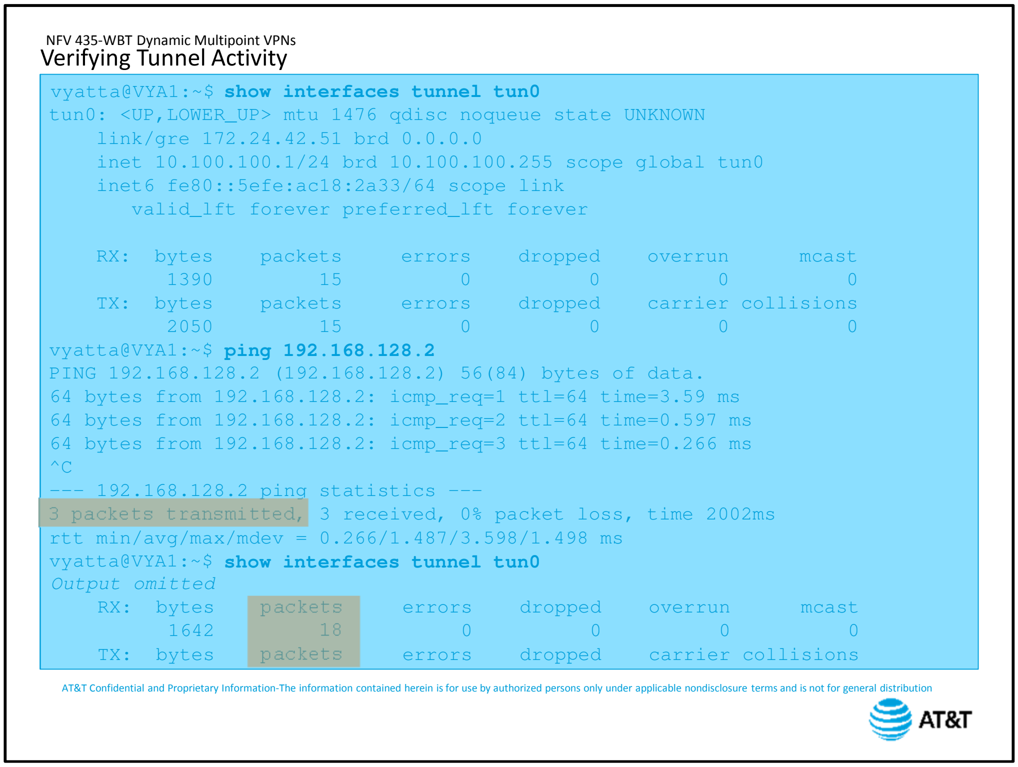
NFV 435-WBT Dynamic Multipoint VPNs

Checking Interface Status

```
vyatta@VYA1:~$ show interfaces
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                        S/L  Description
---------        ----------                        ---  -----------
dp0p1p0          172.24.42.51/24                   u/u
dp0p1p1          192.168.101.1/24                  u/u
dp0p1p2          192.168.12.1/24                   u/u
dp0p1p3          192.168.13.1/24                   u/u
lo               127.0.0.1/8                       u/u
                 10.10.10.1/32
                 ::1/128
tun0             10.100.100.1/24                   u/u
vyatta@VYA1:~$ show interfaces tunnel tun0
tun0: <UP,LOWER_UP> mtu 1476 qdisc noqueue state UNKNOWN
    link/gre 172.24.42.51 brd 0.0.0.0
    inet 10.100.100.1/24 brd 10.100.100.255 scope global tun0
    inet6 fe80::5efe:ac18:2a33/64 scope link
       valid_lft forever preferred_lft forever

    RX:  bytes    packets     errors    dropped    overrun       mcast
          1176         13          0          0          0           0
    TX:  bytes    packets     errors    dropped    carrier collisions
          1748         13          0          0          0           0
vyatta@VYA1:~$
```

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

The first thing to check is the status of the tunnel interface.
The `show interfaces` command will display a list of all interfaces on the vRouter.
You are looking for the tunnel interface, checking that the correct IP address is configured, and that both the state and link show as *up*.
You can look at the details, including counters, by specifying the interface name in the `show interfaces` command.



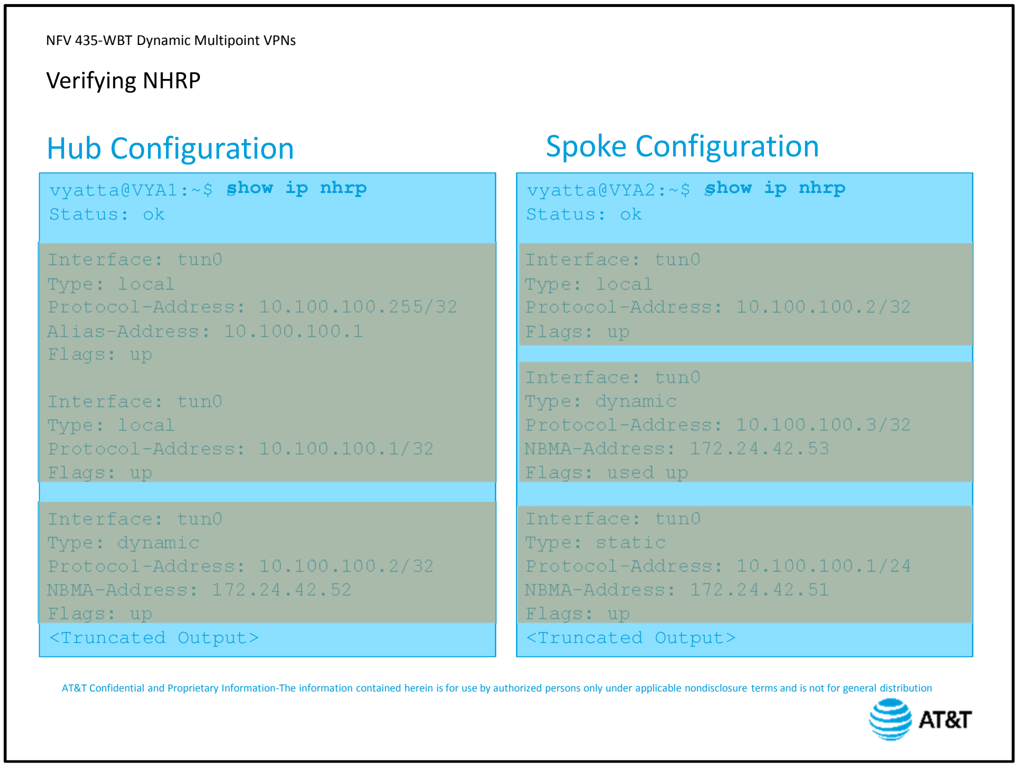
NFV 435-WBT Dynamic Multipoint VPNs

Verifying Tunnel Activity

```
vyatta@VYA1:~$ show interfaces tunnel tun0
tun0: <UP,LOWER_UP> mtu 1476 qdisc noqueue state UNKNOWN
    link/gre 172.24.42.51 brd 0.0.0.0
    inet 10.100.100.1/24 brd 10.100.100.255 scope global tun0
    inet6 fe80::5efe:ac18:2a33/64 scope link
       valid_lft forever preferred_lft forever

    RX:  bytes    packets     errors    dropped    overrun      mcast
          1390         15          0          0          0          0
    TX:  bytes    packets     errors    dropped    carrier collisions
          2050         15          0          0          0          0
vyatta@VYA1:~$ ping 192.168.128.2
PING 192.168.128.2 (192.168.128.2) 56(84) bytes of data.
64 bytes from 192.168.128.2: icmp_req=1 ttl=64 time=3.59 ms
64 bytes from 192.168.128.2: icmp_req=2 ttl=64 time=0.597 ms
64 bytes from 192.168.128.2: icmp_req=3 ttl=64 time=0.266 ms
^C
--- 192.168.128.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 0.266/1.487/3.598/1.498 ms
vyatta@VYA1:~$ show interfaces tunnel tun0
Output omitted
    RX:  bytes    packets     errors    dropped    overrun      mcast
          1642         18          0          0          0          0
    TX:  bytes    packets     errors    dropped    carrier collisions
```

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 test that traffic is crossing the tunnel,
display the interface counters,
then ping a host on a private network on the other side of the tunnel. Your first checkpoint is that the ping is successful.
To verify that the traffic crossed the tunnel, check the interface counters again.
We sent 3 packets in our ping, and the tunnel counter incremented by 3 packets.



NFV 435-WBT Dynamic Multipoint VPNs

Verifying NHRP

Hub Configuration

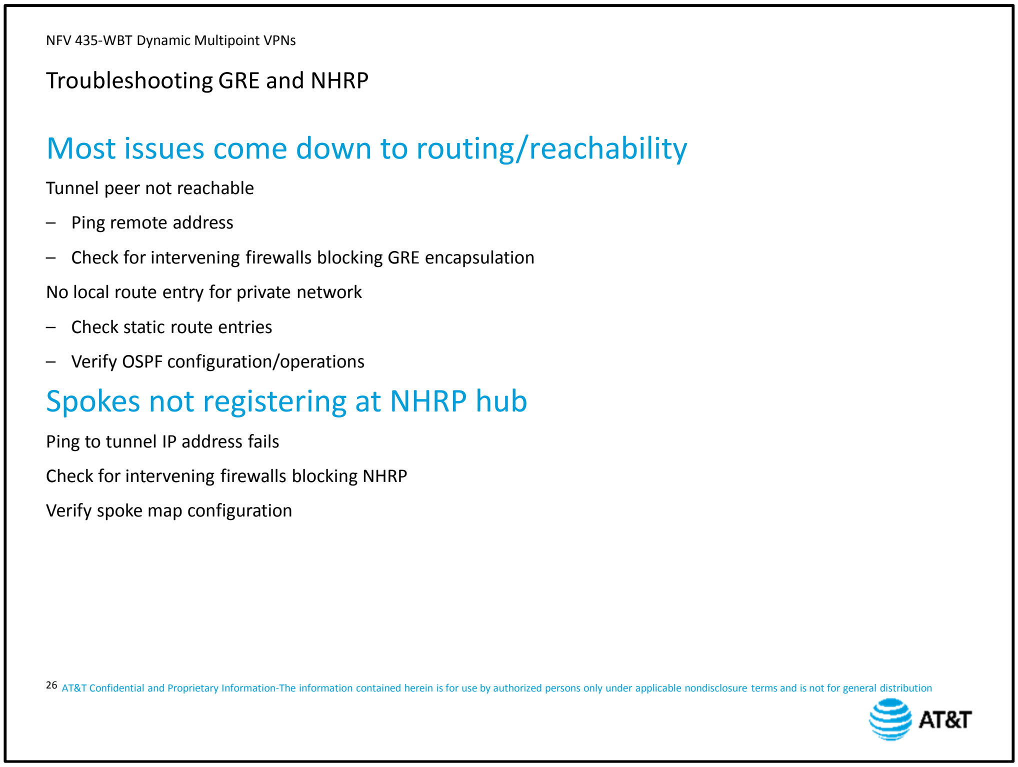
```
vyatta@VYA1:~$ show ip nhrp
Status: ok

Interface: tun0
Type: local
Protocol-Address: 10.100.100.255/32
Alias-Address: 10.100.100.1
Flags: up

Interface: tun0
Type: local
Protocol-Address: 10.100.100.1/32
Flags: up

Interface: tun0
Type: dynamic
Protocol-Address: 10.100.100.2/32
NBMA-Address: 172.24.42.52
Flags: up
<Truncated Output>
```

Spoke Configuration

```
vyatta@VYA2:~$ show ip nhrp
Status: ok

Interface: tun0
Type: local
Protocol-Address: 10.100.100.2/32
Flags: up

Interface: tun0
Type: dynamic
Protocol-Address: 10.100.100.3/32
NBMA-Address: 172.24.42.53
Flags: used up

Interface: tun0
Type: static
Protocol-Address: 10.100.100.1/24
NBMA-Address: 172.24.42.51
Flags: up
<Truncated Output>
```

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 NHRP is working, use the command `show ip nhrp`.
On the hub, the output will display two local addresses –
the tunnel address, and the broadcast address for the tunnel subnet.
It will also display all addresses that have been dynamically registered via NHRP, and the associated physical interface address. These dynamic addresses are the ones that will be shared across all NHRP clients.
On the spoke,
you will see the same two local addresses – we have omitted one here to make room on the screen.
Dynamic addresses are ones learned from the NHRP next-hop server – in this case, the hub.
This is the address of another spoke in the network.
On a spoke, you will also see a static entry. This is the address map that you configured when you set the spoke up as an NHRP client.



NFV 435-WBT Dynamic Multipoint VPNs

Troubleshooting GRE and NHRP

Most issues come down to routing/reachability

Tunnel peer not reachable

- Ping remote address
- Check for intervening firewalls blocking GRE encapsulation

No local route entry for private network

- Check static route entries
- Verify OSPF configuration/operations

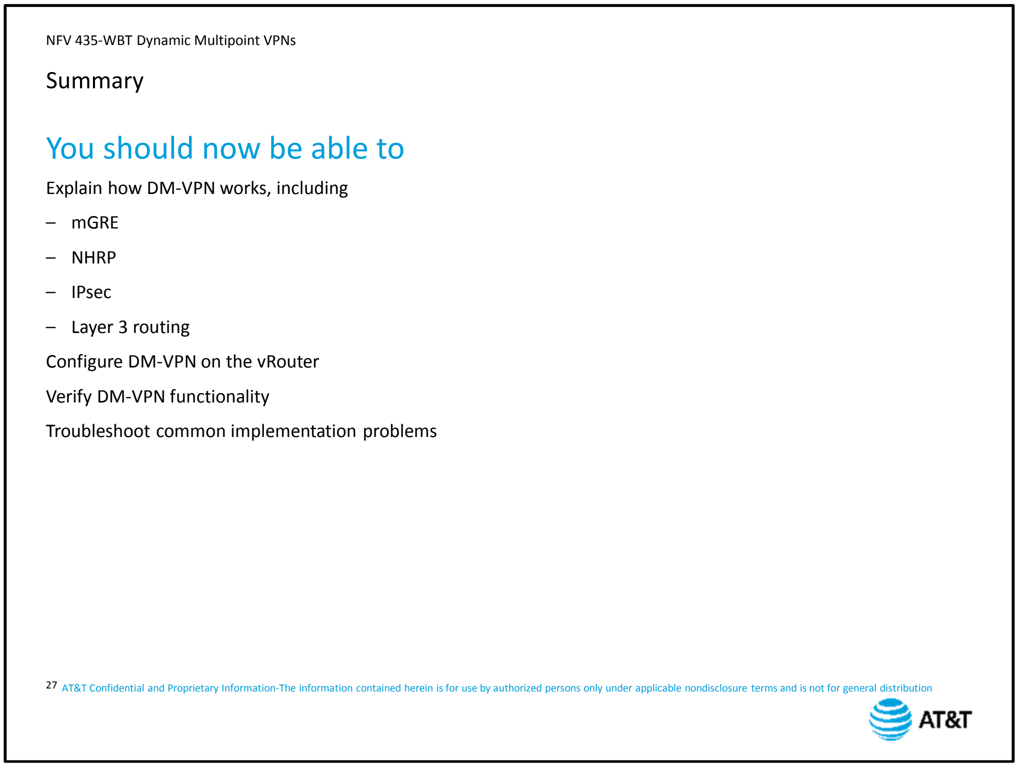
Spokes not registering at NHRP hub

Ping to tunnel IP address fails

Check for intervening firewalls blocking NHRP

Verify spoke map configuration

In most cases, problems with GRE and NHRP come down to routing and reachability issues.
If the tunnel interface is down, it means that the device was unable to establish a GRE connection to the peer device.
The first test in that case is to ping the physical address of the remote peer. If the ping is successful, it means that basic IP connectivity is working. If not, then you need to troubleshoot the routing between the two sites.
If ping works but there is still no GRE connection, check to see if there are any firewalls between the two sites that are blocking GRE packets.
If the tunnel interface is up, but the private networks cannot reach each other, the problem is usually a routing issue on the hub or spoke.
If you are using static route entries, make sure that you have a static route on both sides of the tunnel.
If you are using OSPF, verify that you are learning routes over the tunnel. If not, troubleshoot OSPF accordingly.
Another problem that may arise with NHRP is that the spoke devices are not registering with the hub, preventing a spoke from reaching any other device, including the hub itself.
In this case, the tunnel interface will show as up, but no traffic will flow.



NFV 435-WBT Dynamic Multipoint VPNs

Summary

You should now be able to

Explain how DM-VPN works, including

- mGRE
- NHRP
- IPsec
- Layer 3 routing

Configure DM-VPN on the vRouter

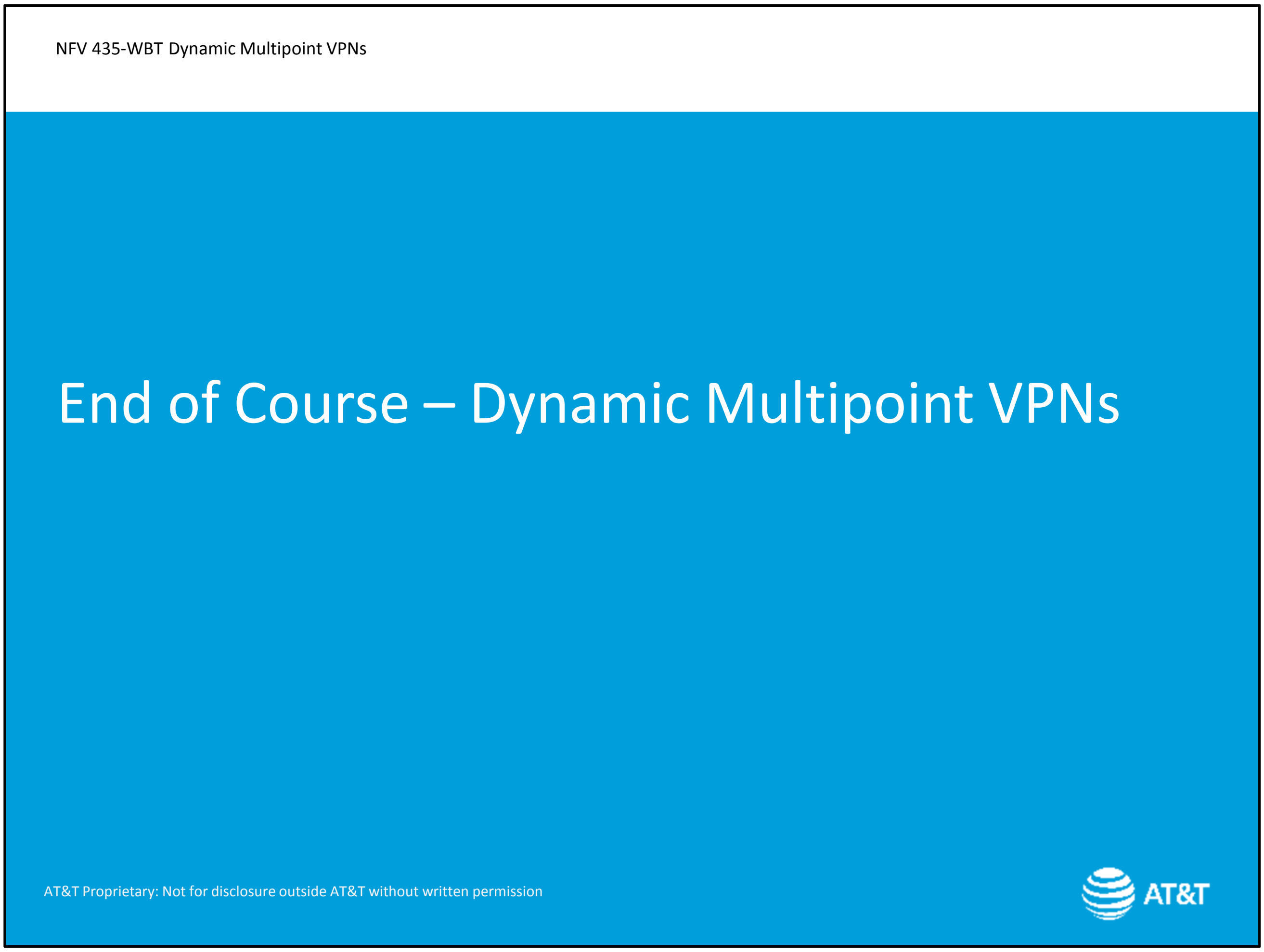
Verify DM-VPN functionality

Troubleshoot common implementation problems

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

Congratulations! You have completed the AT&T vRouter Dynamic Multipoint VPN course. You should now be able to:

- Explain how Dynamic Multipoint VPNs work
- Configure DM-VPNs on the vRouter
- Verify DM-VPN functionality
- Troubleshoot common implementation problems



NFV 435-WBT Dynamic Multipoint VPNs

End of Course – Dynamic Multipoint VPNs

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

AT&T